Skript zur Vorlesung „Algebra und Zahlentheorie“

Alexander Schmitt

Berlin, Wintersemester 2011/2012

Inhalt

Vorwort

Ein großer Teil der Algebra beschäftigt sich mit Systemen polynomialer Gleichungen mit Koeffizienten in einem **Ring** R,[1] d.h. zu Polynomen

$$f_i \in R[x_1, ..., x_n], \quad i = 1, ..., s,$$

sind die Elemente $\xi_1, ..., \xi_n \in R$ mit

$$f_i(\xi_1, ..., \xi_n) = 0, \quad i = 1, ..., s, \tag{1}$$

gesucht. Wir schauen uns ein paar Beispiele dazu an.

(1) Es seien R ein Körper und $f_1, ..., f_s$ **lineare** Polynome, d.h. es gibt Elemente a_{ij}, $b_i \in R$, $j = 1, ..., n$, $i = 1, ..., s$, so dass

$$f_i(x_1, ..., x_n) = a_{i1} \cdot x_1 + \cdots + a_{in} \cdot x_n + b_i.$$

In diesem Fall ist die Untersuchung des Gleichungssystems (1) Teil der Linearen Algebra und wird mit dem Gauß-Algorithmus durchgeführt.

a) Das Gleichungssystem

$$\begin{array}{rrcl} \text{I)} & 3x_1 - 5x_2 & = & 2 \\ \text{II)} & -3x_1 + 5x_2 & = & 1 \end{array}$$

hat keine Lösung, denn die Addition der beiden Gleichungen führt zu

$$0 = 3.$$

Im abstrakten Formalismus der Linearen Algebra kann man das durch

$$\begin{pmatrix} 2 \\ 1 \end{pmatrix} \notin \left\langle \begin{pmatrix} 3 \\ -3 \end{pmatrix}, \begin{pmatrix} -5 \\ 5 \end{pmatrix} \right\rangle = \left\langle \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right\rangle$$

ausdrücken.

b) Das Gleichungssystem

$$\begin{array}{rcl} 4x_1 - x_2 - 9x_3 & = & 0 \\ -x_1 + 2x_2 + 4x_3 & = & 0 \\ 2x_1 - x_2 - 5x_3 & = & 0 \end{array}$$

[1] An dieser Stelle genügt es, sich unter R einen Körper, z.B. $\mathbb{Q}$, $\mathbb{R}$ oder $\mathbb{C}$, oder den Ring $\mathbb{Z}$ der ganzen Zahlen vorzustellen.

formen wir zunächst in das äquivalente Gleichungssystem

$$\begin{aligned} x_1 - 2x_2 - 4x_3 &= 0 \\ 7x_2 + 7x_3 &= 0 \\ 3x_2 + 3x_3 &= 0 \end{aligned}$$

um. Dieses ist wiederum äquivalent zu

$$\begin{aligned} x_2 &= -x_3 \\ x_1 + 2x_2 &= 0 \end{aligned}$$

und damit zu

$$x_1 = -2x_2 = 2x_3.$$

Der Lösungsraum des gegebenen Gleichungssystems ist somit der lineare Teilraum

$$\mathbb{L} = \left\langle \begin{pmatrix} 2 \\ -1 \\ 1 \end{pmatrix} \right\rangle$$

des $\mathbb{R}^3$. Die Tatsache, dass der Lösungsraum eindimensional ist, ist im Dimensionsbegriff der Linearen Algebra begründet: Der Vektorraum R^3 ist dreidimensional und

$$\dim_R \left(\left\langle \begin{pmatrix} 4 \\ -1 \\ 2 \end{pmatrix}, \begin{pmatrix} -1 \\ 2 \\ -1 \end{pmatrix}, \begin{pmatrix} -9 \\ 4 \\ -5 \end{pmatrix} \right\rangle \right) = 2.$$

(2) Verlässt man das Reich der linearen Gleichungen, wird alles gleich komplizierter: Die Gleichung

$$x^2 - 2$$

hat

- ⋆ in $\mathbb{Q}$ keine Lösung,
- ⋆ in $\mathbb{R}$ zwei Lösungen, und zwar $\pm\sqrt{2}$.

Die Gleichung

$$x^2 + 1$$

hat

- ⋆ in $\mathbb{R}$ keine Lösung,
- ⋆ in $\mathbb{C}$ zwei Lösungen, und zwar $\pm i$.

Die Lösbarkeit der Gleichung hängt also davon ab, über welchem Körper wir arbeiten.

Allgemein hat die quadratische Gleichung

$$ax^2 + bx + c = 0, \quad a, b, c \in \mathbb{C},\ a \neq 0,$$

die **komplexen** Lösungen

$$\frac{-b \pm \sqrt{b^2 - 4ac}}{2a}. \tag{2}$$

Es gilt sogar der

Fundamentalsatz der Algebra. *Seien $n \geq 1$ und $a_0, ..., a_n \in \mathbb{C}$, $a_n \neq 0$. Dann hat das Polynom*

$$f = a_0 + a_1 x + \cdots + a_n x^n$$

eine Nullstelle $\xi \in \mathbb{C}$.

So wichtig dieses Ergebnis für die Mathematik ist, es hilft uns nicht sehr viel bei der Untersuchung polynomialer Gleichungen mit Koeffizienten in $\mathbb{Q}$, denn

- ⋆ der Körper $\mathbb{C}$ hängt nicht vom Polynom $f \in \mathbb{Q}[x]$ ab,
- ⋆ $\dim_{\mathbb{Q}}(\mathbb{C}) = \infty$.

Wir verfolgen deshalb folgende Strategie: Zu einem Polynom $f \in \mathbb{Q}[x]$ suchen wir einen „möglichst kleinen“ Körper K mit $\mathbb{Q} \subset K \subset \mathbb{C}$, so dass a) f in K eine Nullstelle hat oder b) f über K vollständig in Linearfaktoren zerfällt. Für solch einen Körper K gilt

$$\dim_{\mathbb{Q}}(K) < \infty.$$

Damit können wir die Techniken der Linearen Algebra bei der Untersuchung der **Körpererweiterung** $\mathbb{Q} \subset K$ einsetzen.

Für die Gleichung $x^2 - 2 = 0$ bekommen wir den Körper

$$K = \mathbb{Q}(\sqrt{2}) := \{\, a + b \cdot \sqrt{2} \mid a, b \in \mathbb{Q} \,\}.$$

Als $\mathbb{Q}$-Vektorraum ist K zweidimensional.

Die Gleichung $x^2 + 1 = 0$ führt uns zum Körper

$$K = \mathbb{Q}(i) := \{\, a + b \cdot i \mid a, b \in \mathbb{Q} \,\}.$$

Auch dies ist ein zweidimensionaler $\mathbb{Q}$-Vektorraum.

Das Studium polynomialer Gleichungen mit rationalen Koeffizienten haben wir nun in das Studium von Körpererweiterungen $\mathbb{Q} \subset K$ mit $\dim_{\mathbb{Q}}(K) < \infty$ überführt. Leider genügt die Lineare Algebra nicht, um solche Körpererweiterungen vollständig zu verstehen. Das wirksamste Werkzeug ist hier die sogenannte **Galois-Theorie**. Man ordnet einer Körpererweiterung $\mathbb{Q} \subset K$ ihre **Galois-Gruppe**

$$\mathrm{Gal}_{\mathbb{Q}}(K) := \{\, f \colon K \longrightarrow K \mid f \text{ ist Körperautomorphismus und } f_{|\mathbb{Q}} = \mathrm{id}_{\mathbb{Q}} \,\}$$

zu.

Mit dem gerade skizzierten Formalismus kann man folgende Probleme verstehen:

- ⋆ Die Konstruktionsprobleme der Antike, d.h. die Würfelverdopplung, die Winkeldreiteilung und die Quadratur des Kreises (s. Kapitel IV).
- ⋆ Eine Gleichung vom Grad 2, 3 oder 4 lässt sich durch iteriertes Wurzelziehen lösen (vgl. (2)). Ist dies auch für Gleichungen beliebigen Grades möglich?

(3) Es seien p eine Primzahl und $\mathbb{F}_p$ ein endlicher Körper mit p Elementen. Für ein Polynom

$$f = a_0 + a_1 x + \cdots + a_n x^n, \quad a_0, ..., a_n \in \{ 0, ..., p-1 \}, \quad a_n \neq 0,$$

entspricht die Gleichung

$$f(\xi) = 0 \quad (\text{in } \mathbb{F}_p)$$

der Kongruenz

$$f(\zeta) \equiv 0 \bmod p \quad (\text{in } \mathbb{Z}).$$

(4) **Diophantische Gleichungen.** Hier ist $R = \mathbb{Z}$ oder $R = \mathbb{Q}$. Als Beispiel einer sogenannten diophantischen Gleichung betrachten wir die **Fermat-Gleichung** aus dem Jahr **1637**:

Fermatsche Vermutung. *Es sei $p \geq 3$ eine Primzahl. Dann gibt es keine drei nichtverschwindenden ganzen Zahlen $a, b, c \in \mathbb{Z} \setminus \{0\}$ mit*[2]

$$a^p + b^p = c^p.$$

Der Fall $p = 2$ ist anders gelagert. Hier gilt z.B.

$$3^2 + 4^2 = 5^2.$$

Die Fermatsche Vermutung konnte erst im Jahr 1995 durch Taylor und Wiles ([21], [23], [3]) gelöst werden. Der Beweis gehört zu den anspruchsvollsten mathematischen Werken und dürfte nur wenigen MathematikerInnen auf der Welt völlig verständlich sein.

Zwischen diophantischen Gleichungen und Gleichungen über endlichen Körpern bzw. Kongruenzen in den ganzen Zahlen besteht folgender Zusammenhang: Es sei $f \in \mathbb{Z}[x_1, ..., x_n]$ ein ganzzahliges Polynom. Eine **notwendige Bedingung** für die Lösbarkeit der Gleichung

$$f(\eta_1, ..., \eta_n) = 0$$

mit $\eta_1, ..., \eta_n \in \mathbb{Z}$ ist, dass für **jede Primzahl** p die Gleichung

$$f(\xi_1, ..., \xi_n) = 0 \tag{3}$$

in $\mathbb{F}_p$ bzw. die Kongruenz

$$f(\zeta_1, ..., \zeta_n) \equiv 0 \bmod p$$

in $\mathbb{Z}$ lösbar ist. Für jede gegebene Primzahl p ist letzteres wesentlich einfacher zu verifizieren: Schlimmstenfalls kann man in (3) die endlich vielen Möglichkeiten für $\xi_1, ..., \xi_n$ aus $\mathbb{F}_p$ ausprobieren.

Die obige Diskussion motiviert die Themenauswahl für die Vorlesung: In Kapitel I bzw. Kapitel III werden wir uns mit linearen bzw. quadratischen Kongruenzen beschäftigen. In Kapitel IV untersuchen wir Körpererweiterungen und erste Beispiele der Galois-Theorie in Hinblick auf die Konstruktionsprobleme der Antike und die Konstruierbarkeit regelmäßiger n-Ecke, $n \geq 3$. Den Schwerpunkt des Skripts bildet Kapitel II. Dort werden die Grundzüge der Gruppentheorie behandelt. Die obigen Beispiele zeigen, dass die

[2] Dahinter steckt die Gleichung $x^p + y^p - z^p = 0$.

Gruppentheorie relevant für das Studium algebraischer Gleichungen ist. Daneben ist sie für viele andere Disziplinen von Bedeutung und auch von eigenständigem Interesse. Wir versuchen, den Gruppenbegriff von verschiedenen Standpunkten aus zu beleuchten. Dabei werden wir sowohl einige praktische Beispiele kennenlernen als auch fundanmentale Strukturresultate.

Der Fall allgemeiner Gleichungssysteme über beliebigen Körpern oder Ringen ist Gegenstand der Kurse Algebra I-III.

Ich danke Frau Anna Wißdorf und Herrn Norbert Hoffmann für die Durchsicht des Manuskripts und zahlreiche Korrekturen. Die biographischen Angaben zu den MathematikerInnen stammen aus WIKIPEDIA. Die Literaturvorlagen werden in den Einleitungen der Kapitel genannt.

Alexander Schmitt
Berlin, im Februar 2012

I

Der Hauptsatz der elementaren Zahlentheorie

Erwartungsgemäß beschäftigt sich die Zahlentheorie mit Zahlen. Die zu untersuchenden Zahlen sind zunächst die **ganzen Zahlen**. Wir sind seit früher Kindheit mit dem Rechnen in den natürlichen Zahlen vertraut. Das gilt insbesondere für die Division mit Rest: Sollen 14 Bonbons an fünf Kinder verteilt werden, dann erhält jedes Kind 2 Bonbons und vier Bonbons bleiben übrig. Die Division 14:5 „geht nicht auf“. Wenn für zwei ganze Zahlen a und b die Division $b : a$ aufgeht, dann sagt man, dass die Zahl a die Zahl b **teilt**. Damit gelangen wir zur Teilbarkeitsrelation auf den ganzen Zahlen. Eine besondere Rolle kommt dabei den **Primzahlen** zu. Dies sind — mit Ausnahme der 1 — diejenigen natürlichen Zahlen, die nur von 1 und sich selbst geteilt werden. Jede natürliche Zahl lässt sich in eindeutiger Weise als Produkt von Primzahlen schreiben. Die Primzahlen sind also die Bausteine für alle natürlichen Zahlen. Dieses Resultat ist der **Hauptsatz der elementaren Zahlentheorie**. Wir werden den Hauptsatz in diesem Abschnitt detailliert herleiten. Zum einen üben wir damit den mathematischen Formalismus an einem wohlbekannten Resultat ein, zum anderen stellen wir damit eine wichtige Grundlage für viele weitere Ergebnisse bereit.

Interessiert man sich bei der Division mit Rest nur für den Rest, dann gelangt man zu der Kongruenzrechnung. Das simultane Lösen von Kongruenzen gehört seit langer Zeit zum Repertoire der Mathematik. Das Verfahren, das man hier verwendet, besteht aus dem euklidischen Algorithmus und dem chinesischen Restsatz. Der chinesische Restsatz wird uns in Kapitel III im Rahnem der Ringtheorie erneut begegnen und dort neben seiner praktischen Bedeutung beim Rechnen eine theoretische Bedeutung für die Strukturtheorie von Gruppen und Ringen erlangen.

Die Darstellung in diesem Kapitel basiert auf den entsprechenden Abschnitten im Buch [14]. Für weiterführende Ergebnisse zu Primzahlen empfehlen wir [15].

I.1 Division mit Rest

Der Ring $\mathbb{Z}$ und die Betragsfunktion $|\cdot|\colon \mathbb{Z} \longrightarrow \mathbb{N}$ werden als bekannt vorausgesetzt (vgl. z.B. [16], Abschnitt 1.4 und Definition 1.6.5).

I.1.1 Satz (Division mit Rest). *Es seien $a, b \in \mathbb{Z}$ ganze Zahlen mit $b \neq 0$. Dann existieren **eindeutig bestimmte** ganze Zahlen q, r, so dass gilt*

- $\star$ $a = q \cdot b + r$,
- $\star$ $0 \leq r < |b|$.

Im Beweis des Satzes verwenden wir:

I.1.2 Das Prinzip vom kleinsten Element. *Es sei $S \subset \mathbb{N}$ eine **nichtleere** Teilmenge. Dann gibt es ein Element $s_0 \in S$, so dass*

$$\forall s \in S : \quad s_0 \leq s.$$

Beweis. [16], Satz 1.3.22. □

Die Beweise, die wir im Folgenden mit dem Prinzip vom kleinsten Element führen werden, ließen sich auch mit vollständiger Induktion führen. Allerdings wäre die Induktion in den entsprechenden Fällen etwas mühsam zu formulieren.

Beweis von Satz I.1.1. Wir widmen uns zunächst der Eindeutigkeit. Dazu betrachten wir ganze Zahlen q_1, q_2, r_1 und r_2 mit

$$q_1 \cdot b + r_1 = q_2 \cdot b + r_2$$

und

$$0 \leq r_1 \leq r_2 < |b|.$$

Damit schließen wir, dass

$$(q_1 - q_2) \cdot b = r_2 - r_1.$$

Zusammen mit $0 \leq r_2 - r_1 \leq r_2 < |b|$ folgern wir

$$|b| > \big|(q_1 - q_2) \cdot b\big| = |q_1 - q_2| \cdot |b|.$$

Da $|q_1 - q_2|$ eine nichtnegative ganze Zahl ist, bedeutet dies $|q_1 - q_2| = 0$, also $q_1 = q_2$. Daraus folgt auch $r_1 = r_2$.

Die Existenz beweisen wir zunächst im Fall $b > 0$. Wir fordern $r = a - q \cdot b \geq 0$. Es sei

$$S := \{\, s \in \mathbb{N} \mid \exists u \in \mathbb{Z} : s = a - u \cdot b \,\} \subset \mathbb{N}.$$

Wir beweisen zunächst, dass S nichtleer ist. Für $u = -|a|$ gilt

$$a - u \cdot b = a + |a| \cdot b \overset{b>0}{\geq} a + |a| \geq 0,$$

so dass $a + |a| \cdot b \in S$. Nach Satz I.1.2 enthält S ein kleinstes Element r. Nach Definition gilt $r \geq 0$. Sei weiter $q \in \mathbb{Z}$ mit $r = a - q \cdot b$. Mit $b > 0$ finden wir

$$r > r - b = a - q \cdot b - b = a - (q + 1) \cdot b.$$

Nach Wahl von r gilt $r - b \notin S$, d.h. $r - b < 0$ und folglich $r < b$. Zusammengefasst gilt $a = q \cdot b + r$ und $0 \leq r < b$.

Jetzt behandeln wir den Fall $b < 0$. Nach dem zuvor Gesagten gibt es Elemente $q', r \in \mathbb{Z}$, so dass

$$a = q' \cdot (-b) + r \quad \text{mit} \quad 0 \leq r < -b = |b|.$$

Wir setzen folglich $q := -q'$. □

I.2 Teilbarkeit

Die Grundidee bei der Untersuchung ganzer Zahlen ist, diese in kleinere Bestandteile zu zerlegen. Dabei wird ein Produkt $b = a \cdot c$ mit $a, b, c \in \mathbb{Z} \setminus \{0, \pm 1\}$ als Zerlegung der ganzen Zahl b in die kleineren Bestandteile a und c aufgefasst. Diese Idee formulieren wir eleganter mit Hilfe der Teilbarkeitsrelation.

I.2.1 Definition. Es seien $a, b \in \mathbb{Z}$. Wir sagen, *a teilt b*, wenn es eine ganze Zahl c mit

$$b = a \cdot c$$

gibt.
Schreibweise. $a|b$.

Wir erstellen nun eine Liste mit den ersten grundlegenden Eigenschaften der Teilbarkeitsrelation. Sie werden im Folgenden immer wieder benötigt werden.

I.2.2 Eigenschaften. i) $\forall a \in \mathbb{Z} : a|0$.
ii) $\forall a \in \mathbb{Z} : 0|a \iff a = 0$.
iii) $\forall b \in \mathbb{Z} : \pm 1|b$ *und* $\pm b|b$.
iv) $\forall a, b, c \in \mathbb{Z} : a|b \implies a|(b \cdot c)$.
v) $\forall a, b_1, b_2, c_1, c_2 \in \mathbb{Z}$*:* $(a|b_1 \wedge a|b_2) \implies a|(b_1 \cdot c_1 + b_2 \cdot c_2)$.
vi) $\forall a, b \in \mathbb{Z}$*,* $c \in \mathbb{Z} \setminus \{0\}$*:* $a|b \iff (a \cdot c)|(b \cdot c)$.
vii) $\forall a, b, c \in \mathbb{Z} : (a|b \wedge b|c) \implies a|c$.
viii) $\forall a, b \in \mathbb{Z} : (a|b \wedge b|a) \iff a = \pm b$.

Beweis. i) Es gilt $0 = a \cdot 0$.

ii) Die Richtung „$\Longleftarrow$“ folgt aus i). Wenn $0|a$ für $a \in \mathbb{Z}$ gilt, dann existiert ein $b \in \mathbb{Z}$ mit $a = 0 \cdot b = 0$.

iii) Dies folgt aus der Gleichung $b = 1 \cdot b = (-1) \cdot (-b)$, $b \in \mathbb{Z}$.

iv) Dies ist eine Folgerung aus der Implikation „$b = a \cdot d \implies b \cdot c = a \cdot (d \cdot c)$“, $a, b, c \in \mathbb{Z}$.

v) Für $d_1, d_2 \in \mathbb{Z}$ mit $b_1 = a \cdot d_1$ und $b_2 = a \cdot d_2$ gilt $b_1 \cdot c_1 + b_2 \cdot c_2 = a \cdot (d_1 \cdot c_1 + d_2 \cdot c_2)$.

vi) Sei $d \in \mathbb{Z}$ mit $b = a \cdot d$. Dann gilt auch $b \cdot c = (a \cdot c) \cdot d$. Wenn umgekehrt $d \in \mathbb{Z}$ mit $b \cdot c = (a \cdot c) \cdot d$ gegeben ist, dann folgt $b \cdot c = (a \cdot d) \cdot c$ und $(b - a \cdot d) \cdot c = 0$. Da $c \neq 0$, impliziert diese Gleichung $b - a \cdot d = 0$ und daher $b = a \cdot d$.

vii) Die Gleichungen $b = a \cdot d$ und $c = b \cdot e$ führen auf die Gleichung $c = a \cdot (d \cdot e)$.

viii) Die Richtung „$\Longleftarrow$“ ist klar. Umgekehrt seien $c, d \in \mathbb{Z}$ mit $b = a \cdot c$ und $a = b \cdot d$. Daher haben wir $b = b \cdot (c \cdot d)$, i.e. $b \cdot (1 - c \cdot d) = 0$. Daraus folgt $b = 0$ (und damit $a = b \cdot d = 0$) oder $c \cdot d = 1$ und damit $d = \pm 1$. □

I.2.3 Aufgaben. Gegeben seien natürliche Zahlen $k, m, n \in \mathbb{N} \setminus \{0\}$, so dass $n = k \cdot m$.

a) Beweisen Sie folgende Aussage:

$$\forall a, b \in \mathbb{Z}: \quad (a^m - b^m) | (a^n - b^n).$$

b) Zeigen Sie weiter:

$$k \text{ ungerade} \quad \Longrightarrow \quad (\forall a, b \in \mathbb{Z}: \quad (a^m + b^m) | (a^n + b^n)).$$

Hinweis. Vgl. Beweis von Satz I.3.7 und Satz I.3.10.

I.3 Primzahlen

Wir verfolgen die zuvor formulierte Idee der Zerlegung ganzer Zahlen in kleinere Bausteine weiter. Offenbar kommt den Zahlen, die sich nicht zerlegen lassen, eine besondere Rolle zu.

I.3.1 Definition. Eine ganze Zahl $p \in \mathbb{Z}$ ist eine *Primzahl*, wenn

- $p > 1$,
- $\forall a \in \mathbb{N}: a | p \Longrightarrow a = 1 \vee a = p$.

Die Primzahlen sind die Bausteine für alle ganzen Zahlen. Diese Tatsache wird durch die Primfaktorzerlegung ausgedrückt.

I.3.2 Satz (Existenz einer Primfaktorzerlegung). *Es seien $n \in \mathbb{Z} \setminus \{0, \pm 1\}$ und $\varepsilon \in \{\pm 1\}$, so dass $\varepsilon \cdot n > 0$. Dann gibt es eine natürliche Zahl $s \geq 1$, Primzahlen $p_1 < \cdots < p_s$ und positive ganze Zahlen $k_1, ..., k_s$, so dass*

$$n = \varepsilon \cdot p_1^{k_1} \cdot \cdots \cdot p_s^{k_s}.$$

Wir werden weiter unten (Folgerung I.4.7) die Eindeutigkeit einer solchen Primfaktorzerlegung beweisen. Dies erklärt, warum wir 1 nicht als Primzahl zugelassen haben. Eine Primfaktorzerlegung können wir für jedes $k \geq 1$ mit $1 = 1^k$ multiplizieren, ohne das Ergebnis zu ändern.

Beweis von Satz I.3.2. Es genügt offenbar, den Fall $n > 0$ zu behandeln. Wir betrachten die Menge

$$S := \{ n > 1 \mid n \text{ ist kein Produkt von Primzahlen} \}.$$

Wir wollen nachweisen, dass diese Menge leer ist. Falls sie nicht leer wäre, besäße sie ein kleinstes Element n_0 (Satz I.1.2). Die Zahl n_0 ist keine Primzahl. Deshalb gibt es ganze Zahlen $a > 1$ und $b > 1$, so dass $n_0 = a \cdot b$. Es folgt $a < n_0$ und $b < n_0$. Deshalb sind a und b nicht in S enthalten und somit Produkte von Primzahlen. Dann ist aber auch $n_0 = a \cdot b$ ein Produkt von Primzahlen, und wir haben die Annahme $S \neq \emptyset$ zum Widerspruch geführt. □

Ein Großteil der Zahlentheorie beschäftigt sich mit Eigenschaften von Mengen von Primzahlen. Die erste wichtige Eigenschaft ist, dass die Menge aller Primzahlen unendlich ist.

I.3.3 Satz. *Es gibt unendlich viele Primzahlen.*

Beweis. Wir nehmen das Gegenteil an. Es seien

$$1 < p_1 < \cdots < p_s$$

alle Primzahlen und

$$n := 1 + p_1 \cdot \cdots \cdot p_s.$$

Gemäß Satz I.3.2 seien $k_1, ..., k_s$ nichtnegative ganze Zahlen, so dass

$$n = p_1^{k_1} \cdot \cdots \cdot p_s^{k_s}.$$

Sei $j \in \{ 1, ..., s \}$ mit $k_j \geq 1$. Dann gilt $p_j | n$. Weiter gilt $p_j | (p_1 \cdot \cdots \cdot p_s)$. Nach Eigenschaft I.2.2, v), folgt

$$p_j | (n - p_1 \cdot \cdots \cdot p_s), \quad \text{d.h.} \quad p | 1.$$

Das ist aber unmöglich. □

Nachdem den Primzahlen eine besondere Rolle verliehen wurde, ist es jetzt von Interesse herauszufinden, welche Zahlen Primzahlen sind. Wir beginnen mit einem einfachen klassischen Verfahren, mit dem sich leicht „kleine“ Primzahlen finden lassen.

Das Sieb des Eratosthenes

Es sei $N \in \mathbb{N}$ eine natürliche Zahl. Wir nehmen $N \geq 2$ an. Der folgende Algorithmus, das *Sieb des Eratosthenes*[1] genannt, bestimmt alle Primzahlen zwischen 2 und N.

- ⋆ Es seien $p_0 := 2$ und $N_0 := \{ 3, ..., N \}$.
- ⋆ Für $k \geq 0$ seien p_k und N_k bestimmt. Man setze

$$N_{k+1} := N_k \setminus \{ n \cdot p_k \mid n \geq 1 \}.$$

- ⋆ Falls $N_{k+1} = \emptyset$, breche man den Algorithmus ab.
- ⋆ Falls $N_{k+1} \neq \emptyset$, sei p_{k+1} die kleinste Zahl in N_{k+1}.

Der Algorithmus bricht nach endlich vielen Schritten ab und liefert Zahlen $p_0, p_1, ..., p_s$. Dies sind die Primzahlen, die zwischen 2 und N liegen. Man kann den Algorithmus noch etwas anschaulicher formulieren:

- ⋆ Man trage alle Zahlen zwischen 2 und N in eine Liste ein.
- ⋆ $p_0 := 2$.
- ⋆ Für $k \geq 0$ sei p_k bekannt.
- ⋆ Man streiche alle Zahlen der Form $n \cdot p_k$ mit $n \geq 2$ aus der Liste.

[1] Eratosthenes von Kyrene (ca. 276 - 194 v.u.Z.), griechischer Gelehrter.

- ⋆ Wenn es keine nicht gestrichene Zahl gibt, die größer als p_k ist, so beende man den Algorithmus. Andernfalls sei p_{k+1} die kleinste, nicht gestrichene Zahl, welche größer als p_k ist.
- ⋆ Wegen $p_0 < p_1 < \cdots$ bricht der Algorithmus nach endlich vielen Schritten ab. Die nicht gestrichenen Zahlen in der Liste sind die Primzahlen zwischen 2 und N.

I.3.4 Beispiel. Wir führen das Verfahren für $N = 50$ durch:

	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~

.

Die Primzahlen zwischen 2 und 50 sind 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 und 47.

I.3.5 Bemerkung. Ein Paar (p_1, p_2) von natürlichen Zahlen ist ein *Primzahlzwilling*, wenn p_1 und p_2 Primzahlen sind und $p_2 - p_1 = 2$ gilt. Beispiele sind $(3, 5)$, $(5, 7)$, $(11, 13)$, $(17, 19)$, $(29, 31)$ und $(41, 43)$. Der größte bekannte Primzahlzwilling ([15], Kapitel 4, Abschnitt III, Tabelle 17) ist

$$65\,516\,468\,355 \cdot 2^{333\,333} \pm 1,$$

hat 100 355 Stellen und wurde 2009 entdeckt. Es ist ein **ungelöstes Problem**, ob es unendlich viele Primzahlzwillinge gibt oder nicht.

I.3.6 Aufgabe. Bestimmen Sie mit dem Sieb des Eratosthenes alle Primzahlen zwischen 2 und 200.

Wir stellen zwei weitere mögliche Verfahren zur Erzeugung von Primzahlen vor.

Primzahlen der Form $b^m + 1$

Zunächst ergeben sich Einschränkungen an b und m, damit $b^m + 1$ eine Primzahl sein kann.

I.3.7 Satz. *Es seien $b \geq 2$ und $m \geq 1$ ganze Zahlen. Wenn $b^m + 1$ eine Primzahl ist, dann ist b gerade und es gibt eine ganze Zahl $k \geq 0$, so dass $m = 2^k$.*

Beweis. Wenn b ungerade ist, dann ist $b^m + 1$ gerade. Wegen $b \geq 2$ und $m \geq 1$ gilt $b^m + 1 > 2$, und $b^m + 1$ ist keine Primzahl.

Nun gelte $m \neq 2^k$ für alle $k \geq 0$. Folglich existieren eine Primzahl $p \geq 3$ und eine natürliche Zahl m' mit $m = p \cdot m'$. Da

$$b^m + 1 = (b^{m'})^p + 1,$$

können wir b durch $b^{m'}$ ersetzen und ohne Beschränkung der Allgemeinheit voraussetzen, dass $m = p$ und m damit ungerade ist. Wegen der Faktorisierung

$$b^p + 1 = (b + 1) \cdot (b^{p-1} - b^{p-2} + \cdots - b + 1)$$

ist $b^p + 1$ keine Primzahl. □

I.3.8 Definition. Eine Primzahl der Form

$$F_k := 2^{(2^k)} + 1, \quad k \geq 0,$$

nennt man *Fermat*[2]*-Primzahl*.

I.3.9 Beispiel. Die Zahlen $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ und $F_4 = 65\,537$ sind Fermat-Primzahlen. Die Zahl

$$F_5 = 4\,294\,967\,297$$

wird von 641 geteilt und ist daher keine Primzahl. Es ist ein **ungelöstes Problem**, ob es unendlich viele Fermat-Primzahlen gibt oder nicht. Es wird angenommen, dass es nur endlich viele Fermat-Primzahlen gibt.

Bis heute ist 65 537 die größte bekannte Fermat-Primzahl. Die beschriebene Methode scheint sich also nicht für die Erzeugung von Primzahlen zu eignen. Dabei sind Fermat-Primzahlen von großem Interesse: Gauß[3] zeigte nämlich, dass sich ein regelmäßiges n-Eck genau dann mit Zirkel und Lineal konstruieren lässt (vgl. Abschnitt IV.4), wenn die Primfaktorzerlegung von n die Gestalt $2^k \cdot p_1 \cdot \cdots \cdot p_s$ mit Fermat-Primzahlen $p_1 < \cdots < p_s$ hat. Solange es offene Fragen zu Fermat-Primzahlen gibt, ist auch das klassische Problem der Konstruierbarkeit von regelmäßigen n-Ecken mit Zirkel und Lineal nicht vollständig gelöst! Weitere Fragen und Ergebnisse zu den Zahlen F_k, $k \in \mathbb{N}$, enthält Kapitel 2 des Buchs [15].

Primzahlen der Form $2^m - 1$

Auch hier formulieren wir zunächst einschränkende Bedingungen.

I.3.10 Satz. *Es sei $m \geq 2$ eine ganze Zahl. Wenn $2^m - 1$ eine Primzahl ist, dann ist m eine Primzahl.*

Beweis. Es seien p eine Primzahl und m' eine ganze Zahl, so dass $m = p \cdot m'$. Es gilt $b := 2^p \geq 4$ und

$$2^m - 1 = b^{m'} - 1 = (b-1) \cdot (b^{m'-1} + \cdots + b + 1).$$

Es muss somit $m' = 1$ sein. □

I.3.11 Definition. Eine Primzahl der Form

$$M_p := 2^p - 1, \quad p \text{ Primzahl},$$

ist eine *Mersenne*[4]*-Primzahl*.

I.3.12 Beispiel. i) Die Zahlen $M_2 = 3$, $M_3 = 7$, $M_5 = 31$ und $M_7 = 127$ sind Mersenne-Primzahlen. Die Zahl $M_{11} = 2047 = 23 \cdot 89$ ist keine Primzahl.

ii) Die größte bekannte Mersenne-Primzahl (s. Wikipedia) ist

$$M_{57\,885\,161}.$$

Sie hat 17 425 170 Stellen.

iii) Die folgenden Fragen sind **ungelöst**:

[2]Pierre de Fermat (Anfang 17. Jahrhundert - 1665), französischer Mathematiker und Jurist.

[3]Johann Carl Friedrich Gauß (1777 - 1855), deutscher Mathematiker, Astronom, Geodät und Physiker.

[4]Marin Mersenne (1588 - 1648), französischer Theologe, Mathematiker und Musiktheoretiker.

⋆ Gibt es unendlich viele Mersenne-Primzahlen?

⋆ Gibt es unendlich viele Primzahlen $p \geq 2$, so dass M_p **keine** Primzahl ist?

Obwohl die Formel zur Erzeugung von Mersenne-Primzahlen der Formel zur Erzeugung von Fermat-Primzahlen ähnelt, ist sie wesentlich erfolgreicher. Mit ihr gelingt die — auch für praktische Belange relevante — Erzeugung großer Primzahlen. Ein Blick auf den entsprechenden WIKIPEDIA-Artikel zeigt, dass die Mersenne-Primzahlen seit geraumer Zeit die größten bekannten Primzahlen überhaupt liefern! Weitere spannende Informationen zu Mersenne-Primzahlen enthält das Buch [15] in Kapitel 2.

I.4 Größter gemeinsamer Teiler und kleinstes gemeinsames Vielfaches

Wir vertiefen das Studium der Teilbarkeitsrelation. Dadurch gelangen wir zu einer neuen Charakterisierung von Primzahlen, die es uns ermöglicht, die Eindeutigkeit der Primfaktorzerlegung zu beweisen und somit den Hauptsatz der elementaren Zahlentheorie zu gewinnen.

I.4.1 Definition. Es seien $a, b \in \mathbb{Z}$ zwei ganze Zahlen. Dann ist

$$T_{a,b} := \{\, k \in \mathbb{Z} \mid k|a \wedge k|b \,\}$$

die *Menge der gemeinsamen Teiler* von a und b.

I.4.2 Bemerkungen. i) Es gilt immer $1 \in T_{a,b}$, so dass $T_{a,b}$ nicht leer ist.
ii) Für $a = b = 0$ gilt nach Eigenschaft I.2.2, i), dass $T_{a,b} = \mathbb{Z}$.
iii) Es sei $a = 0$ und $b \neq 0$, dann gilt wieder nach Eigenschaft I.2.2, i), dass

$$T_{a,b} = \{\, k \in \mathbb{Z} \mid k|b \,\}.$$

Insbesondere haben wir

$$\forall k \in T_{a,b}: \quad |k| \leq |b|.$$

Gilt $a \neq 0$ und $b \neq 0$, dann finden wir

$$\forall k \in T_{a,b}: \quad |k| \leq \min\{\, |a|, |b| \,\}.$$

Wir erkennen, dass $T_{a,b}$ eine endliche Menge ist, wenn a und b nicht beide null sind.
iv) Für $a, b \in \mathbb{Z}$ hat man offenbar

$$\forall k \in \mathbb{Z}: \quad k \in T_{a,b} \quad \Longleftrightarrow \quad -k \in T_{a,b}.$$

I.4.3 Definitionen. Es seien $a, b \in \mathbb{Z}$ ganze Zahlen, nicht beide null.
i) Der *größte gemeinsame Teiler* von a und b ist die Zahl

$$\mathrm{ggT}(a, b) := \max T_{a,b}.$$

ii) Die Zahlen a und b sind *teilerfremd*, wenn $\mathrm{ggT}(a, b) = 1$, d.h. $T_{a,b} = \{\, \pm 1 \,\}$, erfüllt ist.

I.4.4 Satz. *Es seien $a, b \in \mathbb{Z}$ zwei ganze Zahlen, die nicht beide null sind, und $d := \mathrm{ggT}(a, b)$ ihr größter gemeinsamer Teiler.*

i) *Man hat*

$$d = \min\{\, n \geq 1 \mid \exists x, y \in \mathbb{Z} : n = x \cdot a + y \cdot b \,\}.$$

ii) *Sind a und b teilerfremd, dann gibt es ganze Zahlen x, y, so dass*

$$x \cdot a + y \cdot b = 1.$$

iii) *Für $k \in T_{a,b}$ gilt $k|d$.*

Beweis. i) Wir bilden die Menge

$$L_+ := \{\, n \geq 1 \mid \exists x, y \in \mathbb{Z} : n = x \cdot a + y \cdot b \,\}.$$

Da $a \neq 0$ oder $b \neq 0$, gilt $a^2 + b^2 > 0$ und somit $a^2 + b^2 \in L_+$, so dass $L_+ \neq \emptyset$. Es sei $l \in L_+$ das kleinste Element.

Behauptung 1. *Es gilt $l|a$ und $l|b$.*

Um dies einzusehen, seien $x_0, y_0 \in \mathbb{Z}$ ganze Zahlen mit $l = x_0 \cdot a + y_0 \cdot b$. Wir führen die Division $a = q \cdot l + r$ mit $0 \leq r < l$ durch. Nun haben wir

$$r = a - q \cdot l = a - q \cdot x_0 \cdot a - q \cdot y_0 \cdot b = (1 - q \cdot x_0) \cdot a + (-q \cdot y_0) \cdot b.$$

Aus $0 \leq r < l$ und der Definition von l folgt $r = 0$, d.h. $l|a$. Analog sieht man $l|b$ ein. ✓

Behauptung 2. *Für $k \in T_{a,b}$ folgt $k|l$.*

Nach Eigenschaft I.2.2, v), der Teilbarkeitsrelation „|“ implizieren $k|a$ und $k|b$, dass $k|(x_0 \cdot a + y_0 \cdot b)$. ✓

Behauptung 2 zeigt $d|l$ und damit insbesondere $d \leq l$. Aus der ersten Behauptung ergibt sich $l \in T_{a,b}$ und deshalb $l \leq d$ nach Definition des größten gemeinsamen Teilers. Damit haben wir $d = l$ gezeigt.

ii) Dies ist ein Spezialfall von i).

iii) Auf Grund von Behauptung 2 gilt $k|l$ für jeden gemeinsamen Teiler $k \in T_{a,b}$ von a und b. Wie in i) gesehen gilt $d = l$, so dass die Behauptung gezeigt ist, □

Mit diesen Ergebnissen lässt sich eine weitere nützliche Charakterisierung von Primzahlen ableiten.

I.4.5 Satz. *Für eine natürliche Zahl $p \geq 2$ sind folgende Aussagen äquivalent:*

i) *p ist eine Primzahl.*

ii) $\forall a, b \in \mathbb{Z} : p|(a \cdot b) \Longrightarrow (p|a \vee p|b)$.

Beweis. „ii)$\Longrightarrow$i)“. Es gelte $p = a \cdot b$ mit $a > 0$ und $b > 0$. Aus $p|p$ folgern wir $p|a$ oder $p|b$. Ohne Beschränkung der Allgemeinheit setzen wir $p|a$ voraus. Es sei $a' \in \mathbb{Z}$ mit $a = a' \cdot p$. Damit folgt $p = (a' \cdot b) \cdot p$. Diese Gleichung kann nur gelten (vgl. Beweis von Eigenschaft I.2.2, vi), wenn $a' \cdot b = 1$. Wegen $b > 0$ bedeutet diese Gleichung $a' = b = 1$, und p ist als Primzahl gekennzeichnet.

„i)$\Longrightarrow$ii)“. Es seien a, b ganze Zahlen, so dass $p|(a \cdot b)$ und $p \nmid a$. Letzteres bedeutet $\mathrm{ggT}(a, p) = 1$. Nach Satz I.4.4, ii), existieren ganze Zahlen x, y mit

$$1 = x \cdot p + y \cdot a.$$

Somit gilt auch

$$b = (x \cdot b) \cdot p + y \cdot (a \cdot b).$$

Mit $p|p$, $p|(a \cdot b)$ und Eigenschaft I.2.2, v), sehen wir $p|((x \cdot b) \cdot p + y \cdot (a \cdot b))$. □

I.4.6 Folgerung. *Es seien p eine Primzahl, $n \geq 2$ und $a_1, ..., a_n \in \mathbb{Z}$ ganze Zahlen. Dann gilt:*

$$p|(a_1 \cdot \cdots \cdot a_n) \quad \Longleftrightarrow \quad \exists k \in \{1, ..., n\} : \ p|a_k.$$

Beweis. Nach Satz I.4.5 hat eine Primzahl Eigenschaft ii). Dies ist die Behauptung für $n = 2$. Der allgemeine Fall folgt mit einem leichten Induktionsbeweis. (Übung.) □

I.4.7 Folgerung. *Die Primfaktorzerlegung einer ganzen Zahl ist eindeutig bestimmt. Genauer gesagt folgt für ganze Zahlen $s, s' \geq 1$, Primzahlen $p_1 < \cdots < p_s$ und $p'_1 < \cdots < p'_{s'}$ und positive natürliche Zahlen $k_1, ..., k_s$ und $k'_1, ..., k'_{s'}$ mit*

$$p_1^{k_1} \cdot \cdots \cdot p_s^{k_s} = {p'_1}^{k'_1} \cdot \cdots \cdot {p'_{s'}}^{k'_{s'}}, \tag{I.1}$$

dass

$$s = s', \quad p_i = p'_i \quad \textit{und} \quad k_i = k'_i, \quad i = 1, ..., s.$$

Beweis. **Schritt 1.** Sei $j \in \{1, ..., s\}$. Gleichung (I.1) zeigt

$$p_j|({p'_1}^{k'_1} \cdot \cdots \cdot {p'_{s'}}^{k'_{s'}}).$$

Mit Folgerung I.4.6 schließen wir auf die Existenz eines Indexes $j' \in \{1, ..., s'\}$ mit

$$p_j|p'_{j'}, \quad \text{d.h.} \quad p_j = p'_{j'}.$$

Es folgt

$$\{p_1, ..., p_s\} \subset \{p'_1, ..., p'_{s'}\}.$$

Aus Symmetriegründen gilt auch die Inklusion „$\supset$“, so dass

$$\{p_1, ..., p_s\} = \{p'_1, ..., p'_{s'}\}.$$

Schritt 2. Seien nun $s \geq 1$, $p_1 < \cdots < p_s$ Primzahlen und $k_1, ..., k_s, k'_1, ..., k'_s$ positive ganze Zahlen mit

$$p_1^{k_1} \cdot \cdots \cdot p_s^{k_s} = p_1^{k'_1} \cdot \cdots \cdot p_s^{k'_s}. \tag{I.2}$$

Wir wollen $k_i = k'_i$, $i = 1, ..., s$, zeigen. Wir nehmen an, dass das nicht stimmt und setzen $j_0 := \min\{i = 1, ..., s \,|\, k_i \neq k'_i\}$. Wir dürfen dann ohne Beschränkung der Allgemeinheit $k_{j_0} < k'_{j_0}$ fordern. Wir teilen in (I.2) durch

$$p_1^{k_1} \cdot \cdots \cdot p_{j_0}^{k_0}$$

und finden

$$p_{j_0+1}^{k_{j_0+1}} \cdot \cdots \cdot p_s^{k_s} = p_{j_0}^{k'_{j_0} - k_{j_0}} \cdot p_{j_0+1}^{k'_{j_0+1}} \cdot \cdots \cdot p_s^{k'_s}.$$

Diese Gleichung widerspricht aber den Erkenntnissen aus Schritt 1. □

Satz I.3.2 und Folgerung I.4.7 fassen wir zusammen zu:

I.4.8 Hauptsatz der elementaren Zahlentheorie. *Es seien $n \in \mathbb{Z} \setminus \{0, \pm 1\}$ und $\varepsilon \in \{\pm 1\}$, so dass $\varepsilon \cdot n > 0$. Dann gibt es eine eindeutig bestimmte natürliche Zahl $s \geq 1$, eindeutig bestimmte Primzahlen $p_1 < \cdots < p_s$ und eindeutig bestimmte positive ganze Zahlen $k_1, ..., k_s$, so dass*

$$n = \varepsilon \cdot p_1^{k_1} \cdot \cdots \cdot p_s^{k_s}.$$

I.4.9 Aufgabe. Geben Sie die Primfaktorzerlegung der Zahl $-1\,601\,320$ an.

I.4.10 Aufgaben. Für eine natürliche Zahl $n \geq 1$ sei $T_n := \{ l \geq 1 \mid l|n \}$ die Menge ihrer Teiler.

a) Es sei $n = p_1^{k_1} \cdot \cdots \cdot p_s^{k_s}$ die Primfaktorzerlegung von n. Geben Sie eine Formel für die Anzahl $\#T_n$ der Teiler von n an.

b) Charakterisieren Sie diejenigen Zahlen, für die $\#T_n$ ungerade ist.

I.4.11 Aufgabe (Die Amnestie). Ein Herrscher hält 500 Personen in Einzelzellen gefangen, die von 1 bis 500 durchnummeriert sind. Anlässlich seines fünfzigsten Geburtstags gewährt er eine Amnestie nach folgenden Regeln:

- ⋆ Am ersten Tag werden alle Zellen aufgeschlossen.
- ⋆ Am Tag i wird der Schlüssel der Zellen i, $2i$, $3i$ usw. einmal umgedreht, d.h. Zelle j wird versperrt, wenn sie offen war, und geöffnet, wenn sie verschlossen war, $j = i$, $2i$, $3i$ usw., $i = 2, ..., 500$.
- ⋆ Wer am Ende des 500. Tages in einer offenen Zelle sitzt, ist frei und darf gehen.

Wieviele Gefangene kommen frei? Ist der Insasse von Zelle 179 unter den Freigelassenen?

Das Konzept des größten gemeinsamen Teilers ergänzen wir durch das Konzept des kleinsten gemeinsamen Vielfachen, das z.B. bei der Lösung von Kongruenzen dienlich sein wird.

I.4.12 Definition. Für ganze Zahlen a und b ist ihr *kleinstes gemeinsames Vielfaches* die Zahl[5]

$$\mathrm{kgV}(a,b) = \begin{cases} 0, & \text{falls } a = 0 \vee b = 0 \\ \min\{\, n \geq 1 \mid a|n \wedge b|n \,\}, & \text{falls } a \neq 0 \wedge b \neq 0 \end{cases}.$$

I.4.13 Lemma. *Für jede ganze Zahl k mit der Eigenschaft $a|k$ und $b|k$ folgt*

$$\mathrm{kgV}(a,b)|k.$$

Beweis. Es sei $m := \mathrm{kgV}(a,b)$. Wenn $a = 0$ oder $b = 0$, dann haben wir $m = 0$, und jedes gemeinsame Vielfache von a und b ist ebenfalls null. Andernfalls gilt $m \neq 0$, und wir schreiben $k = q \cdot m + r$ mit $0 \leq r < m$. Für $r = k - q \cdot m$ folgt aus $a|k$ und $a|m$, dass $a|r$ (Eigenschaft I.4.4, iv). Ebenso gilt $b|r$. Also $r \in \{ n \in \mathbb{N} \mid a|n \wedge b|n \}$. Aus der Definition von m folgt wie üblich $r = 0$. □

[5] Wenn $a \neq 0$ und $b \neq 0$, dann enthält die Menge $\{ n \geq 1 \mid a|n \wedge b|n \}$ das Element $|a| \cdot |b|$ und ist daher nicht leer.

I.4.14 Satz. *Für **positive** ganze Zahlen a und b hat man die Formel*

$$a \cdot b = \mathrm{ggT}(a,b) \cdot \mathrm{kgV}(a,b).$$

Beweis. Wir schreiben $m := \mathrm{kgV}(a,b)$. Nach Lemma I.4.13 gilt $m|(a \cdot b)$. Wir setzen $g := (a \cdot b)/m \in \mathbb{Z}$. Aus den Gleichungen

$$a = g \cdot \frac{m}{b} \quad \text{und} \quad b = g \cdot \frac{m}{a}$$

folgt

$$g|a \quad \text{und} \quad g|b.$$

Satz I.4.4, iii), zeigt $g|\mathrm{ggT}(a,b)$. Sei $d := \mathrm{ggT}(a,b)$. Wir haben

$$a\left|\left(a \cdot \frac{b}{d}\right)\right. \quad \text{und} \quad b\left|\left(\frac{a}{d} \cdot b\right)\right.$$

Lemma I.4.13 zeigt wieder

$$m\left|\left(\frac{a \cdot b}{d}\right)\right..$$

Daraus schließen wir

$$d\left|\left(\frac{a \cdot b}{m}\right)\right., \quad \text{d.h. } d|g.$$

Nach Eigenschaft I.2.2, viii), folgt aus $g|d$ und $d|g$, dass $d = \pm g$. Da beide Zahlen positiv sind, finden wir wie erwartet $d = g$. □

I.4.15 Aufgaben. Es seien $a, b \in \mathbb{N} \setminus \{0, 1\}$ natürliche Zahlen sowie

$$a = p_1^{k_1} \cdot \dots \cdot p_s^{k_s} \quad \text{und} \quad b = q_1^{l_1} \cdot \dots \cdot q_t^{l_t}$$

ihre Primfaktorzerlegungen.

a) Geben Sie die Primfaktorzerlegungen von $\mathrm{ggT}(a,b)$ und $\mathrm{kgV}(a,b)$ an.

b) Beweisen Sie die Formel

$$\mathrm{ggT}(a,b) \cdot \mathrm{kgV}(a,b) = a \cdot b$$

mit den Ergebnissen aus a).

I.5 Der euklidische Algorithmus

Wir stellen jetzt ein einfaches Verfahren vor, das es einem gestattet, den größten gemeinsamen Teiler von zwei ganzen Zahlen $a, b \in \mathbb{Z} \setminus \{0\}$ zu ermitteln, den sogenannten *euklidischen*[6] *Algorithmus*:

- ⋆ Man setze $a_0 := a$ und $a_1 := b$.
- ⋆ Falls $a_k = 0$ gilt, dann beende man die Rechnung.

[6] Euklid von Alexandria (ca. 360 bis 280 v.u.Z.), griechischer Mathematiker.

- ⋆ Andernfalls fahre man wie folgt fort: Wenn a_{k-1} und a_k für $k \geq 1$ schon bekannt sind, so wird a_{k+1} durch Divsion mit Rest bestimmt:

$$a_{k-1} = q_{k+1} \cdot a_k + a_{k+1}, \quad 0 \leq a_{k+1} < |a_k|.$$

Da $0 \leq a_{k+1} < |a_k| < |b|$, stoppt der Algorithmus nach höchstens $|b| - 1$ Schritten.

I.5.1 Bemerkung. Im Fall $a = 0$ und $b \neq 0$, der bisher ausgeschlossen wurde, und im Fall $a_2 = 0$ teilt b die Zahl a, und wir haben $\mathrm{ggT}(a, b) = |b|$.

Auf Grund dieser Bemerkung brauchen wir nur diejenigen Fälle anzuschauen, in denen $a_2 \neq 0$ gilt.

I.5.2 Satz. *Sei* $\boldsymbol{k \geq 2}$*, so dass* $a_i \neq 0$ *für* $i = 0, ..., k$ *und* $a_{k+1} = 0$*. Dann folgt*

$$a_k = \mathrm{ggT}(a, b).$$

Beweis. Für $i = 1, ..., k$ überlegt man sich leicht, dass

$$\mathrm{ggT}(a_{i-1}, a_i) = \mathrm{ggT}(q_{i+1} \cdot a_i + a_{i+1}, a_i) = \mathrm{ggT}(a_{i+1}, a_i).$$

Daraus folgt

$$\mathrm{ggT}(a, b) = \mathrm{ggT}(a_0, a_1) = \mathrm{ggT}(a_k, a_{k+1}) = \mathrm{ggT}(a_k, 0) \overset{\text{I.5.1}}{=} a_k$$

und somit die Behauptung des Satzes. □

I.5.3 Beispiel. Für $a = 93$ und $b = 42$ läuft der Algorithmus folgendermaßen ab:[7]

$$\begin{aligned} 93 &= 2 \cdot 42 + 9 \\ 42 &= 4 \cdot 9 + 6 \\ 9 &= 1 \cdot 6 + 3 \\ 6 &= 2 \cdot 3. \end{aligned}$$

Es folgt, dass $\mathrm{ggT}(93, 42) = 3$. (Probe: $93 = 3 \cdot 31$, $42 = 3 \cdot 14$ und $\mathrm{ggT}(31, 14) = 1$, denn 31 ist eine Primzahl, die 14 nicht teilt.)

I.5.4 Aufgaben. a) Bestimmen Sie den größten gemeinsamen Teiler von 165 und 585 mit dem euklidischen Algorithmus.

b) Geben Sie die Primfaktorzerlegungen von 165 und 585 an und überprüfen Sie das Ergebnis aus a) mit Ihrer Formel aus Aufgabe I.4.15, a).

Erweiterter euklidischer Algorithmus

Im nächsten Schritt verfeinern wir den euklidischen Algorithmus, so dass er zu gegebenen ganzen Zahlen $a, b \in \mathbb{Z} \setminus \{0\}$ nicht nur deren größten gemeinsamen Teiler auswirft, sondern auch Koeffizienten $x, y \in \mathbb{Z}$, für die $\mathrm{ggT}(a, b) = x \cdot a + y \cdot b$ gilt.

- ⋆ Es seien $a_0 := a$, $a_1 := b$, $x_0 := 1$, $x_1 := 0$, $y_0 := 0$ und $y_1 := 1$.

[7] Vertauscht man die Rollen von a und b, so lautet der erste Schritt $42 = 0 \cdot 93 + 42$. Danach läuft der Algorithmus ab wie dargestellt.

- ⋆ Falls $a_k = 0$, dann beende man die Berechnungen.
- ⋆ Andernfalls verfahre man folgendermaßen: Wenn für $k \geq 1$ die Zahlen a_{k-1}, a_k, x_{k-1}, x_k, y_{k-1} und y_k schon bestimmt wurden, so seien

$$\begin{aligned} a_{k+1} &:= a_{k-1} - q_{k+1} \cdot a_k, \qquad 0 \leq a_{k+1} < |a_k|, \\ x_{k+1} &:= x_{k-1} - q_{k+1} \cdot x_k, \\ y_{k+1} &:= y_{k-1} - q_{k+1} \cdot y_k. \end{aligned}$$

Der Algorithmus bricht offenbar nach endlich vielen Schritten ab. Die Fälle mit $a_2 = 0$ sind uninteressant (s. Bemerkung I.5.1). In den anderen Fällen haben wir:

I.5.5 Satz. *Sei* $\boldsymbol{k \geq 2}$*, so dass* $a_i \neq 0$ *für* $i = 0, ..., k$ *und* $a_{k+1} = 0$*. Dann folgt*

$$\mathrm{ggT}(a, b) = x_k \cdot a + y_k \cdot b.$$

Beweis. Wir zeigen induktiv, dass für alle i

$$a_i = x_i \cdot a + y_i \cdot b$$

gilt. Wegen $a_0 = a$ und $a_1 = b$ stimmt die behauptete Gleichung für $i = 0, 1$.

Weiter gilt nach Definition und Induktionsvoraussetzung

$$\begin{aligned} a_{i+1} &= a_{i-1} - q_{i+1} \cdot a_i \\ &= (x_{i-1} \cdot a + y_{i-1} \cdot b) - q_{i+1} \cdot (x_i \cdot a_i + y_i \cdot b_i) \\ &= (x_{i-1} - q_{i+1} \cdot x_i) \cdot a + (y_{i-1} - q_{i+1} \cdot y_i) \cdot b \end{aligned}$$

für $i \geq 1$. □

I.5.6 Beispiel. Wir betrachten abermals $a = 93$ und $b = 42$.

k	a_k	q_k	x_k	y_k
0	93	–	1	0
1	42	–	0	1
2	9	2	1	−2
3	6	4	−4	9
4	3	1	5	−11
5	0	2	–	–

.

Die Probe lautet:

$$3 = 5 \cdot 93 - 11 \cdot 42 = 465 - 462.$$

I.5.7 Aufgabe. Berechnen Sie mit dem erweiterten euklidischen Algorithmus den größten gemeinsamen Teiler d von 142 und 202 und ganze Zahlen x und y, so dass

$$d = x \cdot 142 + y \cdot 202.$$

I.6 Kongruenzrechnung

I.6.1 Definition. Es seien $a, b \in \mathbb{Z}$ zwei ganze Zahlen und $n \in \mathbb{N}$ eine natürliche Zahl. Wir sagen, dass *a kongruent b modulo n* ist, wenn

$$n|(a-b).$$

Schreibweise. $a \equiv b \bmod n$.

I.6.2 Aufgaben. Es sei $n \geq 1$ eine **positive** ganze Zahl. Beweisen Sie die folgenden Aussagen mit Hilfe der Division mit Rest I.1.1:

a) Zu jeder ganzen Zahl existiert **genau eine** Zahl $r \in \{0, ..., n-1\}$ mit $a \equiv r \bmod n$.

b) Zwei ganze Zahlen $a, b \in \mathbb{Z}$ sind genau dann kongruent modulo n, wenn sie denselben Rest bei der Division durch n haben, d.h., wenn es ganze Zahlen $q, q' \in \mathbb{Z}$ sowie $r \in \{0, ..., n-1\}$ mit

$$a = q \cdot n + r \quad \text{und} \quad b = q' \cdot n + r$$

gibt.

I.6.3 Lemma. *Die Relation „$\equiv \bmod n$“ ist eine Äquivalenzrelation.*

Beweis. Wir beginnen mit der **Reflexivität**. Es ist zu zeigen, dass $a \equiv a \bmod n$ für alle $a \in \mathbb{Z}$ gilt. Dies bedeutet $n|(a-a)$, $a \in \mathbb{Z}$, also $n|0$, und ist richtig.

Als nächstes ist die **Symmetrie** zu überprüfen. Zu zeigen ist, dass für $a \equiv b \bmod n$ auch $b \equiv a \bmod n$ gilt. Das stimmt, weil für alle $a, b \in \mathbb{Z}$ die Beziehung $n|(a-b)$ äquivalent zu $n|(b-a)$ ist.

Schließlich ist die **Transitivität** nachzuweisen. Gegeben seien $a, b, c \in \mathbb{Z}$ mit $a \equiv b \bmod n$ und $b \equiv c \bmod n$, und es ist $a \equiv c \bmod n$ zu folgern. Aus den vorausgesetzten Beziehungen $n|(a-b)$ und $n|(b-c)$ ergibt sich nach Eigenschaft I.2.2, v), auch die Beziehung $n|((a-b)+(b-c))$, d.h. die gewünschte Relation $n|(a-c)$. □

I.6.4 Beispiele. i) $-2 \equiv 7 \bmod 9$, $7 \equiv 16 \bmod 9$, $-1 \equiv 1 \bmod 2$. Für $n > 2$ gilt $-1 \not\equiv 1 \bmod n$.

ii) Die Aussage $a \equiv b \bmod 0$ ist äquivalent zu $a = b$.

iii) Für zwei beliebige ganze Zahlen a, b gilt $a \equiv b \bmod 1$.

iv) Für $a \in \mathbb{Z}$ und $n \in \mathbb{N}$ ist $a \equiv 0 \bmod n$ äquivalent zu $n|a$.

I.6.5 Beobachtung. *Gegeben seien eine natürliche Zahl $n \in \mathbb{N}$ und ganze Zahlen $a, a', b, b' \in \mathbb{Z}$, die den Bedingungen*

$$a \equiv a' \bmod n \quad \textit{und} \quad b \equiv b' \bmod n$$

genügen. Dann hat man auch

- ⋆ $a + b \equiv a' + b' \bmod n$,
- ⋆ $a \cdot b \equiv a' \cdot b' \bmod n$.

Beweis. Es gibt ganze Zahlen k, l, so dass $a = a' + k \cdot n$ und $b = b' + l \cdot n$. Damit berechnen wir

$$a + b = a' + k \cdot n + b' + l \cdot n = (a' + b') + k \cdot n + l \cdot n = (a' + b') + (k + l) \cdot n.$$

Daher teilt n die Differenz $(a + b) - (a' + b') = (k + l) \cdot n$, so dass $a + b \equiv a' + b' \bmod n$.

Weiter finden wir

$$\begin{aligned} a \cdot b &= (a' + k \cdot n) \cdot (b' + l \cdot n) \\ &= a' \cdot b' + a' \cdot l \cdot n + b' \cdot k \cdot n + k \cdot l \cdot n^2 \\ &= a' \cdot b' + (a' \cdot l + b' \cdot k + k \cdot l \cdot n) \cdot n. \end{aligned}$$

Die Differenz $a \cdot b - a' \cdot b' = (a' \cdot l + b' \cdot k + k \cdot l \cdot n) \cdot n$ ist durch n teilbar, und wir erkennen $a \cdot b \equiv a' \cdot b' \bmod n$. □

I.6.6 Beispiel (Teilbarkeitstests). Mit Hilfe der Kongruenzrechnung können wir die bekannten Teilbarkeitstests aus der Schule rechtfertigen. Es sei

$$a = \sum_{k=0}^{m} a_k \cdot 10^k \in \mathbb{Z} \quad \text{mit} \quad a_k \in \{0, ..., 9\},\ k = 0, ..., m.$$

Wir schreiben dies als Dezimalzahl:

$$a = a_m a_{m-1} \cdots a_1 a_0.$$

i) *Die Zahl a ist genau dann durch* 2 *teilbar, wenn die Ziffer* a_0 *es ist.* Da $10 \equiv 0 \bmod 2$ gilt nach Beobachtung I.6.5, dass

$$a = \sum_{k=0}^{m} a_k \cdot 10^k \equiv a_0 \bmod 2.$$

Die Kongruenzrelation ist transitiv (Lemma I.6.3), so dass genau dann $a \equiv 0 \bmod 2$ gilt, wenn $a_0 \equiv 0 \bmod 2$.

ii) *Die Zahl a ist genau dann durch* 3 *teilbar, wenn ihre Quersumme* $\sum_{k=0}^{m} a_k$ *es ist.* Wir haben $10 \equiv 1 \bmod 3$ und deshalb

$$a = \sum_{k=0}^{m} a_k \cdot 10^k \equiv \sum_{k=0}^{m} a_k \bmod 3.$$

Dies liefert sofort die Behauptung.

iii) *Die Zahl a ist genau dann durch* 5 *teilbar, wenn die Zahl* a_0 *durch* 5 *teilbar ist, d.h.* $a_0 = 0$ *oder* $a_0 = 5$. Wegen $10 \equiv 0 \bmod 5$ beweist man das genauso wie Teil i).

iv) *Die Zahl a ist genau dann durch* 11 *teilbar, wenn die* ***alternierende Quersumme*** $\sum_{k=0}^{m} (-1)^k \cdot a_k$ *durch* 11 *teilbar ist.* Mit $10 \equiv -1 \bmod 11$ sieht man

$$a = \sum_{k=0}^{m} a_k \cdot 10^k \equiv \sum_{k=0}^{m} (-1)^k \cdot a_k \bmod 11$$

und leitet die Behauptung ab.

I.6.7 Aufgabe. Es sei $(\varepsilon_k)_{k\in\mathbb{N}}$ die periodische Folge $(1, 3, 2, -1, -3, -2, ...)$, d.h. $\varepsilon_{6l} = 1$, $\varepsilon_{6l+1} = 3$, $\varepsilon_{6l+2} = 2$, $\varepsilon_{6l+3} = -1$, $\varepsilon_{6l+4} = -3$ und $\varepsilon_{6l+5} = -2$, $l \in \mathbb{N}$.

Beweisen Sie, dass eine ganze Zahl $a = \sum_{k=0}^{m} a_k \cdot 10^k$ genau dann durch 7 teilbar ist, wenn ihre **gewichtete Quersumme**

$$\sum_{k=0}^{m} \varepsilon_k \cdot a_k$$

es ist. Testen Sie mit diesem Kriterium die Zahlen 10 167 157 und 8 484 372 auf Teilbarkeit durch 7.

I.6.8 Aufgabe. Entwicklen Sie einen zu Aufgabe I.6.7 analogen Teilbarkeitstest für die Zahl 13. Wenden Sie diesen Test auf die Zahl 28 286 375 an.

I.6.9 Aufgabe. Es sei $a = \sum_{k=0}^{m} \varepsilon_k \cdot 2^k$, $\varepsilon_k \in \{0, 1\}$, $k = 0, ..., m$, eine ganze Zahl in **binärer Darstellung**. Geben Sie eine notwendige und hinreichende Bedingung an die Zahlen ε_0, ..., ε_m an, damit a durch 3 teilbar ist. Schreiben Sie die Zahl 351 in binärer Schreibweise und wenden den Test auf sie an.

I.6.10 Lemma. *Es seien $a, b \in \mathbb{Z}$ ganze Zahlen und $m, n \in \mathbb{N}$ natürliche Zahlen.*

i) *Falls $a \equiv b \bmod n$ und $m|n$ gilt, dann folgt $a \equiv b \bmod m$.*

ii) *Aus $a \equiv b \bmod n$ ergibt sich $m \cdot a \equiv m \cdot b \bmod (m \cdot n)$. Ist m nicht null, so gilt auch die Umkehrung.*

Beweis. i) Aus $m|n$ und $n|(a - b)$ folgt nach Eigenschaft I.2.2, vii), dass $m|(a - b)$, i.e. $a \equiv b \bmod m$.

ii) Mit $n|(a - b)$ erhält man offenbar $(m \cdot n)|(m \cdot (a - b))$, also $(m \cdot n)|(m \cdot a - m \cdot b)$ und $m \cdot a \equiv m \cdot b \bmod (m \cdot n)$. Falls $m \neq 0$, so zeigt Eigenschaft I.2.2, vi), dass $(m \cdot n)|(m \cdot (a - b))$ auch $n|(a - b)$ und damit $a \equiv b \bmod n$ impliziert. □

Lineare Kongruenzen

Zu ganzen Zahlen $a, b \in \mathbb{Z}$ und einer natürlichen Zahl[8] $n \geq 1$ möchten wir die Lösbarkeit der Kongruenz

$$a \cdot x \equiv b \bmod n \tag{I.3}$$

untersuchen.

Wenn $a \equiv 0 \bmod n$, dann muss auch $b \equiv 0 \bmod n$ gelten, damit (I.3) lösbar ist. In diesem Fall wird (I.3) durch alle ganzen Zahlen gelöst.

Wenn $a \not\equiv 0 \bmod n$, dann sind wir versucht, nach x aufzulösen, d.h. durch a zu dividieren. Das ist aber nicht immer möglich! Nehmen wir zuerst an, dass $n = p$ eine Primzahl ist. Nach Beispiel I.6.4, iv), bedeutet $a \not\equiv 0 \bmod p$, dass $p \nmid a$. Da p eine Primzahl ist, ist dies äquivalent zu $\mathrm{ggT}(a, p) = 1$. Nach Satz I.4.4, ii), existieren $y, z \in \mathbb{Z}$ mit

$$y \cdot a + z \cdot p = 1.$$

[8]Durch die Voraussetzung $n \neq 0$ garantieren wir, dass die vorkommenden größten gemeinsamen Teiler definiert sind.

Damit folgt aus I.3 unter Beachtung von Lemma I.6.3 und Beobachtung I.6.5

$$x \equiv y \cdot a \cdot x \equiv y \cdot b \bmod p. \tag{I.4}$$

Aus (I.4) erhält man (I.3) durch Multiplikation mit a. Die beiden Kongruenzen sind also äquivalent. Somit gibt Kongruenz (I.4) die Lösungen von (I.3) an, und wir haben diese Lösungen in gewisser Weise durch Division durch a erhalten. Dasselbe Verfahren funktioniert, wenn $\mathrm{ggT}(a, n) = 1$ gilt.

Sind a und n **nicht teilerfremd**, dann ergibt sich eine zusätzliche Lösbarkeitsbedingung. Der folgende Satz behandelt alle Fälle.

I.6.11 Satz. i) *Gilt* $\mathrm{ggT}(a, n) \nmid b$*, dann besitzt* (I.3) *keine Lösung.*

ii) *Es sei* $d := \mathrm{ggT}(a, n)$*, und es gelte* $d|b$*. Weiter seien ganze Zahlen* $y, z \in \mathbb{Z}$ *gegeben, so dass*

$$y \cdot a + z \cdot n = d.$$

Dann ist Gleichung (I.3) *äquivalent zu der Gleichung*

$$x \equiv y \cdot \frac{b}{d} \bmod \frac{n}{d}. \tag{I.5}$$

Mit dem erweiterten euklidischen Algorithmus lassen sich d und Zahlen y, z bestimmen, die $d = y \cdot a + z \cdot n$ erfüllen. Damit liefert der Satz ein explizites Verfahren zur Bestimmung aller Lösungen von (I.3).

Für eine Zahl $d \in \mathbb{Z} \setminus \{0\}$ mit $d|a$, $d|n$ und $d|b$ ist (I.3) nach Lemma I.6.10 äquivalent zu

$$\frac{a}{d} \cdot x \equiv \frac{b}{d} \bmod \frac{n}{d}.$$

Ist d der größte gemeinsame Teiler von a und n, dann sind a/d und n/d teilerfremd, und das Verfahren, das vor dem Satz geschildert wurde, ist anwendbar. Damit ist das Lösungsverfahren vollständig erklärt. Zur größeren Klarheit führen wir die Rechnungen im anschließenden Beweis detailliert aus.

Beweis von Satz I.6.11. i) Es sei $d := \mathrm{ggT}(a, n)$. Wenn x eine ganze Zahl ist, für die $a \cdot x \equiv b \bmod n$, dann existiert eine ganze Zahl k mit

$$a \cdot x = b + k \cdot n. \tag{I.6}$$

Anders gesagt, es ist $b = a \cdot x - k \cdot n$. Nun teilt d sowohl a als auch n und deshalb auch b (Eigenschaft I.2.2, v).

ii) „(I.3)$\Longrightarrow$(I.5)“. Auf Grund von (I.6) gilt

$$y \cdot a \cdot x = y \cdot b + y \cdot k \cdot n.$$

Mit Hilfe von $y \cdot a + z \cdot n = d$ formen wir diese Gleichung um zu

$$(d - z \cdot n) \cdot x = y \cdot b + y \cdot k \cdot n$$

und weiter zu

$$\begin{aligned} & d \cdot x &&= y \cdot b + (z \cdot x + y \cdot k) \cdot n \\ \Longleftrightarrow \quad & x &&= y \cdot \frac{b}{d} + (z \cdot x + y \cdot k) \cdot \frac{n}{d}. \end{aligned}$$

Anhand der letzten Gleichung erkennen wir

$$x \equiv y \cdot \frac{b}{d} \bmod \frac{n}{d}.$$

„(I.5)$\Longrightarrow$(I.3)“. Nach Voraussetzung existiert eine ganze Zahl $k \in \mathbb{Z}$, so dass

$$x = y \cdot \frac{b}{d} + k \cdot \frac{n}{d}.$$

Damit ergeben sich folgende Gleichungen

$$\begin{aligned} a \cdot x &= a \cdot y \cdot \frac{b}{d} + a \cdot k \cdot \frac{n}{d} \\ \Longrightarrow \quad a \cdot x &= (d - z \cdot n) \cdot \frac{b}{d} + \frac{a}{d} \cdot k \cdot n \\ \Longrightarrow \quad a \cdot x &= b + \left(k \cdot \frac{a}{d} - z \cdot \frac{b}{d} \right) \cdot n \\ \Longrightarrow \quad a \cdot x &\equiv b \bmod n. \end{aligned}$$

Damit ist eine Lösung der untersuchten Kongruenz gefunden worden. □

I.6.12 Beispiel. Es ist die Kongruenz

$$30 \cdot x \equiv 1 \bmod 101$$

zu lösen.

Die Primzahlen aus der Primfaktorzerlegung von 30 sind 2, 3 und 5. Keine dieser Primzahlen teilt 101, so dass ggT(30, 101) = 1 gilt. Mit dem erweiterterten euklidischen Algorithmus berechnen wir ganze Zahlen y und z, für die $30 \cdot y + 101 \cdot z = 1$ gilt:

k	a_k	q_k	y_k	z_k
0	30	–	1	0
1	101	–	0	1
2	30	0	1	0
3	11	3	−3	1
4	8	2	7	−2
5	3	1	−10	3
6	2	2	27	−8
7	1	1	−37	11
8	0	2	–	–

.

Es gilt in der Tat

$$-37 \cdot 30 + 11 \cdot 101 = -1110 + 1111 = 1.$$

Der Satz liefert die Lösungen

$$x \equiv -37 \bmod 101.$$

Mit $-37 \equiv 64 \bmod 101$ schreiben wir die Lösungen in der Form

$$x \equiv 64 \bmod 101.$$

Wir führen wieder eine Proberechnung aus:

$$30 \cdot 64 = 1920 = 19 \cdot 101 + 1 \equiv 1 \bmod 101.$$

Der chinesische Restsatz

Jetzt wollen wir ein Verfahren vorstellen, mit dem ein System von Kongruenzen gelöst werden kann. Zu gegebenen ganzen Zahlen $a, b, c, d \in \mathbb{Z}$ und $m, n \geq 1$ suchen wir eine ganze Zahl x mit

$$\begin{aligned} c \cdot x &\equiv a \bmod m \\ d \cdot x &\equiv b \bmod n. \end{aligned} \tag{I.7}$$

Nach Satz I.6.11, i), sind die Beziehungen

$$\mathrm{ggT}(c, m) | a \quad \text{und} \quad \mathrm{ggT}(d, n) | b$$

notwendig für die Lösbarkeit von (I.7). Wir setzen diese Beziehungen voraus. Dann sagt uns Satz I.6.11, ii), dass wir $c = 1 = d$ annehmen dürfen. Daher betrachten wir ein System von Kongruenzen der Form

$$\begin{aligned} x &\equiv a \bmod m \\ x &\equiv b \bmod n \end{aligned} \tag{I.8}$$

mit $a, b \in \mathbb{Z}$.

I.6.13 Beobachtung. *Es sei* $d := \mathrm{ggT}(m, n)$. *Dann folgt*

$$a \equiv b \bmod d$$

aus den Kongruenzen (I.8).

Beweis. Wir wenden Lemma I.6.10, i), an:

$$\begin{aligned} x \equiv a \bmod m &\implies x \equiv a \bmod d \\ x \equiv b \bmod n &\implies x \equiv b \bmod d. \end{aligned}$$

Die beiden Kongruenzen auf der rechten Seite zeigen wegen der Transitivität von „$\equiv \bmod d$“ (Lemma I.6.3), dass $a \equiv b \bmod d$. □

Es seien $y, z \in \mathbb{Z}$ ganze Zahlen mit

$$y \cdot m + z \cdot n = d.$$

Wir folgern

$$\frac{a-b}{d} \cdot y \cdot m + \frac{a-b}{d} \cdot z \cdot n = a - b$$

und damit

$$a - \frac{a-b}{d} \cdot y \cdot m = b + \frac{a-b}{d} \cdot z \cdot n.$$

Die ganze Zahl

$$x := a - \frac{a-b}{d} \cdot y \cdot m$$

löst (I.8).

I.6.14 Chinesischer Restsatz. i) *Das System* (I.8) *ist genau dann lösbar, wenn* $a \equiv b \bmod d$.

ii) *Falls* $a \equiv b \bmod d$*, dann ist* (I.8) *äquivalent zu*

$$x \equiv a - \frac{a-b}{d} \cdot y \cdot m \bmod \frac{m \cdot n}{d}. \tag{I.9}$$

Beweis. i) Dieser Teil folgt aus Beobachtung I.6.13 und den anschließenden Rechnungen.

ii) Wir setzen

$$x_0 := a - \frac{a-b}{d} \cdot y \cdot m.$$

Es wurde bereits überprüft, dass $x_0 \equiv a \bmod m$ und $x_0 \equiv b \bmod n$. Es gilt auch

$$\frac{m \cdot n}{d} \equiv 0 \bmod m \quad \text{und} \quad \frac{m \cdot n}{d} \equiv 0 \bmod n.$$

Damit ist auch $x_0 + k \cdot (m \cdot n)/d$ eine Lösung von (I.8), $k \in \mathbb{Z}$.

Es bleibt zu zeigen, dass jede Lösung von (I.8) von der in (I.9) angegebenen Form ist. Sei dazu x eine Lösung von (I.8). Wir schließen

$$x - x_0 \equiv 0 \bmod m \quad \text{und} \quad x - x_0 \equiv 0 \bmod n.$$

Lemma I.4.13 impliziert

$$\mathrm{kgV}(m,n) | (x - x_0).$$

Nach Satz I.4.14 haben wir

$$\mathrm{kgV}(m,n) = \frac{m \cdot n}{\mathrm{ggT}(m,n)} = \frac{m \cdot n}{d}.$$

Also finden wir die behauptete Kongruenz $x \equiv x_0 \bmod (m \cdot n/d)$. □

I.6.15 Bemerkung. Induktiv kann man jetzt Kongruenzsysteme der Form

$$c_i \cdot x \equiv a_i \bmod m_i, \quad i = 1, ..., n,$$

behandeln.

I.6.16 Beispiel. In Sun Tsus „Handbuch der Arithmetik“[9] (vermutlich zwischen 280 und 473 entstanden) wird gefordert, die Kongruenzen

$$\begin{aligned} x &\equiv 2 \bmod 3 \\ x &\equiv 3 \bmod 5 \\ x &\equiv 2 \bmod 7 \end{aligned}$$

zu lösen.

Wegen $1 = 3 \cdot 2 - 1 \cdot 5$ sind die Kongruenzen $x \equiv 2 \bmod 3$ und $x \equiv 3 \bmod 5$ äquivalent zu der Kongruenz

$$x \equiv 2 - 2 \cdot 3 \cdot (2 - 3) = 8 \bmod 15.$$

[9] Dieses Buch ist für den Namen „Chinesischer Restsatz“ verantwortlich, obwohl der Satz nicht wie oben formuliert wird sondern nur in Beispielaufgaben wie der folgenden auftritt.

Weiter gilt $1 = 15 - 2 \cdot 7$. Daher sind die Kongruenzen $x \equiv 8 \bmod 15$ und $x \equiv 2 \bmod 7$ äquivalent zu

$$x \equiv 8 - 15 \cdot (8 - 2) = -82 \equiv 23 \bmod 105.$$

In der Tat gilt

$$23 \equiv 2 \bmod 3, \quad 23 \equiv 3 \bmod 5 \quad \text{und} \quad 23 \equiv 2 \bmod 7.$$

I.6.17 Aufgabe. Von einem Bienenvolk sind folgende Daten bekannt: Es hat zwischen 200 und 250 Mitglieder. Stellen sich die Bienen in 7er-Reihen auf, dann bleibt eine Biene alleine. Wenn sie sich in 5er-Reihen aufstellen, dann bleiben drei übrig. Wieviele Mitglieder hat das Bienenvolk?

II

Gruppentheorie

Wir legen nun die Grundlagen für die Gruppentheorie. Gruppen sind Teil der mathematischen Formalisierung des Konzepts der Symmetrie. Symmetrie gehört bis zu einem gewissen Grad unserer Alltagserfahrung an, z.B. in Form eines sich wiederholenden Tapetenmusters oder in der Architektur. Der Begriff der Gruppe ist in der Mengenlehre verankert. Dadurch ergibt sich ein reizvolles Zusammenspiel zwischen Anschauung und Abstraktion. Wir können etwa ein dreidimensionales Objekt, z.B. ein Polyeder, erkunden und somit seine Symmetriegruppe beschreiben. Auf der anderen Seite können wir gruppentheoretische Aussagen an konkreten Beispielen veranschaulichen. Diese beiden Vorgehensweisen werden wir unter anderem bei den Platonischen Körpern, die die Menschheit schon seit mehr als 4000 Jahren begleiten,[1] kennenlernen. Die flexibelste Verkörperung des Symmetriegedankens ist das Konzept der Gruppenwirkung. Eine Gruppe G wird mit der Symmetriegruppe einer Menge M vermöge eines Homomorphismus in Verbindung gesetzt. Etwaige Strukturen der Menge M, die von der Gruppenwirkung unberührt bleiben, können verwendet werden, um die Gruppe G zu untersuchen. So liefert die Theorie der Jordanschen Normalform aus der Linearen Algebra eine Beschreibung der Konjugationsklassen in der allgemeinen linearen Gruppe $\mathrm{GL}_n(\mathbb{C})$. Umgekehrt zerfällt die Menge M unter der Wirkung von G in eine disjunkte Vereinigung von G-Bahnen. Im Fall, dass G und M endlich sind, wird diese Situation durch eine Reihe von Sätzen beschrieben, die sich um den Satz von Lagrange gruppieren. Darunter ist eine Formel, die die Berechnung der Anzahl der G-Bahnen in M ermöglicht. Diese Sätze lassen sich in praxisnahen Situationen einsetzen, um Konfigurationen einer bestimmten Art, z.B. Moleküle, die sich aus vorgegebenen Atomen zusammensetzen, zu zählen. Darüber hinaus werden wir mit ihnen tiefer liegende Aussagen über die Struktur von Gruppen gewinnen. Mit diesen Aussagen werden wir die endlichen Untergruppen von $\mathrm{O}(2)$ und $\mathrm{SO}(3)$ sowie endliche Gruppen bis zur Ordnung 14 klassifizieren. Unter der Voraussetzung, dass die betrachteten Gruppen abelsch sind, lassen sich allgemeinere Aussagen gewinnen. Wir beschließen das Kapitel mit dem Hauptsatz über endlich erzeugte abelsche Gruppen. Dieser Satz illustriert unter anderem den Übergang von der Linearen Algebra zur Gruppentheorie. Dieses Kapitel

[1] `http://en.wikipedia.org/wiki/Carved_Stone_Balls`

beruht größtenteils auf den Büchern [2] und [11].

II.1 Definition einer Gruppe und erste Beispiele

Wir beginnen mit der Definition der Hauptakteurin dieses Kapitels.

II.1.1 Definition. Eine *Gruppe* ist ein Paar $(G, \cdot)$, das aus einer Menge G und einer Abbildung

$$\begin{aligned} \cdot\colon G \times G &\longrightarrow G \\ (g,h) &\longmapsto g \cdot h \end{aligned}$$

besteht und folgende Eigenschaften aufweist:

a) Das *Assoziativgesetz* ist erfüllt, d.h.

$$\forall a,b,c \in G: \quad (a \cdot b) \cdot c = a \cdot (b \cdot c).$$

b) Es gibt ein *neutrales Element*, d.h.

$$\exists e \in G \forall g \in G: \quad e \cdot g = g = g \cdot e.$$

c) Zu jedem Element gibt es ein *inverses Element*, d.h.

$$\forall g \in G \exists h \in G: \quad g \cdot h = e = h \cdot g.$$

Vereinbarung. Wir schreiben meist nur G statt $(G, \cdot)$ für eine Gruppe.

In ein System von Axiomen schreibt man so wenig Forderungen wie möglich hinein (vgl. Aufgabe II.1.3), damit der Nachweis, dass eine gewisse Struktur diese Forderungen erfüllt, möglichst einfach wird. Es gibt oft — wie im vorliegenden Fall — einige direkte Konsequenzen aus den Axiomen, die für den Umgang mit den entsprechenden Strukturen eine grundlegende Bedeutung haben. Wir halten im Folgenden zwei dieser Konsequenzen aus den Gruppenaxiomen fest.

II.1.2 Beobachtungen. i) *In einer Gruppe gibt es* ***genau ein*** *neutrales Element.*

ii) *Zu jedem Gruppenelement $g \in G$ existiert* ***genau ein*** *inverses Element.*

Bezeichnung. Auf Grund dieser Beobachtung sprechen wir für $g \in G$ von **dem** inversen Element und notieren es als g^{-1}.

Beweis. i) Seien $e, e' \in G$ zwei neutrale Elemente. Dann folgt $e = e \cdot e' = e'$. Dabei wurde in der ersten Gleichung die Neutralität von e' benutzt und in der zweiten die von e.

ii) Seien $g, h, h' \in G$ Gruppenelemente, so dass $h' \cdot g = h \cdot g = e = g \cdot h = g \cdot h'$. Es folgt $h' = h' \cdot e = h' \cdot (g \cdot h) = (h' \cdot g) \cdot h = e \cdot h = h$. □

II.1.3 Aufgabe (Eine andere Definition des Gruppenbegriffs). Es seien G eine Menge und $\cdot\colon G \times G \longrightarrow G$, $(g,h) \longmapsto g \cdot h$, eine Verknüpfung mit folgenden Eigenschaften:

- ⋆ Das Assoziativgesetz ist erfüllt.
- ⋆ Es gibt ein *linksneutrales Element* $e \in G$, d.h. für jedes $g \in G$ hat man $e \cdot g = g$.

⋆ Zu jedem Element $g \in G$ existiert ein *linksinverses Element* $g' \in G$, d.h. $g' \cdot g = e$.

In dieser Aufgabe soll gezeigt werden, dass $(G, \cdot)$ eine Gruppe ist.

a) Es seien $g \in G$ und $g' \in G$ ein Element mit $g' \cdot g = e$. Zeigen Sie $g \cdot g' = e$.

b) Beweisen Sie, dass $g \cdot e = g$ für alle $g \in G$ gilt.

Die folgende Definition enthält eine wichtige und angenehme Zusatzeigenschaft, die Gruppen haben können oder auch nicht.

II.1.4 Definition. Eine Gruppe G heißt *kommutativ* oder *abelsch*,[2] wenn

$$\forall g, h \in G : \quad g \cdot h = h \cdot g.$$

II.1.5 Aufgabe (Abelsche Gruppen). a) Es sei $g \in G$ eine Gruppe, so dass $g^2 = e$ für alle $g \in G$ gilt. Weisen Sie nach, dass G abelsch ist. Geben Sie für jedes $k \geq 1$ eine Gruppe G mit 2^k Elementen an, in der $g^2 = e$ für jedes Gruppenelement $g \in G$ gilt.[3]

b) Es sei G eine **endliche** abelsche Gruppe. Zeigen Sie, dass

$$\prod_{g \in G} g^2 = e.$$

Motivation und Beispiele

Wir sind mit den Grundrechenarten in den ganzen, rationalen und reellen Zahlen vertraut. Die Gruppenaxiome formulieren **einige** der Eigenschaften, die wir dabei verwenden. Die ersten Beispiele der folgenden Liste präzisieren diese Behauptung.

• $(\mathbb{Z}, +)$ ist eine Gruppe:

⋆ Das neutrale Element ist 0.

⋆ Das inverse Element zu $l \in \mathbb{Z}$ ist $-l$.

⋆ Diese Gruppe ist abelsch.

• $(\mathbb{N}, +)$ ist keine Gruppe. Zwar gilt das Assoziativgesetz und ist die Null ein neutrales Element, aber außer der Null besitzt kein Element ein inverses Element. (Um diesen „Defekt“ zu beheben, wurden die ganzen Zahlen eingeführt (s. [16], Abschnitt 1.4).)

• $(\mathbb{Z} \setminus \{0\}, \cdot)$ ist ebenfalls keine Gruppe. Auch hier gilt das Assoziativgesetz und ist mit der 1 ein neutrales Element vorhanden, aber nur die Zahlen ± 1 haben ein inverses Element. (In diesem Fall veranlasst das Fehlen der inversen Elemente die Konstruktion der rationalen Zahlen ([16], Abschnitt 1.5).)

• Es sei k ein **Körper**, z.B. $k = \mathbb{Q}, \mathbb{R}, \mathbb{C}$.

⋆ $(k, +)$ ist eine abelsche Gruppe.

⋆ $(k \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe.

⋆ $(k, \cdot)$ ist keine Gruppe. Das liegt daran, dass 0 kein inverses Element zulässt: $\forall x \in k : x \cdot 0 = 0 \cdot x = 0 \neq 1$.

[2]

[3] In Folgerung II.7.5 werden wir sehen, dass eine endliche Gruppe G, in der es ein Element $g \neq e$ mit $g^2 = e$ gibt, eine gerade Anzahl von Elementen besitzt.

Wir fahren mit einem Beispiel fort, das den Leserinnen und Lesern aus der linearen Algebra bekannt ist und ein fundamentales Beispiel einer **nichtabelschen** Gruppe darstellt.

• **Die allgemeine lineare Gruppe.** Es seien k ein Körper und $n \geq 1$. Mit $M_n(k)$ bezeichnen wir den Vektorraum der Matrizen vom Format $n \times n$ ([20], §14, Bemerkung 1; [5], Beispiel 1.4.1, b). Das Matrixprodukt ([20], §15, Satz 1; [5], Abschnitt 2.5.2) zweier Matrizen vom Format $n \times n$ existiert und ist wieder vom Format $n \times n$, so dass eine Multiplikation auf $M_n(k)$ erklärt ist. Sie ist assoziativ ([20], §15, Bemerkung 1; [5], Rechenregeln 2.5.4, 3). Damit führt man

$$\begin{aligned} \mathrm{GL}_n(k) &:= \{\, m \in M_n(k) \mid \exists m' \in M_n(k) : m' \cdot m = \mathbb{E}_n \,\} \\ &= \{\, m \in M_n(k) \mid \mathrm{Det}(m) \neq 0 \,\} \end{aligned}$$

ein.

- ⋆ Das neutrale Element ist die Einheitsmatrix $\mathbb{E}_n$.
- ⋆ Das inverse Element zu einer Matrix $m \in \mathrm{GL}_n(k)$ ist die inverse Matrix m^{-1}.

Wiederum ist $M_n(k)$ mit der Matrixmultiplikation keine Gruppe, weil viele Matrizen, darunter die Nullmatrix, keine inversen Elemente besitzen. Das Assoziativgesetz ist allerdings erfüllt, und $\mathbb{E}_n$ ist ein neutrales Element.

Es gilt $\mathrm{GL}_1(k) = (k \setminus \{0\}, \cdot)$, und dies ist eine abelsche Gruppe. In $\mathrm{GL}_2(k)$ berechnen wir

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

Da immer $2 \neq 1$ gilt, ist $\mathrm{GL}_2(k)$ nicht abelsch.

Für $n \geq 3$ zeigt die obige Rechnung, dass die Matrizen

$$A := \left(\begin{array}{cc|c} 1 & 1 & 0 \\ 0 & 1 & \\ \hline 0 & & \mathbb{E}_{n-2} \end{array}\right) \quad \text{und} \quad B := \left(\begin{array}{cc|c} 1 & 0 & 0 \\ 1 & 1 & \\ \hline 0 & & \mathbb{E}_{n-2} \end{array}\right)$$

nicht miteinander kommutieren. Die allgemeine lineare Gruppe $\mathrm{GL}_n(k)$ ist also genau dann abelsch, wenn $n = 1$.

Die Mathematik wird heutzutage in der Sprache der **Mengen** und **Abbildungen** formuliert (s. [16], Abschnitt 1.2, für eine kurze Einführung). Das folgende Beispiel zeigt, dass man damit zwangsläufig sehr schnell auf die Definition einer Gruppe stößt.

• Es seien M eine **nichtleere** Menge und

$$S(M) := \{\, f \colon M \longrightarrow M \mid f \text{ ist bijektiv} \,\}.$$

- ⋆ Die Multiplikation ist die Verknüpfung „$\circ$“ von Abbildungen. Für $f, g \colon M \longrightarrow M$ ist dabei

$$\begin{aligned} f \circ g \colon M &\longrightarrow M \\ x &\longmapsto f(g(x)). \end{aligned}$$

- ⋆ Da zwei Abbildungen von M nach M genau dann gleich sind, wenn sie auf jedem Element von M denselben Wert annehmen, zeigt die folgende Rechnung die Gültigkeit des Assoziativgesetzes. Es seien $f, g, h \in S(M)$ und $x \in M$. Dann haben wir

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

- ⋆ Das neutrale Element ist die Identität $\mathrm{id}_M \colon M \longrightarrow M$, $x \longmapsto x$.

- ⋆ Zur Definition der inversen Elemente erinnere man sich daran, dass die Bijektivität von f bedeutet:[4]

$$\forall y \in M \exists! x \in M : \quad f(x) = y.$$

  Damit erklären wir

$$\begin{array}{rccc} f^{-1} \colon & M & \longrightarrow & M \\ & y & \longmapsto & x. \end{array}$$

  Die *inverse Abbildung* f^{-1} erfüllt $f^{-1} \circ f = \mathrm{id}_M = f \circ f^{-1}$.

Wir untersuchen nun, ob die Gruppe M abelsch ist oder nicht. Wenn M nur ein Element enthält, dann haben wir $S(M) = \{\mathrm{id}_M\}$ und damit eine abelsche Gruppe.

Die Menge M enthalte genau zwei Elemente. Wir schreiben $M = \{1, 2\}$. Damit gilt

$$S(M) = \left\{ \mathrm{id}_M, \quad \begin{array}{rccc} \tau \colon & M & \longrightarrow & M \\ & 1 & \longmapsto & 2 \\ & 2 & \longmapsto & 1 \end{array} \right\}.$$

Dies ist offenbar eine abelsche Gruppe,

Jetzt gebe es mindestens drei Elemente in M. Wir nehmen $\{1, 2, 3\} \subset M$ an und definieren

$$\begin{array}{rccc} f_1 \colon & M & \longrightarrow & M \\ & 1 & \longmapsto & 2 \\ & 2 & \longmapsto & 1 \\ & x & \longmapsto & x, \quad x \notin \{1, 2\} \end{array} \qquad \text{und} \qquad \begin{array}{rccc} f_2 \colon & M & \longrightarrow & M \\ & 2 & \longmapsto & 3 \\ & 3 & \longmapsto & 2 \\ & x & \longmapsto & x, \quad x \notin \{2, 3\} \end{array}$$

und berechnen

$$(f_1 \circ f_2)(1) = f_1(f_2(1)) = f_1(1) = 2 \quad \text{und} \quad (f_2 \circ f_1)(1) = f_2(f_1(1)) = f_2(2) = 3.$$

Wir nennen $S(M)$ die *symmetrische Gruppe* von M. Insbesondere setzt man $S_n := S(M)$ für $n \geq 1$ und $M := \{1, ..., n\}$. Wir haben nachgewiesen, dass S_n genau dann abelsch ist, wenn $n = 1$ oder $n = 2$. Ein Element von S_n wird als *Permutation* bezeichnet.

Da die Mathematik in der Sprache der Mengen und Abbildungen formuliert wird, werden mathematische Objekte als Mengen mit gewissen Zusatzstrukturen erklärt. Jedes mathematische Objekt erhält damit seine **Symmetriegruppe**, nämlich die Gruppe der

[4] Das Symbol „$\exists!$“ ist „Es gibt genau ein“ zu lesen.

bijektiven Selbstabbildungen der zugrundeliegenden Menge, die **mit den Zusatzstrukturen verträglich** sind. Als Beispiel betrachten wir den ***k*-Vektorraum** k^n. Die Zusatzstrukturen sind die **Addition von Vektoren** und die **Skalarmultiplikation**. Die Abbildungen, die mit diesen Zusatzstrukturen verträglich sind, sind die **linearen Abbildungen**. Die Symmetriegruppe des k^n **als *k*-Vektorraum** ist folglich

$$\{ f\colon k^n \longrightarrow k^n \mid f \text{ ist bijektiv und linear} \},$$

also die allgemeine lineare Gruppe $\mathrm{GL}_n(k)$. Wir besprechen nun weitere Beispiele unter den genannten Gesichtspunkten.

• **Die orthogonale und die spezielle orthogonale Gruppe.** Es seien k ein Körper und $n \geq 1$. Wir betrachten folgende Zusatzstrukturen auf k^n:

- ⋆ die k-Vektorraumstruktur,
- ⋆ das **Standardskalarprodukt** ([20], §41; [5], Abschnitt 5.1.1)

$$\begin{array}{rcl} \langle \cdot, \cdot \rangle\colon k^n \times k^n & \longrightarrow & k \\ (v = (v_1, ..., v_n)^t, w = (w_1, ..., w_n)^t) & \longmapsto & v^t \cdot w = \displaystyle\sum_{i=1}^{n} v_i \cdot w_i. \end{array}$$

Die zugehörige Symmetriegruppe ist die *orthogonale Gruppe*

$$\mathrm{O}_n(k) = \left\{ f\colon k^n \longrightarrow k^n \;\middle|\; \begin{array}{ll} \star & f \text{ ist bijektiv} \\ \star & f \text{ ist linear} \\ \star & \forall v, w \in k^n : \langle v, w \rangle = \langle f(v), f(w) \rangle \end{array} \right\}.$$

Es seien $f\colon k^n \longrightarrow k^n$ eine lineare Abbildung und $m \in M_n(k)$ die zugehörige $(n \times n)$-Matrix. Dann finden wir für $v, w \in k^n$, dass

$$\langle f(v), f(w) \rangle = \langle m \cdot v, m \cdot w \rangle = (m \cdot v)^t \cdot (m \cdot w) = v^t \cdot (m^t \cdot m) \cdot w.$$

Wenn für alle $v, w \in k^n$ die Gleichung $\langle v, w \rangle = \langle f(v), f(w) \rangle$ gilt, dann finden wir speziell für $i, j \in \{ 1, ..., n \}$

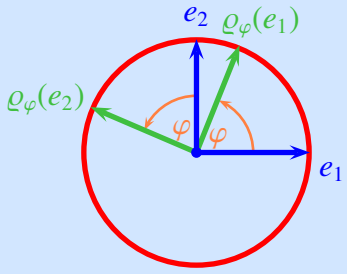
$$e_i \cdot (m^t \cdot m) \cdot e_j = \delta_{ij}.$$

Die Bedingung „$\forall v, w \in k^n : \langle v, w \rangle = \langle f(v), f(w) \rangle$“ ist also äquivalent zu $m^t \cdot m = \mathbb{E}_n$. Damit erhalten wir die alternative Beschreibung

$$\mathrm{O}_n(k) = \{ m \in \mathrm{GL}_n(k) \mid m^t \cdot m = \mathbb{E}_n \}$$

der orthogonalen Gruppe.

$\mathrm{O}_2(\mathbb{R})$. Zunächst listen wir einige spezielle Elemente in $\mathrm{O}_2(\mathbb{R})$ auf. Wir beginnen mit **Drehungen**. Es sei $\varphi \in \mathbb{R}$ ein **Winkel**. Die Drehung ϱ_φ (im mathematisch positiven Sinne) um den Winkel φ ist eine orthogonale Abbildung.



Für diese Abbildung gilt:

$$\text{Bild von } \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \cos(\varphi) \\ \sin(\varphi) \end{pmatrix} \quad \text{und} \quad \text{Bild von } \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} -\sin(\varphi) \\ \cos(\varphi) \end{pmatrix}.$$

Deshalb ist die zugehörige Abbildungsmatrix

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

Zur Probe berechnen wir (unter Berücksichtigung von [16], Folgerung 4.8.1)

$$\varrho_\varphi^t \cdot \varrho_\varphi = \begin{pmatrix} \cos(\varphi) & \sin(\varphi) \\ -\sin(\varphi) & \cos(\varphi) \end{pmatrix} \cdot \begin{pmatrix} \cos(\varphi) & -\sin(\varphi) \\ \sin(\varphi) & \cos(\varphi) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Neben den Drehungen betrachten wir **Spiegelungen**. Dazu geben wir uns wieder einen Winkel $\varphi \in \mathbb{R}$ vor. Die Spiegelung an der Achse, die mit der x-Achse den Winkel $\varphi/2$ einschließt, ist ebenfalls eine orthogonale Matrix. Es sei $\sigma_{\varphi/2}$ die zugehörige (2×2)-Matrix. Wir haben die Gleichung[5]

$$\sigma_{\varphi/2} = \varrho_{\varphi/2} \circ \sigma_0 \circ \varrho_{-\varphi/2}.$$

Mit

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

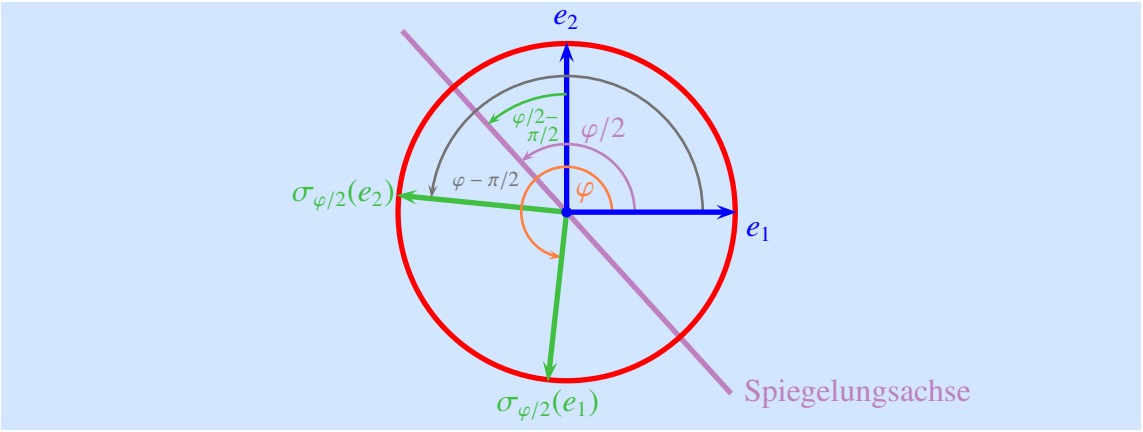
lautet diese Gleichung

$$\begin{aligned}
\sigma_{\varphi/2} &= \begin{pmatrix} \cos\left(\frac{\varphi}{2}\right) & -\sin\left(\frac{\varphi}{2}\right) \\ \sin\left(\frac{\varphi}{2}\right) & \cos\left(\frac{\varphi}{2}\right) \end{pmatrix} \cdot \begin{pmatrix} \cos\left(-\frac{\varphi}{2}\right) & -\sin\left(-\frac{\varphi}{2}\right) \\ -\sin\left(-\frac{\varphi}{2}\right) & -\cos\left(-\frac{\varphi}{2}\right) \end{pmatrix} \\
&= \begin{pmatrix} \cos\left(\frac{\varphi}{2}\right) & -\sin\left(\frac{\varphi}{2}\right) \\ \sin\left(\frac{\varphi}{2}\right) & \cos\left(\frac{\varphi}{2}\right) \end{pmatrix} \cdot \begin{pmatrix} \cos\left(\frac{\varphi}{2}\right) & \sin\left(\frac{\varphi}{2}\right) \\ \sin\left(\frac{\varphi}{2}\right) & -\cos\left(\frac{\varphi}{2}\right) \end{pmatrix} \\
&= \begin{pmatrix} \cos^2\left(\frac{\varphi}{2}\right) - \sin^2\left(\frac{\varphi}{2}\right) & 2 \cdot \cos\left(\frac{\varphi}{2}\right) \cdot \sin\left(\frac{\varphi}{2}\right) \\ 2 \cdot \cos\left(\frac{\varphi}{2}\right) \cdot \sin\left(\frac{\varphi}{2}\right) & \sin^2\left(\frac{\varphi}{2}\right) - \cos^2\left(\frac{\varphi}{2}\right) \end{pmatrix} \\
&= \begin{pmatrix} \cos(\varphi) & \sin(\varphi) \\ \sin(\varphi) & -\cos(\varphi) \end{pmatrix}.
\end{aligned}$$

Bei der letzten Umformung wurden die Additionstheoreme für Sinus und Kosinus ([16], Satz 4.8.8) verwandt.

Man kann die Matrix $\sigma_{\varphi/2}$ auch anhand der Skizze

[5] Diese Gleichung besagt, dass die Spiegelung an der betrachteten Achse erhalten werden kann, indem man zunächst um den Winkel $-\varphi/2$ dreht, so dass die Spiegelungsachse auf der x-Achse zu liegen kommt, dann an der x-Achse spiegelt und schließlich um den Winkel $\varphi/2$ dreht.



bestimmen. So findet man (wieder mit [16], Satz 4.8.8)

$$\sigma_{\varphi/2} = \begin{pmatrix} \cos(\varphi) & \cos\left(\varphi - \frac{\pi}{2}\right) \\ \sin(\varphi) & \sin\left(\varphi - \frac{\pi}{2}\right) \end{pmatrix} = \begin{pmatrix} \cos(\varphi) & \sin(\varphi) \\ \sin(\varphi) & -\cos(\varphi) \end{pmatrix}.$$

Wir haben bereits alle Elemente der orthogonalen Gruppe $\mathrm{O}_2(\mathbb{R})$ aufgelistet:

II.1.6 Satz. *Es sei $m \in \mathrm{O}_2(\mathbb{R})$ eine orthogonale Matrix. Dann existiert eine reelle Zahl $\varphi \in [0, 2\pi)$ mit*

$$m = \varrho_\varphi \quad \textit{oder} \quad m = \sigma_{\varphi/2}.$$

Beweis. Für die orthogonale Matrix m gilt

$$1 = \mathrm{Det}(\mathbb{E}_2) = \mathrm{Det}(m^t \cdot m) = \mathrm{Det}(m^t) \cdot \mathrm{Det}(m) = \mathrm{Det}(m)^2,$$

so dass

$$\mathrm{Det}(m) = \pm 1.$$

Da

$$\sigma_0 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \in \mathrm{O}_2(\mathbb{R}) \quad \text{und} \quad \mathrm{Det}\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} = -1,$$

können wir gegebenenfalls m durch $m \cdot \sigma_0$ ersetzen und deshalb $\mathrm{Det}(m) = 1$ voraussetzen.

Wir schreiben

$$m = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Mit $\mathrm{Det}(m) = a \cdot d - b \cdot c = 1$ folgt

$$m^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Weiter haben wir

$$m^{-1} = m^t = \begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

und somit

$$a = d \quad \text{und} \quad b = -c,$$

d.h.

$$m = \begin{pmatrix} a & -c \\ c & a \end{pmatrix} \quad \text{mit} \quad a^2 + c^2 = 1.$$

Der Vektor $(a, c)^t \in \mathbb{R}^2$ liegt auf dem Einheitskreis, und daher existiert eine reelle Zahl $\varphi \in [0, 2\pi)$ mit $a = \cos(\varphi)$ und $c = \sin(\varphi)$ (vgl. [17], Beispiel 3.2.4, iv). Das bedeutet

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

und zeigt die Behauptung. □

$O_3(\mathbb{R})$. Auch orthogonale (3×3)-Matrizen haben eine einfache Beschreibung:

II.1.7 Satz. *Es sei $m \in O_3(\mathbb{R})$ eine orthogonale Matrix. Dann existieren orthogonale Matrizen $g \in O_3(\mathbb{R})$ und $\widetilde{m} \in O_2(\mathbb{R})$, so dass*

$$g \cdot m \cdot g^t = \left(\begin{array}{c|c} \pm 1 & 0 \\ \hline 0 & \widetilde{m} \end{array}\right).$$

Beweis. Das charakteristische Polynom ([20], §34, Definition 3; [5], Abschnitt 4.2.2) von m hat Grad 3 und damit nach dem Zwischenwertsatz ([16], Folgerung 3.5.2) eine Nullstelle. Die Matrix m hat also einen Eigenvektor v. Aus $m \in O_3(\mathbb{R})$ folgert man:

- Für $\lambda \in \mathbb{R}$ mit $m \cdot v = \lambda \cdot v$ gilt wegen $\lambda^2 \cdot \langle v, v\rangle = \langle m \cdot v, m \cdot v\rangle = \langle v, v\rangle \neq 0$, dass $\lambda = \pm 1$.
- Das orthogonale Komplement $U := \langle v\rangle^\perp$ ist invariant unter Multiplikation mit m: $m \cdot U = U$.

Seien $v_1 := v/\|v\|$, $\|v\| := \sqrt{\langle v, v\rangle}$, und v_2, v_3 eine Basis von U mit $\|v_i\| = 1$, $i = 2, 3$, und $\langle v_2, v_3\rangle = 0$. Somit ist (v_1, v_2, v_3) eine Orthonormalbasis für $\mathbb{R}^3$. Es sei $h := (v_1|v_2|v_3)$ die Matrix mit den genannten Basisvektoren als Spalten. Mit $g := h^t$ ergibt sich die Behauptung des Satzes. □

II.1.8 Bemerkung. Falls $\mathrm{Det}(\widetilde{m}) = -1$ gilt, dann ist $\widetilde{m}$ eine Spiegelung. In diesem Fall kann man

$$\widetilde{m} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

erreichen.

Die Gruppe

$$SO_n(k) := \{\, m \in O_3(k) \,|\, \mathrm{Det}(m) = 1 \,\}$$

ist die *spezielle orthogonale Gruppe*. Die Zusatzstruktur, die zusätzlich festgehalten wird, ist eine **Orientierung** von k^n (vgl. [18], Definition 5.3.3). Satz II.1.7 sagt insbesondere aus, dass jede Matrix $m \in SO_3(\mathbb{R})$ eine Drehung um eine geeignete Achse im $\mathbb{R}^3$ beschreibt.

• **Symmetriegruppen.** Es sei $M \subset \mathbb{R}^n$ eine Teilmenge. Die *Symmetriegruppe* von M ist

$$O(M) := \{\, m \in O_n(\mathbb{R}) \,|\, m \cdot M = M \,\}$$

und die *spezielle Symmetriegruppe*

$$SO(M) := \{\, m \in SO_n(\mathbb{R}) \,|\, m \cdot M = M \,\}.$$

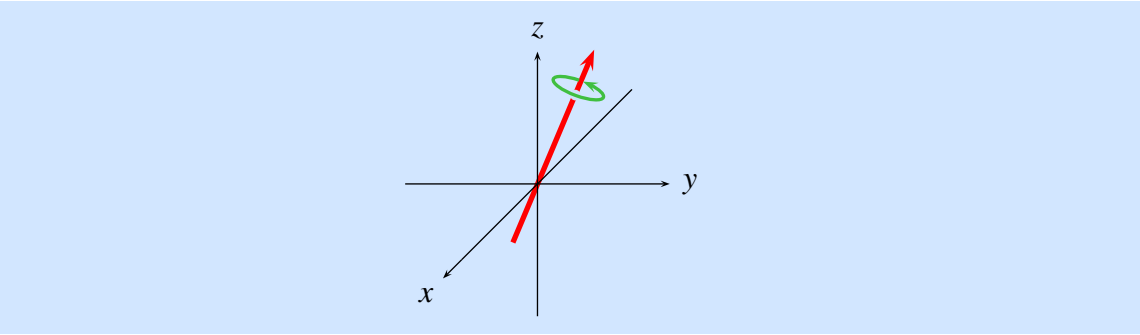


Abbildung II.1: Eine Drehung in $\mathbb{R}^3$

Bemerkung. Einen real existierendes Objekt $M \subset \mathbb{R}^3$ können wir verschieben, um eine beliebige Achse drehen oder durch Verknüpfungen solcher Operationen bewegen. Wenn M endliche Ausdehnung hat, dann gibt es keine Verschiebung, die M in sich überführt. Die Drehungen sind demnach diejenigen Symmetrien von M, die wir real erfahren können.

- ⋆ Als Multiplikation in $\mathrm{O}(M)$ bzw. $\mathrm{SO}(M)$ benutzen wir die Multiplikation in $\mathrm{O}_n(\mathbb{R})$ bzw. $\mathrm{SO}_n(\mathbb{R})$. Es ist demnach zu zeigen, dass für $m_1, m_2 \in \mathrm{O}(M)$ bzw. $\mathrm{SO}(M)$ auch das Produkt $m_1 \cdot m_2$ in $\mathrm{O}(M)$ bzw. $\mathrm{SO}(M)$ liegt. Dies folgt wegen

$$(m_1 \cdot m_2)(M) = m_1(m_2(M)) \overset{m_2(M)=M}{=} m_1(M) = M.$$

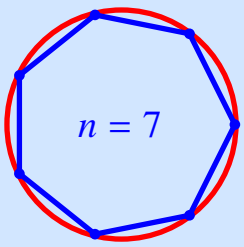
  Da das Produkt in $\mathrm{O}_n(\mathbb{R})$ bzw. $\mathrm{SO}_n(\mathbb{R})$ assoziativ ist, gilt das auch für das Produkt in $\mathrm{O}(M)$ bzw. $\mathrm{SO}(M)$.

- ⋆ Das neutrale Element ist $\mathbb{E}_n \in \mathrm{SO}(M) \subset \mathrm{O}(M)$.

- ⋆ Wenn m in $\mathrm{O}(M)$ bzw. $\mathrm{SO}(M)$ liegt, dann ist zu zeigen, dass dies auch für die inverse Matrix m^{-1} gilt, die zunächst in $\mathrm{O}_n(\mathbb{R})$ bzw. $\mathrm{SO}_n(\mathbb{R})$ existiert. Aus $M = m(M)$ folgt

$$m^{-1}(M) = m^{-1}(m(M)) = (m^{-1} \cdot m)(M) = M.$$

II.1.9 Beispiele. i) **Diedergruppen.** Es seien $n \geq 3$ und $M \subset \mathbb{R}^2$ das regelmäßige n-Eck mit Ecken auf dem Einheitskreis. Die Symmetriegruppe $D_n := \mathrm{O}(M)$ wird *Diedergruppe* genannt.



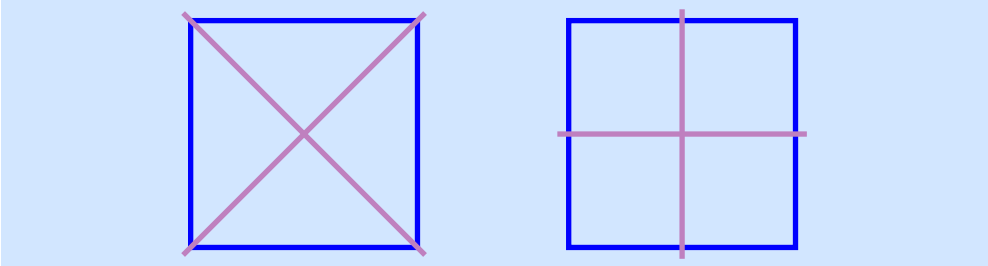
★ **Drehungen in D_n.** Dies sind die Elemente

$$\varrho_{2\pi k/n}, \quad k = 0, ..., n-1.$$

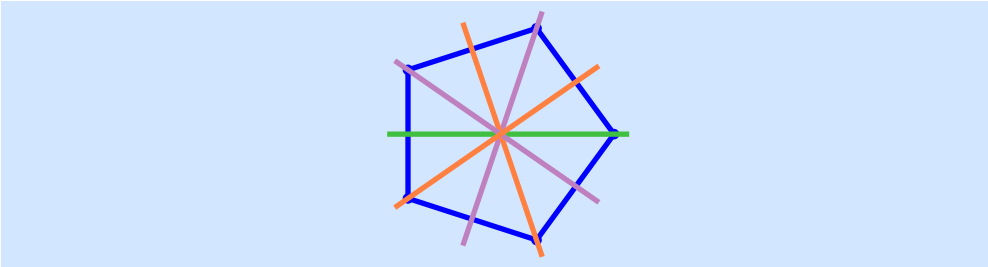
Es gibt also n solche Drehungen.

★ **Spiegelungen in D_n.** Hier müssen wir zwei Fälle unterscheiden:

– Wenn ***n* gerade** ist, dann gibt es $n/2$ Spiegelungen an Achsen, die durch gegenüberliegende Ecken laufen, und $n/2$ Spiegelungen, die durch die Mittelpunkte zweier gegenüberliegender Kanten verlaufen.



– Wenn ***n* ungerade** ist, dann gibt es n Spiegelungen an Achsen, die durch eine Ecke und den Mittelpunkt der gegenüberliegenden Kante verlaufen.



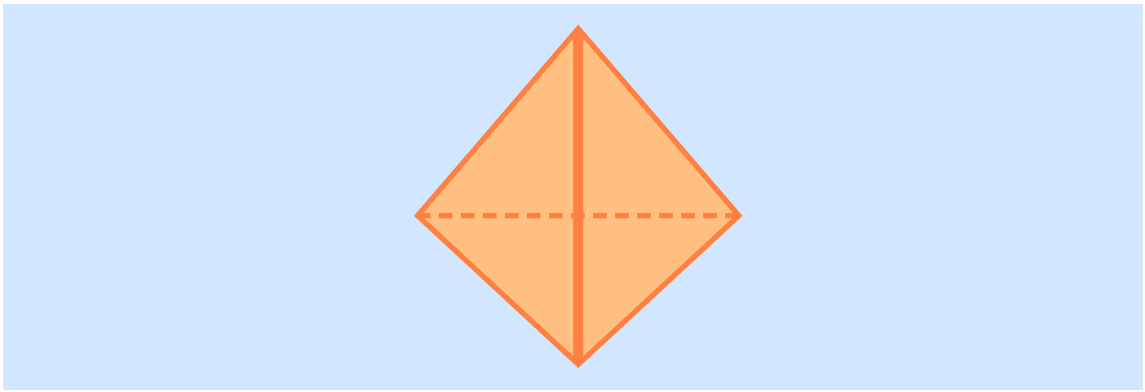
Damit haben wir insbesondere gezeigt:

Satz. *Die Diedergruppe D_n enthält genau $2n$ Elemente.*

ii) **Die Tetraedergruppe.** Wir untersuchen ein regelmäßiges Tetraeder $T \subset \mathbb{R}^3$ mit Mittelpunkt 0. Als Ecken von T können wir z.B.

$$P = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \quad Q = \begin{pmatrix} -1 \\ -1 \\ 1 \end{pmatrix}, \quad R = \begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix}, \quad S = \begin{pmatrix} -1 \\ 1 \\ -1 \end{pmatrix}$$

wählen.



Wir listen nun die verschiedenen Elemente in der speziellen Symmetriegruppe SO(T) auf:

- ⋆ Drehungen um den Winkel 0, $2\pi/3$ oder $4\pi/3$ an einer Achse durch eine Ecke und den Mittelpunkt der gegenüberliegenden Seite. Davon gibt es insgesamt neun Stück.
- ⋆ Drehungen um den Winkel π an einer Achse durch die Mittelpunkte zweier gegenüberliegender Kanten. Davon gibt es drei Stück.

Die spezielle Symmetriegruppe des Tetraeders umfasst also genau 12 Elemente.

II.1.10 Aufgabe (Die Tetraedergruppe). Es seien

$$P = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix}, \quad Q = \begin{pmatrix} -1 \\ -1 \\ 1 \end{pmatrix}, \quad R = \begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix}, \quad S = \begin{pmatrix} -1 \\ 1 \\ -1 \end{pmatrix}.$$

a) Berechnen Sie die Abstände $d(P,Q)$, $d(P,R)$, $d(P,S)$, $d(Q,R)$, $d(Q,S)$ und $d(R,S)$.[6] Schließen Sie, dass die angegebenen Punkte die Eckpunkte eines regulären Tetraeders T sind.

b) Geben Sie die Elemente der speziellen Symmetriegruppe SO(T) in Form von (3×3)-Matrizen an.

II.1.11 Aufgabe (Würfel, Okta- und Dodekaeder). a) Es sei $W \subset \mathbb{R}^3$ der Würfel mit den Eckpunkten

$$\begin{pmatrix} 1 \\ 1 \\ \pm 1 \end{pmatrix}, \quad \begin{pmatrix} -1 \\ 1 \\ \pm 1 \end{pmatrix}, \quad \begin{pmatrix} -1 \\ -1 \\ \pm 1 \end{pmatrix}, \quad \begin{pmatrix} 1 \\ -1 \\ \pm 1 \end{pmatrix}.$$

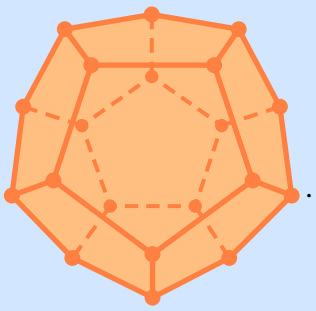
Bestimmen Sie die spezielle Symmetriegruppe SO(W).

b) Die Punkte

$$\begin{pmatrix} \pm 1 \\ 0 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 0 \\ \pm 1 \\ 0 \end{pmatrix}, \quad \begin{pmatrix} 0 \\ 0 \\ \pm 1 \end{pmatrix}$$

sind Eckpunkte eines Polyeders $O \subset \mathbb{R}^3$. Skizzieren Sie O. Bestimmen Sie die spezielle Symmetriegruppe SO(O). Vergleichen Sie SO(O) und SO(W). Was stellen Sie fest? Haben Sie eine Erklärung dafür?

c) Ein Dodekaeder $D \subset \mathbb{R}^3$ ist ein reguläres Polyeder, das von 12 regelmäßigen Fünfecken begrenzt wird:



[6] Hier ist d der euklidische Abstand ([17], Beispiel 1.2.4, i).

Beschreiben Sie die spezielle Symmetriegruppe SO(D).

• **Zyklische Gruppen.** Es seien $n \geq 1$ und $\mathbb{Z}_n = \{0, 1, ..., n-1\}$. Weiter sei

$$\begin{array}{rcl} \oplus : \mathbb{Z}_n \times \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \\ (i,j) & \longrightarrow & \begin{cases} i+j, & \text{falls } i+j \leq n-1 \\ i+j-n, & \text{falls } i+j \geq n \end{cases} \end{array} .$$

Dabei haben wir die Addition „+“ auf $\mathbb{Z}$ verwendet.

⋆ Man überprüft sofort, dass für $i, j, k \in \mathbb{Z}_n$

$$(i \oplus j) \oplus k = i \oplus (j \oplus k) = \begin{cases} i+j+k, & \text{falls } i+j+k \leq n-1 \\ i+j+k-n, & \text{falls } n \leq i+j+k \leq 2n-1 \\ i+j+k-2n, & \text{falls } 2n \leq i+j+k \end{cases}$$

gilt und somit das Assoziativgesetz[7] erfüllt ist.

⋆ Das neutrale Element ist 0.

⋆ Das inverse Element zu i ist $n-i$, $i = 0, ..., n-1$.

• **Eine Konstruktionsmethode.** Gegeben seien zwei Gruppen $(G, \cdot_G)$ und $(H, \cdot_H)$ mit neutralen Elementen e_G und e_H. Wir definieren auf $G \times H$ die folgende Multiplikation:

$$\begin{array}{rcl} \cdot : (G \times H) \times (G \times H) & \longrightarrow & G \times H \\ ((g_1, h_1), (g_2, h_2)) & \longmapsto & (g_1 \cdot_G g_2, h_1 \cdot_H h_2). \end{array}$$

⋆ Unter Verwendung der Assoziativgesetze in G und H ergibt sich das Assoziativgesetz in $G \times H$: Für $g_1, g_2, g_3 \in G$ und $h_1, h_2, h_3 \in H$ hat man

$$\begin{array}{rcl} (g_1, h_1) \cdot ((g_2, h_2) \cdot (g_3, h_3)) & = & (g_1, h_1) \cdot (g_2 \cdot_G g_3, h_2 \cdot_H h_3) \\ & = & (g_1 \cdot_G (g_2 \cdot_G g_3), h_1 \cdot_H (h_2 \cdot_H h_3)) \\ & = & ((g_1 \cdot_G g_2) \cdot_G g_3, (h_1 \cdot_H h_2) \cdot_H h_3) \\ & = & (g_1 \cdot_G g_2, h_1 \cdot_H h_2) \cdot (g_3, h_3) \\ & = & ((g_1, h_1) \cdot (g_2, h_2)) \cdot (g_3, h_3). \end{array}$$

⋆ Das neutrale Element ist $e = (e_G, e_H)$.

⋆ Das inverse Element zu $(g, h) \in G \times H$ ist (g^{-1}, h^{-1}). Dabei ist g^{-1} bzw. h^{-1} das zu g bzw. h inverse Element in G bzw. H.

Man nennt $G \times H$ das *direkte Produkt* der Gruppen G und H.

II.1.12 Aufgabe (Eine neue Multiplikation auf $\mathbb{R}$*).* Auf $\mathbb{R}$ wird folgende Verknüpfung definiert:

$$\begin{array}{rcl} \star : \mathbb{R} \times \mathbb{R} & \longrightarrow & \mathbb{R} \\ (a, b) & \longmapsto & a \cdot b + a + b. \end{array}$$

[7] Das Assoziativgesetz in $\mathbb{Z}_n$ folgt aus dem Assoziativgesetz in $\mathbb{Z}$. Die Beschreibung von $\mathbb{Z}_n$ als Faktorgruppe in Beispiel II.10.2, i), verdeutlicht das noch besser.

a) Zeigen Sie, dass $\star$ das Assoziativgesetz erfüllt und es ein neutrales Element gibt.

b) Welche Elemente in $\mathbb{R}$ besitzen bzgl. $\star$ keine Inversen? Geben Sie die kleinste Teilmenge $N \subset \mathbb{R}$ an, für die $(\mathbb{R} \setminus N, \star)$ eine Gruppe ist.

II.1.13 Aufgabe (Die entgegengesetzte Gruppe). Es seien $(G, \cdot)$ eine Gruppe und

$$\begin{array}{rcl} \star\colon G \times G & \longrightarrow & G \\ (g,h) & \longmapsto & h \cdot g. \end{array}$$

Zeigen Sie, dass $G^{\mathrm{op}} := (G, \star)$ eine Gruppe ist. Sie heißt die zu G *entgegengesetzte Gruppe*.

II.2 Die Verknüpfungstafel einer endlichen Gruppe

Es sei $G = \{ g_0 := e, g_1, ..., g_n \}$ eine endliche Gruppe. Wir legen folgende Tabelle an:

$\cdot$	e	g_1	$\cdots$	g_j	$\cdots$	g_n
e	$e \cdot e$	$e \cdot g_1$	$\cdots$	$e \cdot g_j$	$\cdots$	$e \cdot g_n$
g_1	$g_1 \cdot e$	$g_1 \cdot g_1$	$\cdots$	$g_1 \cdot g_j$	$\cdots$	$g_1 \cdot g_n$
$\vdots$	$\vdots$	$\vdots$		$\vdots$		$\vdots$
g_i	$g_i \cdot e$	$g_i \cdot g_1$	$\cdots$	$g_i \cdot g_j$	$\cdots$	$g_i \cdot g_n$
$\vdots$	$\vdots$	$\vdots$		$\vdots$		$\vdots$
g_n	$g_n \cdot e$	$g_n \cdot g_1$	$\cdots$	$g_n \cdot g_j$	$\cdots$	$g_n \cdot g_n$

Der Eintrag in der $(i+1)$-ten Zeile und $(j+1)$-ten Spalte ist das Produkt $g_i \cdot g_j$, $i, j = 0, ..., n$.

Aus dem Axiom für das neutrale Element folgt, dass

$$e \quad g_1 \quad \cdots \quad g_n$$

die erste Zeile und

$$\begin{matrix} e \\ g_1 \\ \vdots \\ g_n \end{matrix}$$

die erste Spalte dieser Tabelle ist. Eine weitere wichtige Eigenschaft wird sich aus dem folgenden Resultat ergeben.

II.2.1 Lemma. *Es seien G eine (**nicht notwendigerweise endliche**) Gruppe und $g \in G$. Dann sind die Abbildungen*

$$\begin{array}{rcl} \lambda_g\colon G & \longrightarrow & G \\ h & \longmapsto & g \cdot h \end{array}$$

und

$$\begin{array}{rcl} \varrho_g\colon G & \longrightarrow & G \\ h & \longmapsto & h \cdot g \end{array}$$

bijektiv.

Beweis. Wir beweisen das Lemma für die Abbildung λ_g, $g \in G$. Für die **Injektivität** seien $h_1, h_2 \in G$ zwei Elemente, so dass

$$g \cdot h_1 = g \cdot h_2.$$

Multiplikation mit g^{-1} liefert

$$h_1 = e \cdot h_1 = (g^{-1} \cdot g) \cdot h_1 = g^{-1} \cdot (g \cdot h_1) = g^{-1} \cdot (g \cdot h_2) = (g^{-1} \cdot g) \cdot h_2 = e \cdot h_2 = h_2.$$

Für die **Surjektivität** sei $h \in G$. Wir definieren $h' := g^{-1} \cdot h$ und finden

$$\lambda_g(h') = g \cdot (g^{-1} \cdot h) = (g \cdot g^{-1}) \cdot h = e \cdot h = h.$$

Die Bijektivität von λ_g ist somit nachgewiesen. □

II.2.2 Bemerkung. Für jedes Element $g \in G \setminus \{e\}$ gilt $g \cdot g = \lambda_g(g) \neq \lambda_g(e) = g$.

Das Lemma impliziert, dass in der Verknüpfungstafel einer endlichen Gruppe jedes Gruppenelement in jeder Zeile und in jeder Spalte genau einmal vorkommt.

Für eine gegebene endliche Menge $G = \{ g_0, g_1, ..., g_n \}$ können wir im Prinzip alle möglichen Gruppenstrukturen auf G mit neutralem Element g_0 bestimmen. Dazu stellen wir alle möglichen Verknüpfungstafeln auf, die den bereits gefundenen Regeln genügen, und sondern diejenigen aus, in denen das Assoziativgesetz verletzt ist. Für kleine Werte von n lässt sich das auch praktisch durchführen.

II.2.3 Beispiele. i) Für $n = 0$ haben wir $G = \{e\}$ und

$\cdot$	e
e	e

.

ii) Für $n = 1$ gilt $G = \{ e, g \}$ und

$\cdot$	e	g
e	e	g
g	g	e

.

iii) Es seien $n = 2$ und $G = \{ e, g_1, g_2 \}$. Wegen $g_1 \cdot g_2 \neq g_1, g_2$ folgt $g_1 \cdot g_2 = e$ und

$\cdot$	e	g_1	g_2
e	e	g_1	g_2
g_1	g_1	g_2	e
g_2	g_2	e	g_1

.

iv) Für $n = 3$ und $G = \{ e, g_1, g_2, g_3 \}$ haben wir verschiedene Möglichkeiten. Die erste Wahl besteht für das Produkt $g_1 \cdot g_1$. Wenn wir $g_1 \cdot g_1 = g_2$ annehmen, ergibt sich zunächst

$\cdot$	e	g_1	g_2	g_3
e	e	g_1	g_2	g_3
g_1	g_1	g_2	g_3	e
g_2	g_2	g_3		
g_3	g_3	e		

.

Da $g_1 \cdot g_3 = e$, ist $g_2 \cdot g_3 = e$ unmöglich, so dass $g_2 \cdot g_3 = g_1$ und wir die Tabelle vervollständigen können zu

(I) :

$\cdot$	e	g_1	g_2	g_3
e	e	g_1	g_2	g_3
g_1	g_1	g_2	g_3	e
g_2	g_2	g_3	e	g_1
g_3	g_3	e	g_1	g_2

.

Entsprechend finden wir für $g_1 \cdot g_1 = g_3$ die Tabelle

(II) :

$\cdot$	e	g_1	g_2	g_3
e	e	g_1	g_2	g_3
g_1	g_1	g_3	e	g_2
g_2	g_2	e	g_3	g_1
g_3	g_3	g_2	g_1	e

.

Für $g_1 \cdot g_1 = e$ finden wir zwei mögliche Tabellen:

(III) :

$\cdot$	e	g_1	g_2	g_3
e	e	g_1	g_2	g_3
g_1	g_1	e	g_3	g_2
g_2	g_2	g_3	g_1	e
g_3	g_3	g_2	e	g_1

und (IV) :

$\cdot$	e	g_1	g_2	g_3
e	e	g_1	g_2	g_3
g_1	g_1	e	g_3	g_2
g_2	g_2	g_3	e	g_1
g_3	g_3	g_2	g_1	e

.

Es ist wahr, dass für alle diese Verknüpfungstafeln das Assoziativgesetz gilt. Wir rechnen das hier nicht nach, sondern verweisen auf Bemerkung II.3.1. Die durch Tabelle (IV) definierte Gruppe heißt *Kleinsche Vierergruppe*.[8]

II.2.4 Definition. Es sei G eine endliche Gruppe. Die Anzahl ihrer Elemente wird die *Ordnung von G* genannt.

Die obigen Beispiele zeigen:

II.2.5 Lemma. *Alle Gruppen der Ordnung höchstens vier sind abelsch.*

Es wird sich noch zeigen, dass Gruppen mit fünf Elementen ebenfalls abelsch sind (Lemma II.7.6). Die symmetrische Gruppe (Seite 27) S_3 ist eine Gruppe mit sechs Elementen, die nicht abelsch ist.

II.2.6 Aufgabe (Der Zykelgraph einer Gruppe). Es sei G eine endliche Gruppe. Eine Teilmenge $M \subset G$ ist *zyklisch*, wenn ein Element $g \in G$ existiert, so dass

$$M = \langle g \rangle := \{ g^k \mid k \geq 0 \}.$$

Es sei

$$\mathfrak{M} := \{ M \subset G \mid M \text{ ist zyklisch} \}$$

[8] Felix Christian Klein (1849 - 1925), deutscher Mathematiker.

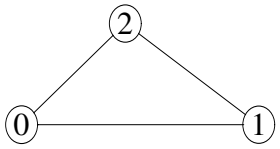
die Menge aller zyklischen Teilmengen von G. Eine zyklische Teilmenge $M \in \mathfrak{M}$ ist *maximal*, wenn sie maximal bzgl. „$\subset$“ ist, d.h.

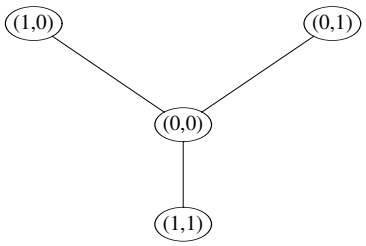
$$\forall N \in \mathfrak{M}: \quad M \subset N \quad \Longrightarrow \quad M = N.$$

Für jede maximale zyklische Teilmenge $M \subset G$ wird ein Element $g \in G$ mit $M = \langle g \rangle$ gewählt. Es seien $g_1, ..., g_s \in G$ die so erhaltenen Elemente und $n_i := \#\langle g_i \rangle$, $i = 1, ..., s$. Der *Zykelgraph*[9] Γ wird nun folgendermaßen definiert:

- ⋆ Die Ecken von Γ sind die Elemente von G.
- ⋆ Die Punkte g_i^j und g_i^{j+1} werden durch eine Kante verbunden, $j = 0, ..., n_i - 1$, $i = 1, ..., s$. Falls $n_i = 2$, dann wird nur eine Kante zwischen e und g gezeichnet. (Man beachte $g_i^0 = e = g_i^{n_i}$, $i = 1, ..., s$.)

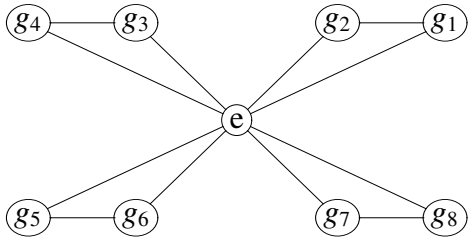
Beispiele:





$\mathbb{Z}_3$ $\qquad\qquad$ $\mathbb{Z}_2 \times \mathbb{Z}_2$

a) Zeigen Sie, dass der Durchschnitt zweier zyklischer Teilmengen von G zyklisch ist.
b) Zeichnen Sie die Zykelgraphen von $\mathbb{Z}_n$, $n \in \mathbb{N}$, der Gruppen aus Aufgabe II.1.5 a) und der Diedergruppe D_6.
c) Geben Sie eine Gruppe mit folgendem Zykelgraphen an:

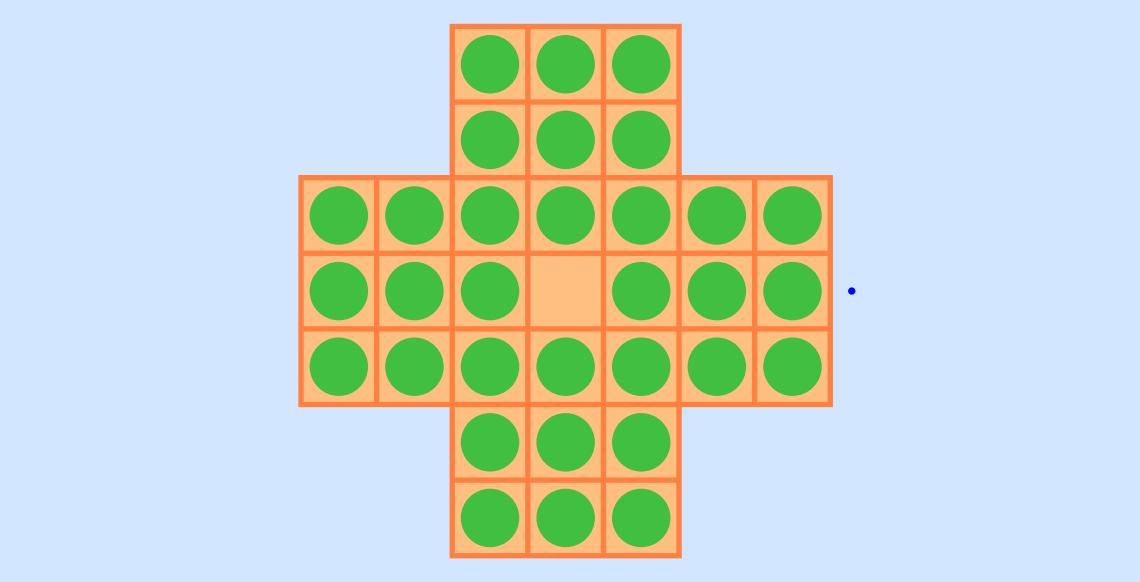


Eine spielerische Anwendung der Kleinschen Vierergruppe

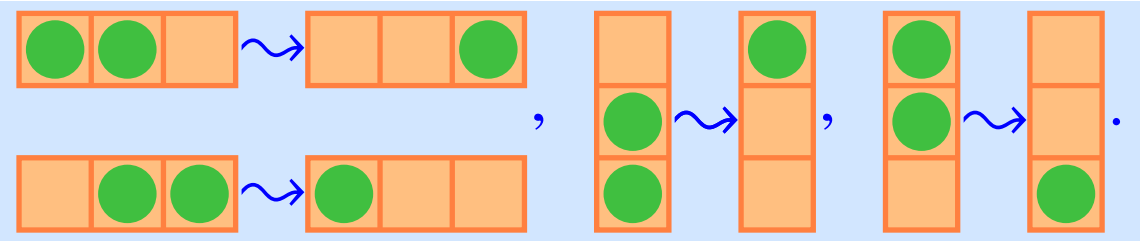
Mathematik wird immer dort besonders spannend, wo Techniken aus verschiedenen Bereichen aufeinandertreffen oder sie auf Fragen außerhalb der Mathematik angewandt wird. Das folgende Beispiel illustriert auf elementare aber dennoch aussagekräftige Weise, wie mathematische Denkweisen bei Problemlösungen eingesetzt werden können. Es stammt aus der Arbeit „The power of groups“ von Colva Roney-Dougal (`http://plus.maths.org/content/os/issue39/features/colva/index`).

Wir betrachten das Spiel **Solitaire**. Es wird mit 32 Spielsteinen ausgehend von folgender Startaufstellung gespielt:

[9] s. [16], Aufgabe 6.3.1, für die Defintion eines Graphen.



Dabei darf ein Stein einen benachbarten Stein überspringen, der sodann vom Spielfeld entfernt wird:



Ziel des Spiels ist, am Ende nur einen einzigen Stein in der Mitte des Spielfelds übrig zu behalten.

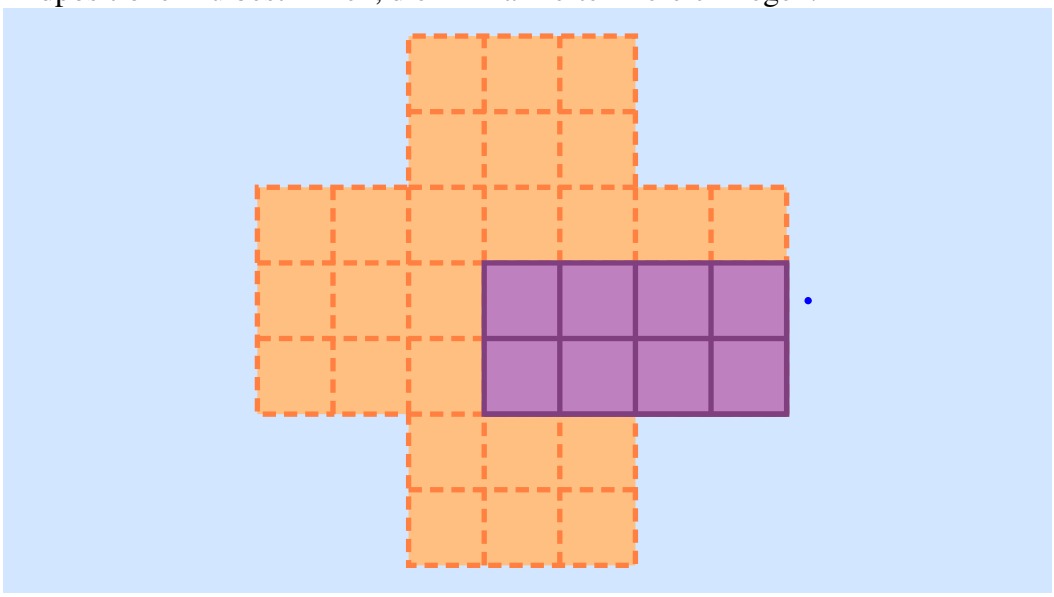
Die Regeln werden nun folgendermaßen modifiziert: Es wird nur noch gefordert, dass am Ende ein einziger Stein, egal wo, vorhanden ist. Wir stellen folgende **Fragen**:

- Welches sind die möglichen Endpositionen für den Stein?
- Wird das Spiel durch die neuen Regeln einfacher?

Die Theorie der Gruppen kommt auf zwei Weisen ins Spiel:

1. Das Spiel weist eine $\boldsymbol{D_4}$**-Symmetrie** auf. Wenn das Feld symmetrisch mit Mittelpunkt im Ursprung gefertigt ist, dann überführt jede Transformation aus D_4 das Spielfeld in sich selbst. Betrachtet man ein vollständiges Solitaire-Spiel vom ersten bis zum letzten Zug und ein Gruppenelement $g \in D_4$, dann kann man g auf jede Position, die im untersuchten Spiel auftrat, anwenden. Auf diese Weise erhält man wiederum ein mögliches Solitaire-Spiel. Deshalb braucht man z.B. nur diejenigen

Endpositionen zu bestimmen, die im markierten Bereich liegen:



2. Wir modellieren das Spiel mit der **Kleinschen Vierergruppe**. Diesmal verwenden wir $G = \{ e, a, b, c \}$ und dementsprechend die Verknüpfungstafel

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

.

Wir nennen $g \in G$ *nichttrivial*, wenn $g \neq e$. Der Verknüpfungstafel entnimmt man die folgenden Eigenschaften:

II.2.7 Lemma. i) *Für jedes Element $g \in G$ gilt $g^2 = e$.*

ii) *Das Produkt zweier verschiedener nichttrivialer Elemente in G ist das dritte nichttriviale Element.*

Jetzt fülle man das Solitaire-Feld mit den Buchstaben a, b und c dergestalt auf, dass auf drei benachbarten Feldern in horizontaler oder vertikaler Richtung immer drei verschiedene Buchstaben stehen. Eine Möglichkeit ist z.B. in Abbildung II.2 wiedergegeben.

II.2.8 Lemma. i) *Jedes Element auf dem Spielfeld ist Produkt der beiden Elemente, die links oder rechts von ihm bzw. über oder unter ihm stehen.*

ii) *Das Produkt aller Elemente auf dem Spielfeld ist e.*

Beweis. i) Dies folgt sofort aus Lemma II.2.7, ii). Für ii) beachte man, dass das Produkt aller Elemente auf dem Spielfeld nur deshalb sinnvoll ist, weil die Gruppe G abelsch ist. Die Behauptung rechnet man sofort nach. □

Mit diesen Vorbereitungen bewerte man eine Aufstellung auf dem Solitaire-Feld durch das Produkt aller Elemente, die zu **belegten** Feldern gehören. Damit erhält man:

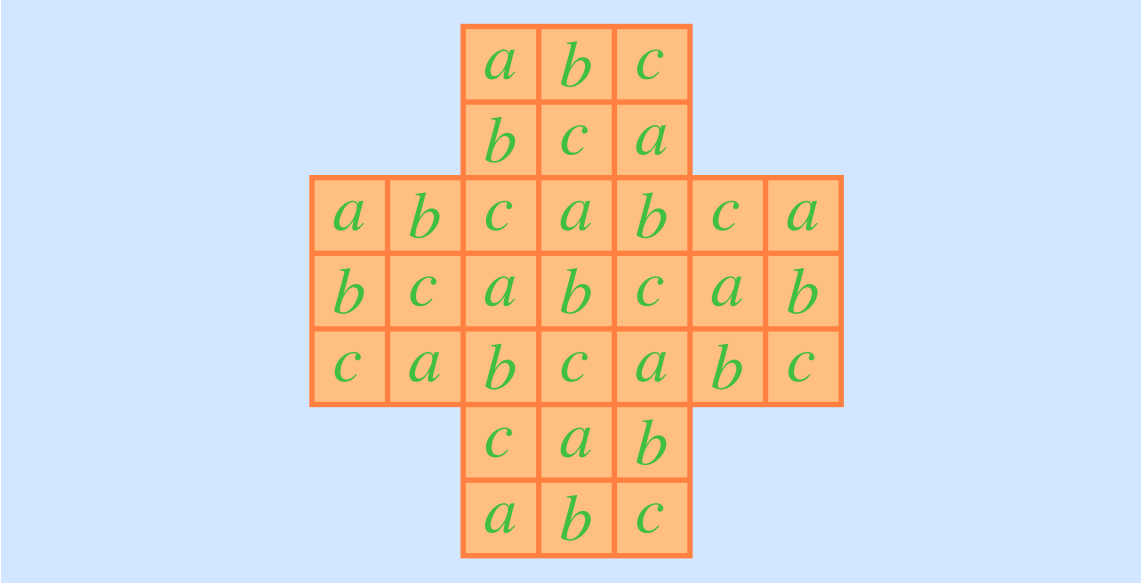


Abbildung II.2: Eine Nummerierung des Solitaire-Felds mit den Elementen der Kleinschen Vierergruppe

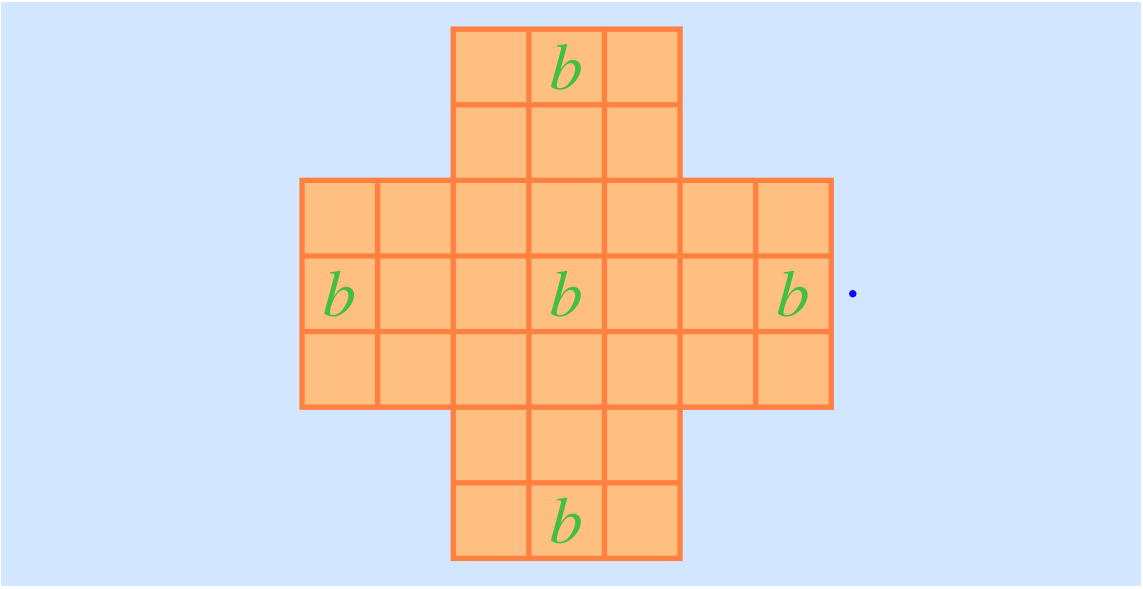
- Die Bewertung der Startaufstellung ist b.
- Die Bewertung ändert sich unter einem Zug **nicht**. (Dies ist Lemma II.2.8, i)

Wir schließen unmittelbar:

II.2.9 Satz. *Ein mögliches Schlussfeld ist ein „b-Feld“.*

Schließlich nutzen wir die D_4-Symmetrie aus: Für jedes Element $h \in D_4$ und jedes Schlussfeld F ist auch $h(F)$ ein Schlussfeld. Es folgt:

II.2.10 Satz. *Die folgende Abbildung zeigt die möglichen Schlussfelder:*



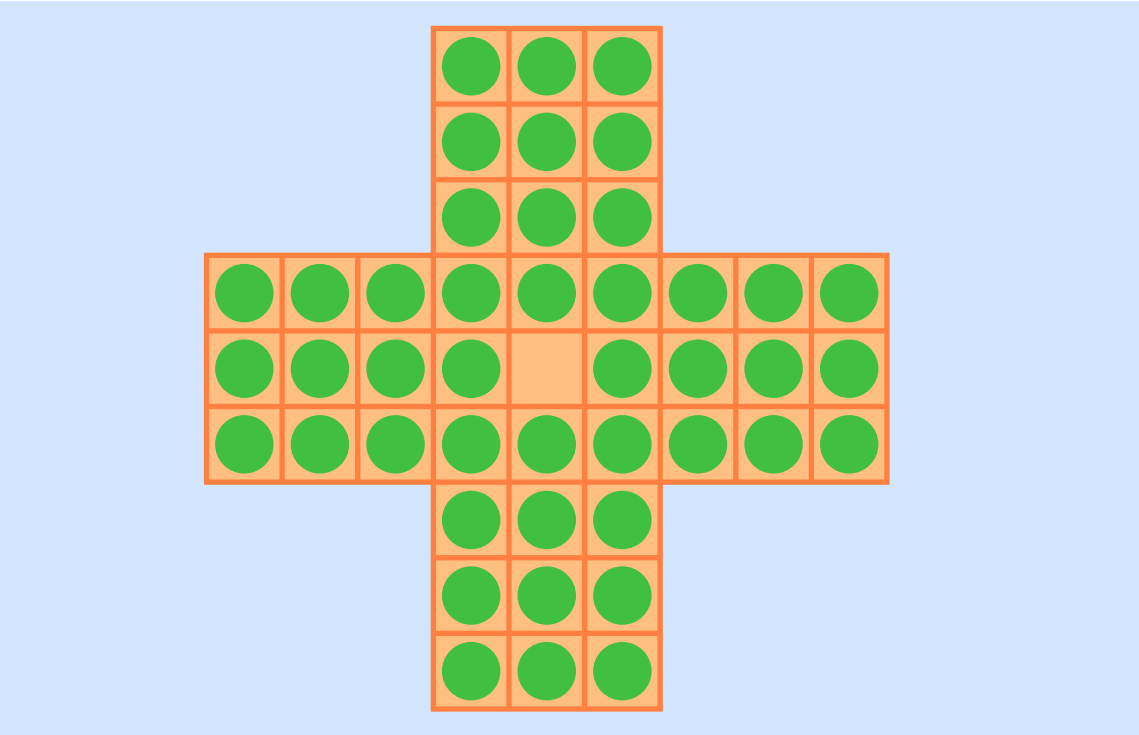
Insbesondere erkennt man:

- Ein Spiel, das auf einem der „äußeren“ Schlussfelder endet, unterscheidet sich von einem Spiel, das auf dem mittleren Feld endet, nur im letzten Zug.
- Da bekanntermaßen Spiele existieren, bei denen am Ende ein einziger Stein in der Mitte verbleibt, gibt es für jedes der markierten Schlussfelder auch ein Spiel, das auf ihm endet.

Das Spiel wird folglich durch die neuen Regeln **nicht** einfacher.

II.2.11 Aufgabe (Solitaire). a) Bestimmen Sie alle Endpositionen des Solitairespiels mit genau zwei Steinen.

b) Führen Sie die Diskussion aus der Vorlesung für das Spielfeld



durch.

II.3 Homomorphismen und Isomorphismen

Wir stellen zwei der Verknüpfungstafeln aus Beispiel II.2.3, iv), den Verknüpfungstafeln von $\mathbb{Z}_4$ und $\mathbb{Z}_2 \times \mathbb{Z}_2$ gegenüber:

$\mathbb{Z}_4$:

$\oplus$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

,

(I) :

$\cdot$	e	g_1	g_2	g_3
e	e	g_1	g_2	g_3
g_1	g_1	g_2	g_3	e
g_2	g_2	g_3	e	g_1
g_3	g_3	e	g_1	g_2

,

$\mathbb{Z}_2 \times \mathbb{Z}_2$:

+	(0,0)	(0,1)	(1,0)	(1,1)
(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)

,

(IV) :

·	e	g_1	g_2	g_3
e	e	g_1	g_2	g_3
g_1	g_1	e	g_3	g_2
g_2	g_2	g_3	e	g_1
g_3	g_3	g_2	g_1	e

.

Wir betrachten G mit der Verknüpfung aus (I). Da $\mathbb{Z}_4$ und $G := \{ e, g_1, g_2, g_3 \}$ verschiedene Mengen sind, sind $\mathbb{Z}_4$ und G auch verschiedene Gruppen. Allerdings ist die Abbildung

$$\begin{aligned} \varphi\colon \mathbb{Z}_4 &\longrightarrow G \\ 0 &\longmapsto e \\ i &\longmapsto g_i, \quad i = 1,2,3 \end{aligned}$$

bijektiv und erfüllt

$$\forall i, j \in \mathbb{Z}_4 : \quad \varphi(i \oplus j) = \varphi(i) \cdot \varphi(j).$$

Wir können also sagen, dass sich die Gruppen $\mathbb{Z}_4$ und G nur durch die Benennung ihrer Elemente unterscheiden und wir sie vermöge φ miteinander identifizieren können.

II.3.1 Bemerkungen. i) In $\mathbb{Z}_4$ gilt bekanntlich das Assoziativgesetz (Seite 35). Mit Hilfe von φ erkennen wir, dass auch die durch die Verknüpfungstafel (I) gegebene Multiplikation dem Assoziativgesetz Folge leistet.

ii) Entsprechende Bijektionen zwischen $\mathbb{Z}_4$ und $\{ e, g_1, g_2, g_3 \}$ findet man auch für die Verknüpfungstafeln (II) und (III) aus Beispiel II.2.3, iv).

Jetzt betrachten wir G mit der Verknüpfung aus (IV). Die Abbildung

$$\begin{aligned} \psi\colon \mathbb{Z}_2 \times \mathbb{Z}_2 &\longrightarrow G \\ (0,0) &\longmapsto e \\ (0,1) &\longmapsto g_1 \\ (1,0) &\longmapsto g_2 \\ (1,1) &\longmapsto g_3 \end{aligned}$$

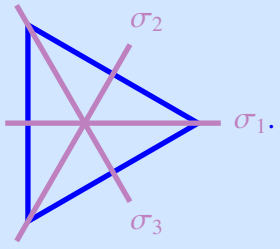
ist bijektiv und erfüllt

$$\forall g, h \in \mathbb{Z}_2 \times \mathbb{Z}_2 : \quad \psi(g + h) = \psi(g) \cdot \psi(h).$$

Auf diese Weise überprüfen wir insbesondere das Assoziativgesetz für die Verknüpfungstafel (IV).

Eine bijektive Abbildung $\chi\colon \mathbb{Z}_4 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_2$ mit $\chi(i \oplus j) = \chi(i) + \chi(j)$, $i, j \in \mathbb{Z}_4$, kann es nicht geben. Für jedes Element $g \in \mathbb{Z}_2 \times \mathbb{Z}_2$ gilt $g^2 = e$, in $\mathbb{Z}_4$ gilt z.B. $1 \oplus 1 = 2 \neq 0$. Die Gruppen $\mathbb{Z}_4$ und $\mathbb{Z}_2 \times \mathbb{Z}_2$ sind also wesentlich verschieden.

Wir untersuchen noch ein weiteres Beispiel dieser Art. Zunächst betrachten wir $D_3 = \{ e, \varrho_1, \varrho_2, \sigma_1, \sigma_2, \sigma_3 \}$. Dabei sei ϱ_1 die Drehung um den Winkel $2\pi/3$ und ϱ_2 diejenige um $4\pi/3$. Die Spiegelungen σ_1, σ_2 und σ_3 sind den Spiegelungsachsen wie folgt zugeordnet:



Wir berechnen die folgende Verknüpfungstafel:

	e	ϱ_1	ϱ_2	σ_1	σ_2	σ_3
e	e	ϱ_1	ϱ_2	σ_1	σ_2	σ_3
ϱ_1	ϱ_1	ϱ_2	e	σ_2	σ_3	σ_1
ϱ_2	ϱ_2	e	ϱ_1	σ_3	σ_1	σ_2
σ_1	σ_1	σ_3	σ_2	e	ϱ_2	ϱ_1
σ_2	σ_2	σ_1	σ_3	ϱ_1	e	ϱ_2
σ_3	σ_3	σ_2	σ_1	ϱ_2	ϱ_1	e

.

Auf der anderen Seite schauen wir uns die Gruppe S_3 an. Für $i, j, k \in \{1, 2, 3\}$ mit $\{i, j, k\} = \{1, 2, 3\}$ stehe $(i\ j\ k)$ für die Bijektion $1 \longmapsto i$, $2 \longmapsto j$ und $3 \longmapsto k$. Damit seien $e = (1\ 2\ 3)$, $r_1 = (2\ 3\ 1)$, $r_2 = (3\ 1\ 2)$, $s_1 = (2\ 1\ 3)$, $s_2 = (3\ 2\ 1)$ und $s_3 = (1\ 3\ 2)$. Dies führt zu der Verknüpfungstafel:

	e	r_1	r_2	s_1	s_2	s_3
e	e	r_1	r_2	s_1	s_2	s_3
r_1	r_1	r_2	e	s_2	s_3	s_1
r_2	r_2	e	r_1	s_3	s_1	s_2
s_1	s_1	s_3	s_2	e	r_2	r_1
s_2	s_2	s_1	s_3	r_1	e	r_2
s_3	s_3	s_2	s_1	r_2	r_1	e

.

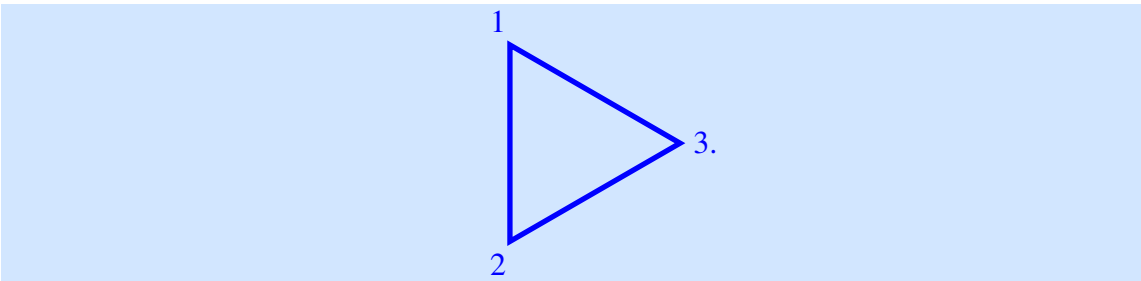
Hier ist

$$\begin{aligned} \varphi\colon D_3 &\longrightarrow S_3 \\ e &\longmapsto e \\ \varrho_i &\longmapsto r_i, \quad i = 1, 2 \\ \sigma_j &\longmapsto s_j, \quad j = 1, 2, 3 \end{aligned}$$

eine bijektive Abbildung, so dass

$$\forall g, h \in D_3 : \quad \varphi(g \cdot_{D_3} h) = \varphi(g) \cdot_{S_3} \varphi(h).$$

II.3.2 Bemerkung. Den Zusammenhang zwischen D_3 und S_3 können wir auch herstellen, indem wir die Ecken des Dreiecks wie folgt nummerieren:



Demnach

$$\varrho_1 \triangleq (2\ 3\ 1), \quad \varrho_2 \triangleq (3\ 1\ 2), \quad \sigma_1 \triangleq (2\ 1\ 3), \quad \sigma_2 \triangleq (3\ 2\ 1), \quad \sigma_3 \triangleq (1\ 3\ 2).$$

II.3.3 Definitionen. Es seien G und H zwei Gruppen.

i) Eine Abbildung $\varphi\colon G \longrightarrow H$ ist ein (*Gruppen-*)*Homomorphismus*, wenn gilt

$$\forall g, h \in G: \quad \varphi(g \cdot h) = \varphi(g) \cdot \varphi(h).$$

(Dabei wird auf der linken Seite der Gleichung die Multiplikation in G und auf der rechten Seite diejenige auf H verwendet.)

ii) Ein Gruppenhomomorphismus $\varphi\colon G \longrightarrow H$ ist ein (*Gruppen-*)*Isomorphismus*, falls es einen Gruppenhomomorphismus $\psi\colon H \longrightarrow G$ mit

$$\psi \circ \varphi = \mathrm{id}_G \quad \text{und} \quad \varphi \circ \psi = \mathrm{id}_H$$

gibt.

Im Sinne einer vorangegangenen Diskussion sind die Homomorphismen diejenigen Abbildungen, die mit der Zusatzstruktur „Multiplikation“ auf den Mengen G und H verträglich sind.

II.3.4 Lemma. *Es seien G, H zwei Gruppen und $\varphi\colon G \longrightarrow H$ ein Gruppenhomomorphismus.*

i) *Es gilt*

- $\varphi(e) = e$.
- $\forall g \in G: \varphi(g^{-1}) = \varphi(g)^{-1}$.

ii) *Der Homomorphismus φ ist genau dann ein Gruppenisomorphismus, wenn er bijektiv ist.*

Beweis. i) Aus der Gleichung $e = e \cdot e$ wird nach Anwendung von φ die Gleichung $\varphi(e) = \varphi(e) \cdot \varphi(e)$. Hier multiplizieren wir beide Seiten von links mit $\varphi(e)^{-1}$ und finden somit $e = \varphi(e)$. Für $g \in G$ folgt wegen $e = g^{-1} \cdot g$ die Gleichung $e = \varphi(e) = \varphi(g^{-1}) \cdot \varphi(g)$, die die Behauptung zeigt.

ii) Wenn φ ein Isomorphismus ist, dann ist φ sicherlich bijektiv. Wenn φ bijektiv ist, dann existiert $\psi = \varphi^{-1}\colon H \longrightarrow G$ als mengentheoretische Abbildung (vgl. Seite 27). Es ist noch zu überprüfen, dass ψ ein Homomorphismus ist. Letzteres läuft auf die Behauptung

$$\forall g, g' \in G,\ h, h' \in H: \quad (\varphi(g) = h \wedge \varphi(g') = h') \quad \Longrightarrow \quad \varphi(g \cdot g') = h \cdot h'$$

hinaus. Diese Gleichung folgt daraus, dass φ ein Homomorphismus ist. □

Wir sagen, dass zwei Gruppen G und H *isomorph* sind, wenn es einen Isomorphismus $\varphi\colon G \longrightarrow H$ zwischen ihnen gibt, und schreiben dann $G \cong H$. Mit diesem Begriff können wir die Klasse aller Gruppen in **Isomorphieklassen** zerlegen. Ein Hauptproblem der Gruppentheorie, mit dem auch wir uns im Folgenden intensiv beschäftigen werden, ist die Klassifikation von Gruppen bis auf Isomorphie.

II.3.5 Beispiele. i) Für $n = 1, 2, 3$ gibt es genau eine Isomorphieklasse von Gruppen der Ordnung n.

ii) Es existieren genau zwei Isomorphieklassen von Gruppen der Ordnung vier, und zwar diejenigen von $\mathbb{Z}_4$ und $\mathbb{Z}_2 \times \mathbb{Z}_2$.

iii) Es seien k ein Körper, $k^\star := k \setminus \{0\}$ und $n \geq 1$. Die Determinantenabbildung $\mathrm{Det}\colon \mathrm{GL}_n(k) \longrightarrow k^\star$ ist ein Homomorphismus. Für $n = 1$ ist Det die Identität und somit ein Isomorphismus. Für $n > 1$ ist Det surjektiv aber nicht injektiv. Für $\lambda \in k^\star$ haben wir

$$\lambda = \mathrm{Det}\left(\begin{array}{cc|c} \lambda & 0 & \\ 0 & 1 & 0 \\ \hline & 0 & \mathbb{E}_{n-2} \end{array}\right) = \mathrm{Det}\left(\begin{array}{cc|c} \lambda & 1 & \\ 0 & 1 & 0 \\ \hline & 0 & \mathbb{E}_{n-2} \end{array}\right).$$

iv) Die Abbildung

$$\begin{array}{rccc} q\colon & \mathbb{R}^\star & \longrightarrow & \mathbb{R}^\star \\ & x & \longmapsto & x^2 \end{array}$$

ist ein Homomorphismus, der weder injektiv noch surjektiv ist.

v) Die Abbildung

$$\begin{array}{rccc} p\colon & \mathbb{Z} & \longrightarrow & \mathbb{Z}_2 \\ & k & \longmapsto & \begin{cases} 0, & \text{falls } k \text{ gerade} \\ 1, & \text{falls } k \text{ ungerade} \end{cases} \end{array}$$

ist ein Homomorphismus. Er ist surjektiv aber nicht injektiv.

vi) Es seien

$$\begin{array}{rccc} \varphi\colon & \mathbb{Z}_2 & \longrightarrow & \mathbb{Z}_4 \\ & 0 & \longmapsto & 0 \\ & 1 & \longmapsto & 2 \end{array} \qquad \text{und} \qquad \begin{array}{rccc} \psi\colon & \mathbb{Z}_4 & \longrightarrow & \mathbb{Z}_2 \\ & 0 & \longmapsto & 0 \\ & 1 & \longmapsto & 1 \\ & 2 & \longmapsto & 0 \\ & 3 & \longmapsto & 1. \end{array}$$

Dies sind beides Gruppenhomomorphismen (Übung). Die Verknüpfung $\psi \circ \varphi\colon \mathbb{Z}_2 \longrightarrow \mathbb{Z}_2$ schickt beide Elemente auf Null, und $\varphi \circ \psi\colon \mathbb{Z}_4 \longrightarrow \mathbb{Z}_4$ ist die Multiplikation mit 2. Die Veknüpfung $\mathbb{Z} \longrightarrow \mathbb{Z}_4 \xrightarrow{\psi} \mathbb{Z}_2$ ist der Homomorphismus aus v).

II.3.6 Aufgabe (Isomorphismen). Zeigen Sie, dass die Gruppen $(\mathbb{R}, +)$ und $(\mathbb{R}_{>0}, \cdot)$ isomorph sind. (**Hinweis.** Hier benötigen Sie etwas Analysis.)

II.3.7 Aufgabe (Homomorphismen). Es sei $Q \subset \mathbb{R}^2$ ein Quadrat mit Mittelpunkt 0.

a) Nummerieren Sie die Eckpunkte von Q entgegen dem Uhrzeigersinn von 1 bis 4. Ein Element $f \in D_4$ definiert die Permutation $\varphi(f) \in S_4$ durch $\varphi(f)(i) = f(i)$, $i = 1, ..., 4$. Geben Sie $\varphi(f)$ für jedes Element $f \in D_4$ an. Ist $\varphi\colon D_4 \longrightarrow S_4$ injektiv und/oder surjektiv?[10]

b) Nummerieren Sie nun die Kanten von Q von 1 bis 4 und konstruieren damit eine weitere Abbildung $\psi\colon D_4 \longrightarrow S_4$. Kann man die Ecken und Kanten so nummerieren, dass $\varphi = \psi$ gilt? Hat man $\varphi(D_4) = \psi(D_4)$?

II.3.8 Aufgabe (Symmetriegruppen und spezielle Symmetriegruppen). Es seien $M \subset \mathbb{R}^2$ eine Teilmenge, die eine Basis für $\mathbb{R}^2$ enthält, und

$$M' := M \times \{0\} = \{\, (x, y, 0) \in \mathbb{R}^3 \mid (x, y) \in M \,\}.$$

Beweisen Sie[11] $\mathrm{O}(M) \cong \mathrm{SO}(M')$.

[10] Sie sollten sich davon überzeugen, dass φ ein Gruppenhomomorphismus ist. Wir werden dies im Rahmen der Gruppenwirkungen nochmals thematisieren.

[11] Die erste Symmetriegruppe wird für $M \subset \mathbb{R}^2$ und die zweite für M' als Teilmenge von $\mathbb{R}^3$ gebildet.

II.4 Untergruppen

Viele der Beispiele von Gruppen, die wir oben angegeben haben, haben wir innerhalb bereits existierender, größerer Gruppen konstruiert, z.B.:

- Es seien k ein Körper und $n \geq 1$. Wir haben $\mathrm{GL}_n(k) \subset S(k^n)$, $\mathrm{O}_n(k) \subset \mathrm{GL}_n(k)$, $\mathrm{SO}_n(k) \subset \mathrm{O}_n(k)$.
- Für $n \geq 1$ und $M \subset \mathbb{R}^n$ haben wir $\mathrm{O}(M) \subset \mathrm{O}_n(\mathbb{R})$, $\mathrm{SO}(M) \subset \mathrm{O}(M)$.

Das führt auf natürlichem Weg zum Begriff der Untergruppe. Untergruppen sind auch ein wichtiges Hilfsmittel zur Untersuchung der Struktur von Gruppen, z.B. um zwei gegebene Gruppen voneinander zu unterscheiden (s. Abschnitt II.11).

II.4.1 Definition. Es seien G eine Gruppe und $H \subset G$ eine Teilmenge. Wir sagen, H ist eine *Untergruppe* von G, wenn gilt:

- ⋆ $e \in H$,
- ⋆ $\forall g \in H : g^{-1} \in H$,
- ⋆ $\forall g, g' \in H : g \cdot g' \in H$.

II.4.2 Bemerkung. Es seien $(G, \cdot_G)$ eine Gruppe und $H \subset G$ eine Untergruppe. Auf Grund der dritten Eigenschaft können wir die Multiplikation

$$\begin{array}{rcl} \cdot_H \colon H \times H & \longrightarrow & H \\ (g, g') & \longmapsto & g \cdot_G g' \end{array}$$

erklären. Es folgt jetzt leicht, dass $(H, \cdot_H)$ eine Gruppe ist.

II.4.3 Beispiele. i) Jede Gruppe G besitzt die Untergruppen $\{e\}$ und G.

ii) Für $k \geq 1$ ist

$$k \cdot \mathbb{Z} = \{\, k \cdot m \,|\, m \in \mathbb{Z} \,\} = \{\, l \in \mathbb{Z} \,|\, k|l \,\}$$

eine Untergruppe von $\mathbb{Z}$.

iii) $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$ ist eine Kette von Untergruppen.

iv) Es ist $\mathbb{Q}^\star \subset \mathbb{R}^\star$ eine Untergruppe.

v) Es ist $\mathbb{R}_{>0} := \{\, x \in \mathbb{R} \,|\, x > 0 \,\} \subset \mathbb{R}^\star$ eine Untergruppe.

vi) Die Gruppe G sei durch die Verknüpfungstafel

$\cdot$	e	g_1	g_2	g_3
e	e	g_1	g_2	g_3
g_1	g_1	g_2	g_3	e
g_2	g_2	g_3	e	g_1
g_3	g_3	e	g_1	g_2

gegeben. Dann ist $\{\, e, g_2 \,\}$ eine Untergruppe.

vii) Die Kleinsche Vierergruppe, die durch die Verknüpfungstafel

$\cdot$	e	g_1	g_2	g_3
e	e	g_1	g_2	g_3
g_1	g_1	e	g_3	g_2
g_2	g_2	g_3	e	g_1
g_3	g_3	g_2	g_1	e

bestimmt wird, hat nach Lemma II.2.7, i), die Untergruppen $\{e\}$, $\{e, g_1\}$, $\{e, g_2\}$ und $\{e, g_3\}$ und $\{e, g_1, g_2, g_3\}$.

viii) Es seien D_n die Diedergruppe und ϱ_k die Drehung um den Winkel $2\pi k/n$, $k = 0, ..., n-1$. Dann ist

$$H = \{e = \varrho_0, \varrho_1, ..., \varrho_{n-1}\}$$

eine Untergruppe. Sie ist isomorph zu $\mathbb{Z}_n$. Man kann diese Untergruppe in der Verknüpfungstafel erkennen, z.B. für $n = 3$ (vgl. Seite 45):

	e	ϱ_1	ϱ_2	σ_1	σ_2	σ_3
e	e	ϱ_1	ϱ_2	σ_1	σ_2	σ_3
ϱ_1	ϱ_1	ϱ_2	e	σ_2	σ_3	σ_1
ϱ_2	ϱ_2	e	ϱ_1	σ_3	σ_1	σ_2
σ_1	σ_1	σ_3	σ_2	e	ϱ_2	ϱ_1
σ_2	σ_2	σ_1	σ_3	ϱ_1	e	ϱ_2
σ_3	σ_3	σ_2	σ_1	ϱ_2	ϱ_1	e

.

Man sieht weiter, dass für eine Untergruppe $H' \subset D_3$ aus $H \subsetneq H'$ bereits $H' = D_3$ folgt.[12]

II.4.4 Lemma. *Es seien G, H Gruppen und $\varphi\colon G \longrightarrow H$ ein Gruppenhomomorphismus. Dann ist*

$$\mathrm{Ker}(\varphi) := \{g \in G \mid \varphi(g) = e\}$$

eine Untergruppe von G und

$$\mathrm{Im}(\varphi) := \{h \in H \mid \exists g \in G : \varphi(g) = h\} = \{\varphi(g) \in H \mid g \in G\}$$

eine Untergruppe von H.

Beweis. Wir beginnen mit $\mathrm{Ker}(\varphi)$, dem sogenannten *Kern* des Homomorphismus φ. Bereits in Lemma II.3.4, i), haben wir gezeigt, dass $\varphi(e) = e$, also $e \in \mathrm{Ker}(\varphi)$. Für $g \in \mathrm{Ker}(\varphi)$ haben wir wiederum mit Lemma II.3.4, i), $\varphi(g^{-1}) = \varphi(g)^{-1} = e^{-1} = e$, so dass $g^{-1} \in \mathrm{Ker}(\varphi)$ folgt. Schließlich seien $g, g' \in \mathrm{Ker}(\varphi)$. Wir berechnen $\varphi(g \cdot g') = \varphi(g) \cdot \varphi(g') = e \cdot e = e$ und schließen $g \cdot g' \in \mathrm{Ker}(\varphi)$.

Nun zeigen wir, dass $\mathrm{Im}(\varphi)$, das sogenannte *Bild* von φ, eine Untergruppe von H ist. Da $\varphi(e) = e$, folgt $e \in \mathrm{Im}(\varphi)$. Nun seien $h \in \mathrm{Im}(\varphi)$ und $g \in G$ mit $\varphi(g) = h$. Wir finden $h^{-1} = \varphi(g)^{-1} = \varphi(g^{-1})$ und damit $h^{-1} \in \mathrm{Im}(\varphi)$. Zu Elementen $h, h' \in \mathrm{Im}(\varphi)$ existieren $g, g' \in G$ mit $h = \varphi(g)$ und $h' = \varphi(g')$. Somit gilt $h \cdot h' = \varphi(g) \cdot \varphi(g') = \varphi(g \cdot g')$, und wir erkennen $h \cdot h' \in \mathrm{Im}(\varphi)$. □

Das Konzept des Kerns liefert ein nützliches Kriterium für die Injektivität eines Gruppenhomomorphismus.

II.4.5 Lemma. *Es seien G, H Gruppen und $\varphi\colon G \longrightarrow H$ ein Homomorphismus. Dann ist φ genau dann injektiv, wenn $\mathrm{Ker}(\varphi) = \{e\}$ gilt.*

Beweis. Es gilt immer $\{e\} \subset \mathrm{Ker}(\varphi)$. Wenn φ injektiv ist, wird kein weiteres Element aus G auf e abgebildet, so dass $\mathrm{Ker}(\varphi) = \{e\}$.

[12] Folgerung II.7.4 liefert eine allgemeine Erklärung hierfür.

Wir setzen $\mathrm{Ker}(\varphi) = \{e\}$ voraus. Es seien $h \in H$ und $g, g' \in G$ mit $\varphi(g) = h = \varphi(g')$. Aus $\varphi(g) = \varphi(g')$ folgt

$$\varphi(g^{-1} \cdot g') = \varphi(g^{-1}) \cdot \varphi(g') = \varphi(g)^{-1} \cdot \varphi(g') = e,$$

d.h. $g^{-1} \cdot g' \in \mathrm{Ker}(\varphi)$. Die Voraussetzung zeigt $g^{-1} \cdot g' = e$ und folglich $g = g'$. □

II.4.6 Beispiele. i) Es seien k ein Körper und $n \geq 1$. Für den Determinantenhomomorphismus $\mathrm{Det}\colon \mathrm{GL}_n(k) \longrightarrow k^\star$ ist

$$\mathrm{Ker}(\mathrm{Det}) = \{\, m \in \mathrm{GL}_n(k) \,|\, \mathrm{Det}(m) = 1 \,\} =: \mathrm{SL}_n(k),$$

die sogenannte *spezielle lineare Gruppe*.

ii) Bei dem Homomorphismus $q\colon \mathbb{R}^\star \longrightarrow \mathbb{R}^\star$, $x \longmapsto x^2$, haben wir $\mathrm{Ker}(\varphi) = \{\pm 1\}$ und $\mathrm{Im}(\varphi) = \mathbb{R}_{>0}$.

iii) Der Kern des Homomorphismus

$$\begin{array}{rccl} s\colon & \mathbb{Z} & \longrightarrow & \mathbb{Z}_2 \\ & k & \longmapsto & \begin{cases} 0, & \text{falls } k \text{ gerade} \\ 1, & \text{falls } k \text{ ungerade} \end{cases} \end{array}$$

besteht aus den geraden Zahlen:

$$\mathrm{Ker}(s) = 2 \cdot \mathbb{Z}.$$

Das folgende Lemma ist ein bekanntes Kriterium, um zu testen, dass eine Teilmenge einer Gruppe eine Untergruppe ist.

II.4.7 Lemma. *Es seien G eine Gruppe und $H \subset G$ eine Teilmenge. Dann ist H genau dann eine Untergruppe, wenn gilt:*

- $\star$ $H \neq \emptyset$,
- $\star$ $\forall h, h' \in H : h^{-1} \cdot h' \in H$.

Beweis. Wenn H eine Untergruppe von G ist, dann gilt $e \in H$ und $H \neq \emptyset$. Für $h, h' \in H$ haben wir $h^{-1}, h' \in H$ und damit auch $h^{-1} \cdot h' \in H$.

Nun erfülle H das genannte Kriterium. Dann existiert ein Element $h \in H$ und $e = h^{-1} \cdot h \in H$. Für $h \in H$ gilt wegen $e \in H$ dann auch $h^{-1} = h^{-1} \cdot e \in H$. Zu guter Letzt seien $h, h' \in H$. Dann gilt auch $h^{-1}, h' \in H$ und nach Voraussetzung $h \cdot h' = (h^{-1})^{-1} \cdot h' \in H$. □

Wir stellen ein weiteres wichtiges Beispiel für eine Untergruppe vor. Für die Untergruppeneigenschaft überprüfen wir die Axiome aus Definition II.4.1.

II.4.8 Beispiel. Es seien G eine Gruppe, I eine **nichtleere** Indexmenge und $(H_i)_{i \in I}$ eine Familie von Untergruppen von G. Dann ist auch

$$H_I := \bigcap_{i \in I} H_i$$

eine Untergruppe von G. Da H_i eine Untergruppe von G ist, gilt $e \in H_i$, $i \in I$. Daher folgt $e \in H_I$. Für $g, g' \in G$ sind die Bedingungen $g \in H_I$ bzw. $g' \in H_I$ äquivalent zu

$$\forall i \in I : \quad g \in H_i \quad \text{bzw.} \quad g' \in H_i.$$

Die Untergruppeneigenschaft von H_i impliziert $g^{-1} \in H_i$ und $g \cdot g' \in H_i$, $i \in I$, und damit $g^{-1} \in H_I$ und $g \cdot g' \in H_I$.

II.4.9 Aufgaben (Untergruppen). a) Ist $H := \{\sigma \in S_4 \mid \sigma(4) = 3 \vee \sigma(4) = 4\}$ eine Untergruppe von S_4?

b) Es seien G eine **abelsche** Gruppe und $H := \{g \in G \mid g^2 = e\}$. Zeigen Sie, dass H eine Untergruppe von G ist.

c) Weisen Sie nach, dass $H := \{m \in \mathrm{O}_2(\mathbb{R}) \mid m^2 = e\}$ keine **Untergruppe** von $\mathrm{O}_2(\mathbb{R})$ ist. Welche Eigenschaft ist nicht erfüllt?

Erzeugendensysteme

II.4.10 Satz. *Es seien G eine Gruppe und $M \subset G$ eine Teilmenge. Dann gibt es genau eine Untergruppe $H \subset G$, die folgende Eigenschaften aufweist:*

- ⋆ $M \subset H$.
- ⋆ *Für jede Untergruppe $H' \subset G$, für die $M \subset H'$ gilt, hat man auch $H \subset H'$.*

Die Untergruppe H ist somit die kleinste Untergruppe von G, die M enthält.

II.4.11 Definition. In der Situation des Satzes heißt H die *von M erzeugte Untergruppe* von G.
Schreibweise. $\langle M\rangle := H$. Falls $M = \{g_1, ..., g_s\}$, so schreiben wir $\langle g_1, ..., g_s\rangle := \langle M\rangle$.

Beweis von Satz II.4.10. Die **Eindeutigkeit** ist unmittelbar klar: Für zwei Untergruppen H und H' mit den genannten Eigenschaften gilt $H \subset H'$ und $H' \subset H$ und deshalb $H = H'$.

Existenz. Wir setzen

$$I := \{K \subset G \mid K \text{ ist Untergruppe von } G \text{ und } M \subset K\}.$$

Wegen $G \in I$ ist I nicht leer. Nach Beispiel II.4.8 ist

$$H := \bigcap_{K \in I} K$$

eine Untergruppe von G. Sie hat die geforderten Eigenschaften. □

II.4.12 Beispiel. $\langle \varnothing\rangle = \{e\}$.

Bevor wir zusätzliche Beispiele besprechen, stellen wir eine weitere Konstruktion von $\langle M\rangle$ vor, die die Natur dieses Objekts deutlich macht.

II.4.13 Definitionen. Es seien G eine Gruppe und M eine Teilmenge.

i) Für $g \in G$ und $n \in \mathbb{N}$ wird g^n rekursiv definiert:

- ⋆ $g^0 := e$,
- ⋆ $g^{n+1} := g \cdot g^n$, $n \in \mathbb{N}$.

Weiter sei für $k \in \mathbb{Z}$

$$g^k := \begin{cases} g^k, & \text{falls } k \geq 0 \\ (g^{-k})^{-1}, & \text{falls } k < 0 \end{cases}.$$

(Man beachte, dass $(g^{-k})^{-1} = (g^{-1})^{-k}$ für $k < 0$ gilt.)

ii) Ein Element $g \in G$ wird als *Wort in M* bezeichnet, wenn

- ⋆ $g = e$

oder

- ⋆ ein $s \geq 1$, $g_1, ..., g_s \in G$ und $m_1, ..., m_s \in \mathbb{Z}$ existieren, so dass[13]

$$g = g_1^{m_1} \cdot \dots \cdot g_s^{m_s}.$$

II.4.14 Bemerkung. Falls $M \neq \emptyset$, dann benötigen wir nur die zweite Bedingung, denn für $g \in M$ ist $e = g^{-1} \cdot g$ ein Wort in M.

II.4.15 Lemma. *Es seien G eine Gruppe, $M \subset G$ eine Teilmenge und*

$$\mathrm{Erz}(M) := \{\, g \in G \mid g \textit{ ist ein Wort in } M \,\}.$$

Dann gilt

$$\mathrm{Erz}(M) = \langle M \rangle.$$

Beweis. **Schritt 1.** Wir zeigen, dass $\mathrm{Erz}(M)$ eine Untergruppe von G ist.

- ⋆ Die Bedingung $e \in \mathrm{Erz}(M)$ ist in Definition II.4.13, ii), festgehalten.
- ⋆ Es sei $g = g_1^{m_1} \cdot \dots \cdot g_s^{m_s} \in \mathrm{Erz}(M)$. Dann folgt $g^{-1} = g_s^{-m_s} \cdot \dots \cdot g_1^{-m_1} \in \mathrm{Erz}(M)$.
- ⋆ Für $g = g_1^{m_1} \cdot \dots \cdot g_s^{m_s} \in \mathrm{Erz}(M)$ und $h = h_1^{n_1} \cdot \dots \cdot h_s^{n_t} \in \mathrm{Erz}(M)$ hat man auch $g \cdot h = g_1^{m_1} \cdot \dots \cdot g_s^{m_s} \cdot h_1^{n_1} \cdot \dots \cdot h_s^{n_t} \in \mathrm{Erz}(M)$.

Schritt 2. Die Inklusion $M \subset \mathrm{Erz}(M)$ ist offensichtlich.

Schritt 3. Wir weisen $\mathrm{Erz}(M) \subset \langle M \rangle$ nach. Dabei dürfen wir $M \neq \emptyset$ voraussetzen. Zunächst zeigen wir, dass für $g \in M$ und $k \in \mathbb{Z}$ stets auch $g^k \in \langle M \rangle$. Für $k \geq 0$ benutzen wir ein Induktionsargument. Für $k = 0$ bzw. 1 gilt $g^k = e$ bzw. g und deswegen $g^k \in \langle M \rangle$. Weiter haben wir $g^{k+1} = g \cdot g^k$. Nach Induktionsvoraussetzung liegen g und g^k in $\langle M \rangle$. Da $\langle M \rangle$ eine Untergruppe ist, liegt deshalb auch g^{k+1} in $\langle M \rangle$.

Für $k < 0$ liegt g^{-k} in $\langle M \rangle$. Die Untergruppeneigenschaft von $\langle M \rangle$ beinhaltet $g^k = (g^{-k})^{-1} \in \langle M \rangle$.

Weiter seien $s(e) = 0$ und für $g \in \mathrm{Erz}(M) \setminus \{e\}$

$$s(g) := \min\{\, s \geq 1 \mid \exists g_1, ..., g_s \in M,\ m_1, ..., m_s \in \mathbb{Z} : g = g_1^{m_1} \cdot \dots \cdot g_s^{m_s} \,\}.$$

Wir zeigen durch Induktion über s, dass jedes Element von $\mathrm{Erz}(M)$ zu M gehört. Für $\boldsymbol{s = 0}$ und $\boldsymbol{s = 1}$ haben wir dies bereits getan.

[13] In einer abelschen Gruppe würde diese Gleichung als

$$g = m_1 \cdot g_1 + \dots + m_s \cdot g_s$$

geschrieben. Dies erinnert an Linearkombinationen in der Linearen Algebra, die in der Konstruktion der linearen Hülle einer Teilmenge eines Vektorraums auftauchen ([20], §9, Definition 2 und Satz 3; [5], Abschnitt 1.4.4). Ersetzt man den Körper k in der Linearen Algebra durch den Ring $\mathbb{Z}$, so ist das richtige Analogon zu einem k-Vektorraum ein sogenannter $\mathbb{Z}$**-Modul**. Letzteres ist aber nichts anderes als eine abelsche Gruppe. In nichtabelschen Gruppen muss man mit der Interpretation als Linearkombination aber äußerst vorsichtig umgehen.

$\boldsymbol{s \longrightarrow s+1}$**.** Es seien $s \geq 1$, $g_1, ..., g_{s+1} \in M$ und $m_1, ..., m_{s+1} \in \mathbb{Z}$ mit $g = g_1^{m_1} \cdot \cdots \cdot g_{s+1}^{m_{s+1}}$. Wir schreiben

$$g = \underbrace{(g_1^{m_1} \cdot \cdots \cdot g_s^{m_s})}_{=:h} \cdot g_{s+1}^{m_{s+1}}.$$

Wegen $s(h) = s$ gilt nach Induktionsvoraussetzung $h \in \langle M \rangle$. Weiter haben wir $g_{s+1}^{m_{s+1}} \in \langle M \rangle$. Da $\langle M \rangle$ eine Untergruppe von G ist, schließen wir $g = h \cdot g_{s+1}^{m_{s+1}} \in \langle M \rangle$.

Schritt 1 und Schritt 2 implizieren nach Definition II.4.11 $\langle M \rangle \subset \mathrm{Erz}(M)$. Aus Schritt 3 folgt daher die Behauptung. □

II.4.16 Beispiele. i) Wir haben $\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.

ii) Es sei D_n die Diedergruppe (s. Beispiel II.1.9, i). Es seien

- ⋆ r die Drehung um den Winkel $2\pi/n$,
- ⋆ s die Spiegelung an der x-Achse.

Behauptung. *Man hat*

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

Genauer gilt

$$D_n = \{\, e, r, ..., r^{n-1}, s, r \cdot s, ..., r^{n-1} \cdot s \,\}.$$

Beweis. Die Menge $\{\, e, r, ..., r^{n-1} \,\}$ umfasst alle Drehungen, die in der Diedergruppe enthalten sind. Die Abbildung ϱ_s (s. Lemma II.2.1) ist bijektiv, so dass $\{\, s, r \cdot s, ..., r^{n-1} \cdot s \,\}$ ebenfalls n Elemente umfasst. Schließlich gilt

$$\{\, e, r, ..., r^{n-1} \,\} \cap \{\, s, r \cdot s, ..., r^{n-1} \cdot s \,\} = \varnothing.$$

In der Tat haben die Elemente der „linken“ Menge die Determinante 1 und die der rechten Determinante -1. Wegen $\#D_n = 2n$ folgt die Behauptung. □

Bemerkung. Es seien $e_0, ..., e_{n-1}$ die Ecken eines regelmässigen n-Ecks auf dem Einheitskreis. Wir nehmen an, dass $e_0 = (1, 0)$ und e_k auf e_{k-1} im mathematisch positiven Sinne folgt, $k = 1, ..., n-1$. Weiter sei k_l die Kante, die e_l mit e_{l+1} verbindet, $l = 0, ..., n-2$, und k_{n-1} diejenige, die e_{n-1} mit e_0 verbindet.

i) Wir wissen, dass $r \cdot s$ eine Spiegelung ist, und zwar diejenige an der Achse durch den Mittelpunkt der Kante k_0. Es folgt

$$(r \cdot s) \cdot (r \cdot s) = e$$

und zusammen mit $s^2 = e$

$$r \cdot s \cdot r = s.$$

Schließlich impliziert dies

$$s \cdot r = r^{-1} \cdot s = r^{n-1} \cdot s. \tag{II.1}$$

Diese Relation ist entscheidend für das explizite Rechnen in D_n, weil sie zeigt, wie man s an r „vorbeischieben“ kann.

ii) Wir wollen noch ein anschauliches Verfahren angeben, wie man eine Spiegelung als Wort in r und s schreibt. Zunächst sei s' eine Spiegelung, deren Achse durch die Ecke e_k gehe. Dann folgt

$$s' = r^k \cdot s \cdot r^{-k} = r^k \cdot s \cdot r^{n-k}, \quad k = 0, ..., n-1.$$

(Das Element r^{-k} dreht die Spiegelungsachse auf die x-Achse. Dann wird an der x-Achse gespiegelt und schließlich die Drehung rückgängig gemacht. Das Ergebnis ist s'.)

Verläuft die Achse von s' durch den Mittelpunkt der Kante k_l, so findet man entsprechend

$$s' = r^l \cdot (s \cdot r) \cdot r^{-l}, \quad l = 0, ..., n-1.$$

Mit Hilfe von Relation (II.1) kann man diese Wörter in der Form $r^i \cdot s^j$ mit $i \in \{0, ..., n-1\}$ und $j \in \{0, 1\}$ schreiben.

II.4.17 Definitionen. i) Eine Gruppe G heißt *zyklisch*, wenn ein Element $g \in G$ mit

$$G = \langle g \rangle$$

existiert.

ii) Für $g \in G$ ist

$$\mathrm{Ord}(g) := \begin{cases} \infty, & \text{falls } g^n \neq e \text{ für alle } n \geq 1 \\ \min\{ n \geq 1 \mid g^n = e \}, & \text{sonst} \end{cases}$$

die *Ordnung* von g.

II.4.18 Bemerkungen. i) Für eine Gruppe G und ein Element $g \in G$ ist

$$\begin{array}{rccc} \mathrm{ev}_g \colon & \mathbb{Z} & \longrightarrow & G \\ & k & \longmapsto & g^k \end{array}$$

ein Gruppenhomomorphismus. Dabei gilt

- ⋆ Der Homomorphismus ev_g ist genau dann injektiv, wenn $\mathrm{Ord}(g) = \infty$.
- ⋆ Für $n \geq 1$ ist die Gleichung $\mathrm{Ord}(g) = n$ äquivalent zu $\mathrm{Ker}(\mathrm{ev}_g) = n \cdot \mathbb{Z}$ (vgl. Beispiel II.4.3, ii).

ii) Eine zyklische Gruppe ist abelsch. (Aus i) kann man schließen, dass eine zyklische Gruppe isomorph zu $\mathbb{Z}$ oder $\mathbb{Z}_n$ für ein geeignetes $n \geq 1$ ist.)

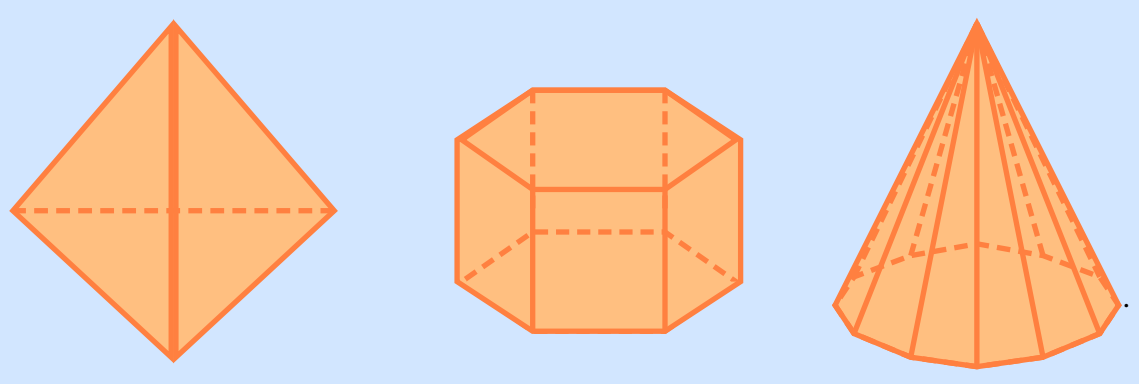
Der Begriff der Ordnung eines Elements ist ein erstes nützliches Hilfsmittel, um nichtisomorphe Gruppen voneinander zu unterscheiden: Gegeben seien zwei Gruppen G_1 und G_2 und ein Element $g \in G_1$ der Ordnung $n \in \{1, 2, 3, ...\} \cup \{\infty\}$. Wenn es in G_2 kein Element der Ordnung n gibt, dann können G_1 und G_2 nicht isomorph sein. Auf diese Weise haben wir bereits $\mathbb{Z}_4$ und $\mathbb{Z}_2 \times \mathbb{Z}_2$ unterschieden: In $\mathbb{Z}_4$ gibt es ein Element der Ordnung 4, während in $\mathbb{Z}_2 \times \mathbb{Z}_2$ jedes Element Ordnung 1 oder 2 hat.

II.4.19 Beispiel. Es seien $T \subset \mathbb{R}^3$ ein regelmäßiges Tetraeder, $G_1 = \mathrm{SO}(T)$ (s. Beispiel II.1.9, ii), $G_2 := D_6$, $E \subset \mathbb{R}^2$ ein regelmäßiges Zwölfeck und $G_3 = \mathrm{SO}(E)$. Diese Gruppen haben alle die Ordnung 12.

Die Gruppe G_3 ist zyklisch. Sie wird z.B. durch die Drehung um den Winkel $\pi/6$ erzeugt. In der Gruppe G_1 gibt es ein Element der Ordnung 1, drei Elemente der Ordnung 2 und acht Elemente der Ordnung 3. Es sei $r \in G_2$ die Drehung um den Winkel $\pi/3$. Die Gruppe G_2 enthält ein Element der Ordnung 1, sieben Elemente der Ordnung 2 (sechs Spiegelungen und r^3), zwei Elemente der Ordnung 3 (r^2 und r^4) und zwei Elemente der Ordnung 6 (r und r^5).

Da es in G_1 und G_2 kein Element der Ordnung 12 gibt, ist keine der beiden Gruppen isomorph zu G_3. Die Gruppe G_1 ist auch nicht isomorph zu G_2, weil G_1 kein Element der Ordnung 6 besitzt.

Wir können die drei Gruppen als spezielle Symmetriegruppen der folgenden dreidimensionalen geometrischen Gebilde auffassen:



Damit können wir die obigen algebraischen Rechnungen mit Hilfe unserer geometrischen Anschauung verstehen und erklären.

Der Satz von Cayley

II.4.20 Satz (Cayley[14]). *Für jede Gruppe G ist*

$$\begin{aligned} \varphi\colon G &\longrightarrow S(G) \\ g &\longmapsto \lambda_g \end{aligned}$$

ein injektiver Gruppenhomomorphismus.

II.4.21 Folgerung. *Es seien G eine endliche Gruppe und n die Anzahl ihrer Elemente. Dann ist G isomorph zu einer Untergruppe der symmetrischen Gruppe S_n.*

Beweis von Satz II.4.20. Es seien $g_1, g_2 \in G$ und $h \in H$. Wir berechnen

$$\lambda_{g_1 \cdot g_2}(h) = (g_1 \cdot g_2) \cdot h = g_1 \cdot (g_2 \cdot h) = g_1 \cdot \lambda_{g_2}(h) = \lambda_{g_1}(\lambda_{g_2}(h)) = (\lambda_{g_1} \circ \lambda_{g_2})(h).$$

Das bedeutet

$$\varphi(g_1 \cdot g_2) = \lambda_{g_1 \cdot g_2} = \lambda_{g_1} \circ \lambda_{g_2} = \varphi(g_1) \circ \varphi(g_2).$$

[14] Arthur Cayley (1821 - 1895), englischer Mathematiker.

Deshalb ist φ ein Gruppenhomomorphismus.

Zum Nachweis der Injektivität von φ benutzen wir das Kriterium aus Lemma II.4.5. Wenn $\lambda_g = \mathrm{id}_G$ für $g \in G$ gilt, dann folgt $e = \mathrm{id}_G(e) = \lambda_g(e) = g \cdot e = g$. Somit ist $\mathrm{Ker}(\varphi) = \{e\}$ gezeigt. □

II.4.22 Aufgabe (Die additive Gruppe von $\mathbb{Q}$). Beweisen Sie, dass $\mathbb{Q}$ nicht endlich erzeugt ist, d.h. für jede **endliche** Teilmenge $M \subset \mathbb{Q}$ gilt $\langle M \rangle \subsetneq \mathbb{Q}$.

II.5 Die symmetrische Gruppe

Es seien $n \geq 1$, $M := \{1, ..., n\}$ und $S_n = S(M) = \{\sigma \colon M \longrightarrow M \mid \sigma \text{ ist bijektiv}\}$. Die symmetrischen Gruppen S_n, $n \geq 1$, sind wichtige Beispiele für Gruppen. Sie haben den Vorteil, dass man in ihnen sehr explizit rechnen kann. Insbesondere können wir Begriffe wie die Ordnung eines Elements oder Erzeuger in diesen Gruppen untersuchen und dadurch greifbarer machen. Der Satz von Cayley zeigt weiter, dass die Berechnungen auch für das Studium beliebiger endlicher Gruppen hilfreich sein können.

Schreibweise. Es sei $\sigma \in S_n$ eine Permutation. Wir schreiben sie in der Form

$$\begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix}$$

oder kurz

$$(\sigma(1) \ \cdots \ \sigma(n)).$$

Die letzte Schreibweise werden wir im Folgenden vermeiden, weil sie mit der Zykelschreibweise (Definiton II.5.2, i) verwechselt werden kann.

II.5.1 Aufgabe. Zeigen Sie, dass $\#S_n = n!$ für $n \geq 1$ gilt.

Erzeuger für die symmetrische Gruppe

II.5.2 Definitionen. i) Es sei $k \geq 2$. Eine Permutation $\sigma \in S_n$ heißt *Zykel der Länge k*, wenn es eine Teilmenge $\{i_1, ..., i_k\} \subset \{1, ..., n\}$ von k verschiedenen Elementen gibt, so dass

$$\sigma(i) = \begin{cases} i, & \text{falls } i \notin \{i_1, ..., i_k\} \\ i_{l+1}, & \text{falls } i = i_l,\ l = 1, ..., k-1 \\ i_1, & \text{falls } i = i_k \end{cases}.$$

Schreibweise. $\sigma = (i_1 \ i_2 \ \cdots \ i_k)$.

ii) Ein Zykel der Länge 2 ist eine *Transposition*.

II.5.3 Beispiel. Der Zykel $\sigma = (5\ 7\ 3) \in S_7$ sieht in ausführlicher Schreibweise folgendermaßen aus:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 5 & 4 & 7 & 6 & 3 \end{pmatrix}.$$

II.5.4 Bemerkung. Ein Zykel $\sigma \in S_n$ der Länge k hat Ordnung k, $k \geq 2$.

II.5.5 Satz. *Die Zykel erzeugen S_n. Anders gesagt, zu $\sigma \in S_n$ existieren Zykel c_1, ..., c_s, so dass*

$$\sigma = c_1 \cdot \cdots \cdot c_s.$$

Beweis. Für eine Permutation $\sigma \in S_n \setminus \{e\}$ sei

$$m_\sigma := \min\{\, i = 1, ..., n \,|\, \sigma(i) \neq i \,\}.$$

Jetzt verwenden wir für $\sigma \in S_n$ den folgenden Algorithmus:

Schritt 1. Falls $\sigma = e$, so breche man den Algorithmus ab. Andernfalls sei

$$k := \min\{\, s \geq 1 \,|\, \sigma^s(m_\sigma) = m_\sigma \,\}.$$

Bemerkung. Für $1 \leq s_1 < s_2 \leq k$ gilt $\sigma^{s_1}(m_\sigma) \neq \sigma^{s_2}(m_\sigma)$. Aus $\sigma^{s_1}(m_\sigma) = \sigma^{s_2}(m_\sigma)$ wird nach Anwendung von σ^{-s_1} die Gleichung $m_\sigma = \sigma^{s_2-s_1}(m_\sigma)$. Wegen $1 \leq s_2 - s_1 < k$ ist das aber unmöglich.

Unsere Überlegungen zeigen, dass

$$c = (m_\sigma\ \sigma(m_\sigma)\ \cdots\ \sigma^{k-1}(m_\sigma))$$

ein Zykel der Länge k ist.

Schritt 2. Man bilde $c^{-1} \cdot \sigma$ und wende Schritt 2 auf $c^{-1} \cdot \sigma$ an.

Man erhält eine Folge $\sigma_1 := \sigma$, $\sigma_2 := c^{-1} \cdot \sigma$ usw. von Permutationen, für die $m_{\sigma_1} < m_{\sigma_2} < \cdots$ gilt. Deshalb bricht der Algorithmus ab. Wir haben somit Zykel c_1, ..., c_s gefunden, so dass

$$c_s^{-1} \cdot \cdots \cdot c_1^{-1} \cdot \sigma = e$$

gilt. Daraus folgt die Behauptung. □

II.5.6 Definition. Zwei Zykel $c_1 = (i_1\ \cdots\ i_k)$ und $c_2 = (j_1\ \cdots\ j_l)$ heißen *disjunkt*, falls

$$\forall \mu = 1, ..., k,\ \nu = 1, ..., l: \quad i_\mu \neq j_\nu.$$

In der folgenden Aufgabe werden weitere Eigenschaften der eben erhaltenen Zerlegung einer Permutation in Zykel bewiesen.

II.5.7 Aufgaben. a) Es seien c_1 und c_2 zwei disjunkte Zykel in S_n. Dann hat man $c_1 \cdot c_2 = c_2 \cdot c_1$.

b) Beweisen Sie folgende Aussage:

Satz. *Es seien c_1, ..., c_s und d_1, ..., d_t Zykel, so dass c_i und c_j für $1 \leq i < j \leq s$ und d_k und d_l für $1 \leq k < l \leq t$ disjunkt sind. Aus*

$$c_1 \cdot \cdots \cdot c_s = d_1 \cdot \cdots \cdot d_t$$

folgt

$$\{\, c_1, ..., c_s \,\} = \{\, d_1, ..., d_t \,\},$$

d.h. $s = t$ und die Zykel c_1, ..., c_s stimmen mit den Zykeln d_1, ..., d_s bis auf die Reihenfolge überein.

c) Leiten Sie das folgende Ergebnis ab:

Folgerung. *Jede Permutation $\sigma \in S_n \setminus \{e\}$ besitzt eine bis auf die Reihenfolge eindeutige Darstellung*

$$\sigma = c_1 \cdot \cdots \cdot c_s$$

als Produkt paarweise disjunkter Zykel.

II.5.8 Definition. Es sei $\sigma \in S_n \setminus \{e\}$. Das Tupel $\underline{n}_\sigma = (n_1, ..., n_s)$, das aus den Längen der Zykel in aufsteigender Reihenfolge einer Darstellung von σ als Produkt paarweise disjunkter Zykel besteht, heißt der *Zykeltyp* von σ.[15]

II.5.9 Beispiele. i) Wir wenden den im Beweis von Satz II.5.5 eingeführten Algorithmus auf die Permutation

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 1 & 6 & 7 & 3 & 5 & 4 & 2 \end{pmatrix}$$

an. Wir finden $c_1 = (1\ 8\ 2)$ und

$$c_1^{-1} \cdot \sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 6 & 7 & 3 & 5 & 4 & 8 \end{pmatrix}.$$

Als nächsten Zykel erhalten wir $c_2 = (3\ 6\ 5)$ und

$$c_2^{-1} \cdot c_1^{-1} \cdot \sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 7 & 5 & 6 & 4 & 8 \end{pmatrix}.$$

Die letzte Permutation ist die Transposition $c_3 = (4\ 7)$. Wir haben

$$\sigma = (1\ 8\ 2) \cdot (3\ 6\ 5) \cdot (4\ 7),$$

und der Zykeltyp von σ ist $\underline{n}_\sigma = (2, 3, 3)$.

ii) Wir haben

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 8 & 9 & 3 & 6 & 2 & 7 & 5 & 4 \end{pmatrix} = (2\ 8\ 5\ 6) \cdot (3\ 9\ 4)$$

und $\underline{n}_\sigma = (3, 4)$.

iii) Es gilt

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 8 & 6 & 1 & 9 & 10 & 2 & 7 & 3 & 12 & 5 & 4 & 11 \end{pmatrix} = (1\ 8\ 3) \cdot (2\ 6) \cdot (4\ 9\ 12\ 11) \cdot (5\ 10)$$

und $\underline{n}_\sigma = (2, 2, 3, 4)$. Wir können einen alternativen Algorithmus entwickeln, bei dem wir statt von links von rechts beginnen, also

$$\widetilde{m}_\sigma := \max\{\, i = 1, ..., n \,|\, \sigma(i) \neq i \,\}$$

usw. setzen. Das liefert die Zerlegung

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 8 & 6 & 1 & 9 & 10 & 2 & 7 & 3 & 12 & 5 & 4 & 11 \end{pmatrix} = (12\ 11\ 4\ 9) \cdot (10\ 5) \cdot (8\ 3\ 1) \cdot (6\ 2).$$

Bis auf die Reihenfolge ist dies natürlich dieselbe Zerlegung wie vorher.

II.5.10 Satz. *Die symmetrische Gruppe S_n wird von Transpositionen erzeugt.*

[15] Der Satz in Aufgabe II.5.7, b), impliziert, dass der Zykeltyp wohldefiniert ist.

Beweis. Es genügt zu zeigen, dass jeder Zykel σ als Produkt von Transpositionen geschrieben werden kann. Dies wird durch Induktion über die Länge k von σ getan.

$\boldsymbol{k = 2.}$ Nach Definition ist ein Zykel der Länge 2 eine Transposition.

$\boldsymbol{k \longrightarrow k + 1.}$ Es sei $\sigma = (i_1 \ \cdots \ i_{k+1})$. Dann ist

$$(i_1 \ \cdots \ i_{k+1}) \cdot (i_1 \ i_2) = (i_1 \ i_3 \ \cdots \ i_{k+1})$$

ein Zykel der Länge k und kann nach Induktionsvoraussetzung als Produkt von Zykeln geschrieben werden. Dasselbe folgt dann für $(i_1 \ \cdots \ i_{k+1})$. □

II.5.11 Bemerkung. Der Beweis zeigt

$$(i_1 \ \cdots \ i_{k+1}) = (i_1 \ i_{k+1}) \cdot \cdots \cdot (i_1 \ i_2)$$

für einen Zykel der Länge k.

II.5.12 Beispiele. Mit der obigen Bemerkung können wir die Permutationen aus Beispiel II.5.9 leicht als Produkte von Transpositionen schreiben:

i) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 1 & 6 & 7 & 3 & 5 & 4 & 2 \end{pmatrix} = (1\ 2) \cdot (1\ 8) \cdot (3\ 5) \cdot (3\ 6) \cdot (4\ 7),$

ii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 8 & 9 & 3 & 6 & 2 & 7 & 5 & 4 \end{pmatrix} = (2\ 6) \cdot (2\ 5) \cdot (2\ 8) \cdot (3\ 4) \cdot (3\ 9),$

iii) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 8 & 6 & 1 & 9 & 10 & 2 & 7 & 3 & 12 & 5 & 4 & 11 \end{pmatrix}$

$= (1\ 3) \cdot (1\ 8) \cdot (2\ 6) \cdot (4\ 11) \cdot (4\ 12) \cdot (4\ 9) \cdot (5\ 10)$

$= (12\ 9) \cdot (12\ 4) \cdot (12\ 11) \cdot (10\ 5) \cdot (8\ 1) \cdot (8\ 3) \cdot (6\ 2).$

II.5.13 Folgerungen. i) *Die Transpositionen* $(1\ 2)$, $(1\ 3)$, ..., $(1\ n)$ *erzeugen die symmetrische Gruppe* S_n.

ii) *Die Transpositionen* $(1\ 2)$, $(2\ 3)$, ..., $(n-1\ n)$ *erzeugen* S_n.

iii) *Die Transposition* $(1\ 2)$ *und der n-Zykel* $(1\ 2\ \cdots\ n)$ *erzeugen* S_n.

II.5.14 Bemerkung. Die Erzeugendensysteme in i) und ii) umfassen $n-1$ Elemente. Da S_n für $n \geq 3$ nicht abelsch und nach Bemerkung II.4.18, ii), damit auch nicht zyklisch ist, benötigt man mindestens zwei Elemente, um diese Gruppe zu erzeugen. Teil iii) der Folgerung gibt ein Erzeugendensystem mit zwei Elementen an.

Beweis der Folgerungen II.5.13. i) Für $1 \leq i_1 < i_2 \leq n$ gilt

$$(i_1 \ i_2) = (1 \ i_1) \cdot (1 \ i_2) \cdot (1 \ i_1). \tag{II.2}$$

Damit folgt die Behauptung aus Satz II.5.10.

ii) Für $k = 2, ..., n$ findet man die Formel

$$(1 \ k) = (k-1 \ k) \cdot (1 \ k-1) \cdot (k-1 \ k)$$

und durch Induktion

$$(1 \ k) = (k-1 \ k) \cdot \cdots \cdot (2\ 3) \cdot (1\ 2) \cdot (2\ 3) \cdot \cdots \cdot (k-1 \ k). \tag{II.3}$$

Zusammen mit i) ergibt sich die Behauptung.

iii) Für $k = 2, ..., n-1$ finden wir

$$(k\ k+1) = (1\ 2\ \cdots\ n) \cdot (k-1\ k) \cdot (1\ 2\ \cdots\ n)^{-1}$$

und somit

$$(k\ k+1) = (1\ 2\ \cdots\ n)^{k-1} \cdot (1\ 2) \cdot (1\ 2\ \cdots\ n)^{1-k}.$$

Wir schließen mit Teil ii). □

II.5.15 Bemerkung. Beispiel II.5.12 sowie die Formel (II.2) und (II.3) illustrieren, dass man ein gegebene Permutation auf vielfältige Weise als Produkt von Transpositionen darstellen kann.

II.5.16 Aufgaben (Rechnen in der symmetrischen Gruppe). a) Schreiben Sie die Permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 3 & 5 & 7 & 13 & 14 & 1 & 12 & 10 & 8 & 9 & 2 & 6 & 4 & 11 \end{pmatrix}$$

als Produkt disjunkter Zykel.

b) Stellen Sie die Permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 11 & 4 & 9 & 3 & 10 & 5 & 2 & 8 & 12 & 6 & 13 & 7 & 1 \end{pmatrix}$$

als Produkt von Transpositionen dar.

Das Vorzeichen einer Permutation

II.5.17 Definitionen. Es sei $\sigma \in S_n$ eine Permutation.

i) Ein Paar $(i\ j)$ mit $1 \le i < j \le n$ heißt *Fehlstand*, wenn $\sigma(i) > \sigma(j)$ gilt.

ii) Es sei $f(\sigma)$ die Anzahl der Fehlstände von σ.

iii) Man sagt, dass σ eine *gerade* bzw. *ungerade* Permutation ist, wenn $f(\sigma)$ gerade bzw. ungerade ist.

iv) Es sei

$$\begin{aligned} \mathrm{Sign}\colon S_n &\longrightarrow \{\pm 1\} \\ \sigma &\longmapsto \begin{cases} 1, & \text{falls } \sigma \text{ gerade} \\ -1, & \text{falls } \sigma \text{ ungerade} \end{cases}. \end{aligned}$$

Wir nennen $\mathrm{Sign}(\sigma)$ das *Vorzeichen* von σ.

II.5.18 Beispiel. Die Transposition (1 2) hat genau einen Fehlstand, so dass $\mathrm{Sign}(1\ 2) = -1$.

II.5.19 Satz. *Es seien $\sigma_1, \sigma_2 \in S_n$ zwei Permutationen. Dann gelten die folgenden Implikationen:*

$$\left.\begin{array}{c} \sigma_1 \text{ und } \sigma_2 \text{ gerade} \\ \text{oder} \\ \sigma_1 \text{ und } \sigma_2 \text{ ungerade} \end{array}\right\} \implies \sigma_1 \cdot \sigma_2 \text{ gerade},$$

$$\left.\begin{array}{c} \sigma_1 \text{ gerade, } \sigma_2 \text{ ungerade} \\ \text{oder} \\ \sigma_1 \text{ ungerade, } \sigma_2 \text{ gerade} \end{array}\right\} \implies \sigma_1 \cdot \sigma_2 \text{ ungerade}.$$

Das bedeutet, dass

$$\mathrm{Sign}(\sigma_1 \cdot \sigma_2) = \mathrm{Sign}(\sigma_1) \cdot \mathrm{Sign}(\sigma_2),$$

also dass

$$\mathrm{Sign}\colon S_n \longrightarrow \{\pm 1\}$$

ein Gruppenhomomorphismus ist.

Beweis. Aus der Definition des Vorzeichens leitet man unmittelbar

$$\forall \sigma \in S_n: \quad \mathrm{Sign}(\sigma) = \prod_{\substack{(i,j):\\ 1\le i<j\le n}} \frac{\sigma(i)-\sigma(j)}{i-j}$$

ab. Für $\sigma_1, \sigma_2 \in S_n$ berechnet man mit dieser Formel

$$\begin{aligned}
\mathrm{Sign}(\sigma_1\cdot\sigma_2) &= \prod_{\substack{(i,j):\\ 1\le i<j\le n}} \frac{(\sigma_1\cdot\sigma_2)(i)-(\sigma_1\cdot\sigma_2)(j)}{i-j} \\
&= \prod_{\substack{(i,j):\\ 1\le i<j\le n}} \frac{\sigma_1(\sigma_2(i))-\sigma_1(\sigma_2(j))}{i-j} \\
&= \prod_{\substack{(i,j):\\ 1\le i<j\le n}} \frac{\sigma_1(\sigma_2(i))-\sigma_1(\sigma_2(j))}{\sigma_2(i)-\sigma_2(j)} \cdot \prod_{\substack{(i,j):\\ 1\le i<j\le n}} \frac{\sigma_2(i)-\sigma_2(j)}{i-j} \\
&= \mathrm{Sign}(\sigma_1)\cdot\mathrm{Sign}(\sigma_2).
\end{aligned}$$

Somit ist nachgewiesen, dass Sign ein Homomorphismus ist. □

II.5.20 Beispiel. Aus (II.2), (II.3) und Beispiel II.5.18 schließen wir, dass jede Transposition das Vorzeichen -1 hat.

II.5.21 Folgerung. *Es seien $s, s' \ge 1$ und $\tau_1, \ldots, \tau_s, \tau'_1, \ldots, \tau'_{s'} \in S_n$ Transpositionen, so dass*

$$\tau_1 \cdot \cdots \cdot \tau_s = \tau'_1 \cdot \cdots \cdot \tau'_{s'}.$$

Dann ist $s - s'$ eine gerade ganze Zahl.

II.5.22 Definition. Die Gruppe

$$A_n := \mathrm{Ker}(\mathrm{Sign}) = \{\, \sigma \in S_n \mid \sigma \text{ ist gerade} \,\}$$

heißt die *alternierende Gruppe*.

II.5.23 Satz. i) *Die alternierende Gruppe A_n enthält genau $n!/2$ Elemente.*
ii) *Die alternierende Gruppe A_n wird von 3-Zykeln der Form $(1\ i_1\ i_2)$ erzeugt.*

Beweis. i) Es sei $\tau \in S_n$ eine Transposition. Dann haben wir:

- ⋆ $\tau \cdot A_n := \{\, \tau\cdot\sigma \mid \sigma \in A_n \,\} = \mathrm{Sign}^{-1}(-1)$.
- ⋆ $S_n = A_n \sqcup \tau \cdot A_n$. (D.h. $S_n = A_n \cup \tau\cdot A_n$ und $A_n \cap \tau\cdot A_n = \varnothing$.)
- ⋆ $\#A_n = \#(\tau\cdot A_n)$. (Nach Lemma II.2.1 ist $\lambda_\tau\colon S_n \longrightarrow S_n$, $\sigma \longmapsto \tau\cdot\sigma$, bijektiv.)

Aus diesen Beobachtungen ergibt sich

$$\#S_n = 2 \cdot \#A_n.$$

Diese Gleichung liefert wegen Aufgabe II.5.1 die Behauptung.

ii) Nach Satz II.5.10 erzeugen die Transpositionen $(1\ n)$, $n = 2, ..., n$, die Gruppe S_n, und nach Satz II.5.19 und Beispiel II.5.20 kann eine gerade Permutation nur als ein Produkt einer geraden Anzahl von Transpositionen geschrieben werden. Es gibt demnach Elemente $a_i, b_i \in \{2, ..., n\}$, $i = 1, ..., s$, so dass

$$\begin{aligned} \sigma &= (1\ a_1) \cdot (1\ b_1) \cdot \cdots \cdot (1\ a_s) \cdot (1 \cdot b_s) \\ &= (1\ b_1\ a_1) \cdot \cdots \cdot (1\ b_s\ a_s). \end{aligned}$$

Bei der Umformung haben wir Bemerkung II.5.11 verwendet. □

II.5.24 Beispiel. Für $n = 4$ findet man:

$$\begin{aligned} A_4 &= \{e, (1\ 2) \cdot (3\ 4), (1\ 3) \cdot (2\ 4), (1\ 4) \cdot (2\ 3), (1\ 2\ 3), (1\ 2\ 4), (1\ 3\ 4), (1\ 3\ 2), \\ &\quad (1\ 4\ 2), (1\ 4\ 3), (2\ 3\ 4), (2\ 4\ 3)\}, \\ S_4 \setminus A_4 &= \{(1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4), (1\ 2\ 3\ 4), (1\ 2\ 4\ 3), (1\ 3\ 2\ 4), \\ &\quad (1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2)\}. \end{aligned}$$

II.5.25 Aufgabe. Geben Sie das Vorzeichen der Permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 7 & 9 & 3 & 6 & 5 & 10 & 2 & 1 & 8 \end{pmatrix}$$

an.

II.5.26 Aufgabe (Vorzeichen und Determinante). a) Zeigen Sie, dass es zu jeder Permutation $\sigma \in S_n$ genau einen linearen Automorphismus $L_\sigma \colon \mathbb{R}^n \longrightarrow \mathbb{R}^n$ mit

$$L_\sigma(e_i) = e_{\sigma(i)}, \quad i = 1, ..., n,$$

gibt und dass

$$\begin{aligned} \iota \colon S_n &\longrightarrow \mathrm{GL}_n(\mathbb{R}) \\ \sigma &\longmapsto L_\sigma \end{aligned}$$

ein injektiver Gruppenhomomorphismus ist. (Dabei bezeichne $(e_1, ..., e_n)$ die Standardbasis des $\mathbb{R}^n$.)

b) Beweisen Sie

$$\forall \sigma \in S_n : \quad \mathrm{Sign}(\sigma) = (\mathrm{Det} \circ \iota)(\sigma) = \mathrm{Det}(L_\sigma).$$

Eine spielerische Anwendung

Auch die oben besprochenen Konstruktionen und Resultate können wir dazu einsetzen, ein bekanntes Spiel zu verstehen. Es handelt sich um das Schiebe-Puzzle mit 16 Feldern:

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

.

Frage. Ist die Stellung

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

möglich?

II.5.27 Satz. *Die Antwort lautet nein.*

Beweis. Wir stellen uns die Felder des Puzzles in den Farben Schwarz und Weiß eingefärbt und von 1 bis 16 durchnummeriert vor:

1	**2**	**3**	**4**
5	**6**	**7**	**8**
9	**10**	**11**	**12**
13	**14**	**15**	**16**

Jeder Zustand des Spiels entspricht einer Permutation:

- ⋆ Das Bild von i ist die Nummer des Felds, auf dem das Puzzle-Teil mit der Nummer i liegt, $i = 1, ..., 15$.
- ⋆ Das Bild von 16 ist die Nummer des freien Felds.

In jedem Schritt wird eine Permutation durchgeführt: Die Zahl unter dem freien Feld wird mit einer benachbarten Zahl vertauscht, z.B.

1	2	3	4
5	6	7	8
9		15	11
13	10	14	12

$\overset{(10\ 11)}{\rightsquigarrow}$

1	2	3	4
5	6	7	8
9	15		11
13	10	14	12

.

Dabei ist die Permutation, die einer gegebenen Stellung auf dem Spielfeld entspricht, genau dann gerade bzw. ungerade, wenn das freie Feld schwarz bzw. weiß ist.

Die in der Frage gezeigte Stellung entspricht einer Transposition, also einer ungeraden Permutation, und einer geraden Permutation, weil das freie Feld schwarz ist, und ist damit unmöglich. □

II.6 Gruppenwirkungen

Wenn eine Gruppe als Symmetriegruppe einer gewissen mathematischen Struktur definiert wird (vgl. Seite 27f), dann hilft die zugrundeliegende mathematische Struktur, die Gruppe zu analysieren und zu verstehen. Beispiele für dieses Vorgehen sind:

- ⋆ Es sei $M \subset \mathbb{R}^2$ oder $\subset \mathbb{R}^3$ eine „Figur“. Dann können wir unsere geometrische Anschauung dieser Figur nutzen, um ihre Symmetriegruppe zu begreifen. Auf diese Weise haben wir schnell alle Elemente der Diedergruppe und der Symmetriegruppe eines Tetraeders aufgefunden (Beispiel II.1.9, i) und ii).

- ⋆ Es seien k ein Körper und $G = \mathrm{GL}_n(k)$, $\mathrm{O}_n(k)$ oder $\mathrm{SO}_n(k)$. Hier haben wir die Mittel der linearen Algebra und, für $k = \mathbb{R}$ oder $\mathbb{C}$, auch diejenigen der Analysis zur Verfügung. In Satz II.1.6 und II.1.7 haben wir so die Gruppen $\mathrm{O}_2(\mathbb{R})$ und $\mathrm{O}_3(\mathbb{R})$ beschrieben. Ein weiteres wichtiges Hilfsmittel für $k = \mathbb{C}$ ist die Theorie der Jordanschen Normalform (s. [20], §54; [5], Abschnitt 4.6). Mit ihr werden wir weiter unten (Seite 73f) die Konjugationsklassen in $\mathrm{GL}_n(\mathbb{C})$ angeben.

Ein möglicher Ansatz für das Studium „abstrakter“ Gruppen ist daher, sie als Symmetriegruppen zu realisieren oder mit Symmetriegruppen in Verbindung zu bringen. Dieser Ansatz wird mit dem Begriff der Gruppenwirkung formalisiert. Zudem beinhaltet dieser Begriff auch wichtige Spezialfälle wie den der Konjugation. Damit gelangen wir auch zu neuen Gegenständen für die weitere Forschung.

II.6.1 Definitionen. Es seien G eine Gruppe und M eine nichtleere Menge.

i) Eine (*Links-*)*Wirkung* von G auf M ist eine Abbildung

$$\begin{aligned} \sigma\colon G \times M &\longrightarrow M \\ (g, m) &\longmapsto \sigma(g, m), \end{aligned}$$

so dass gilt:

a) $\forall m \in M : \sigma(e, m) = m$.

b) $\forall g_1, g_2 \in G,\ m \in M : \sigma(g_1 \cdot g_2, m) = \sigma\big(g_1, \sigma(g_2, m)\big)$.

ii) Eine *Rechtswirkung* von G auf M ist eine Abbildung

$$\begin{aligned} \varrho\colon M \times G &\longrightarrow M \\ (m, g) &\longmapsto \varrho(m, g), \end{aligned}$$

so dass gilt:

a) $\forall m \in M : \varrho(m, e) = m$.

b) $\forall g_1, g_2 \in G,\ m \in M : \varrho(m, g_1 \cdot g_2) = \varrho\big(\varrho(m, g_1), g_2\big)$.

Schreibweise. In i) schreiben wir kurz $g \cdot m$ für $\sigma(g, m)$ und in ii) $m \cdot g$ für $\varrho(m, g)$. Die obigen Axiome lauten in dieser Notation:

i) a) $\forall m \in M : e \cdot m = m.$
b) $\forall g_1, g_2 \in G,\ m \in M : (g_1 \cdot g_2) \cdot m = g_1 \cdot (g_2 \cdot m).$
ii) a) $\forall m \in M : m \cdot e = m.$
b) $\forall g_1, g_2 \in G,\ m \in M : m \cdot (g_1 \cdot g_2) = (m \cdot g_1) \cdot g_2.$

II.6.2 Bemerkungen. i) Es sei $\sigma\colon G \times M \longrightarrow M$ eine Linkswirkung der Gruppe G auf der Menge M. Für $g \in G$ sei

$$\begin{array}{rcl} \sigma_g\colon M & \longrightarrow & M \\ m & \longmapsto & g \cdot m. \end{array}$$

Behauptung. *Die Abbildung σ_g ist bijektiv.*

Beweis. Wir betrachten die Abbildung $\sigma_{g^{-1}}$. Mit a) und b) gilt:

$$\forall m \in M : \quad (\sigma_{g^{-1}} \circ \sigma_g)(m) = g^{-1} \cdot (g \cdot m) \overset{\text{b)}}{=} (g^{-1} \cdot g) \cdot m = e \cdot m \overset{\text{a)}}{=} m.$$

Diese Berechnung zeigt $\sigma_{g^{-1}} \circ \sigma_g = \mathrm{id}_M$. Entsprechend verifiziert man $\sigma_g \circ \sigma_{g^{-1}} = \mathrm{id}_M$. Also ist σ_g bijektiv (vgl. Seite 27). □

Damit erhalten wir die Abbildung

$$\begin{array}{rcl} \widetilde{\sigma}\colon G & \longrightarrow & S(M) \\ g & \longmapsto & \sigma_g. \end{array}$$

Auf Grund von Axiom b) ist $\widetilde{\sigma}$ ein Gruppenhomomorphismus.

Ist umgekehrt ein Gruppenhomomorphismus

$$\widetilde{\sigma}\colon G \longrightarrow S(M)$$

gegeben, so ist

$$\begin{array}{rcl} \sigma\colon G \times M & \longrightarrow & M \\ (g, m) & \longmapsto & \widetilde{\sigma}(g)(m) \end{array}$$

eine Linkswirkung von G auf M.

Wir halten also fest, dass wir eine Entsprechung zwischen den Linkswirkungen von G auf M und den Gruppenhomomorphismen $G \longrightarrow S(M)$ aufgefunden haben.

ii) Für eine Rechtswirkung $\varrho\colon M \times G \longrightarrow M$ der Gruppe G auf der Menge M und $g \in G$ setzen wir

$$\begin{array}{rcl} \varrho_g\colon M & \longrightarrow & M \\ m & \longmapsto & m \cdot g. \end{array}$$

Wie in i) überprüft man, dass ϱ_g bijektiv ist und dass[16]

$$\begin{array}{rcl} \widetilde{\varrho}\colon G & \longrightarrow & S(M)^{\mathrm{op}} \\ g & \longmapsto & \varrho_g \end{array}$$

ein Homomorphismus ist.

Auf diese Weise wird eine Korrespondenz zwischen den Rechtswirkungen von G auf M und den Gruppenhomomorphismen $G \longrightarrow S(M)^{\mathrm{op}}$ hergestellt.

[16] s. Aufgabe II.1.13 für die Definition der entgegengesetzten Gruppe.

Wenn eine Gruppe G als Symmetriegruppe einer gewissen mathematischen Struktur $(M, \cdots)$ definiert wird, dann wirkt G auf natürliche Weise von links auf der Menge M, auf der die Struktur aufgebaut ist. Dies belegen wir mit einigen Beispielen.

II.6.3 Beispiele. i) Es sei M eine Menge. Dann ist

$$\begin{array}{rcl} \sigma\colon S(M)\times M & \longrightarrow & M \\ (f,m) & \longmapsto & f(m) \end{array}$$

eine Wirkung von $S(M)$ auf M. Sie gehört zum Homomorphismus $\widetilde{\sigma} = \mathrm{id}_{S(M)}\colon S(M) \longrightarrow S(M)$.

ii) Es sei k ein Körper. Für $G = \mathrm{GL}_n(k)$, $\mathrm{O}_n(k)$ oder $\mathrm{SO}_n(k)$ ist

$$\begin{array}{rcll} \sigma\colon G\times k^n & \longrightarrow & k^n & \\ (g,v) & \longmapsto & g\cdot v & \text{(Matrixprodukt)} \end{array}$$

eine Linkswirkung von G auf k^n. Für jedes Gruppenelement $g \in G$ ist $\sigma_g\colon k^n \longrightarrow k^n$ in diesem Fall eine lineare Abbildung, und der zugehörige Homomorphismus $\widetilde{\sigma}\colon G \longrightarrow S(k^n)$ ist die natürliche Inklusion.

iii) Aus den Wirkungen in ii) kann man Wirkungen auf weiteren Mengen konstruieren. Seien z.B. $0 < l < n$ und

$$\mathrm{Gr}(l,n) := \{\, V \subset k^n \mid V \text{ ist Unterraum der Dimension } l \,\}.$$

Für $V \in \mathrm{Gr}(l,n)$ und $g \in G$ sei

$$g\cdot V := \{\, g\cdot v \mid v \in V \,\}.$$

Dann ist

$$\begin{array}{rcl} G\times \mathrm{Gr}(l,n) & \longrightarrow & \mathrm{Gr}(l,n) \\ (g,V) & \longmapsto & g\cdot V \end{array}$$

eine Linkswirkung von G auf $\mathrm{Gr}(l,n)$.

iv) Es seien k ein Körper, $M \subset k^n$ und $G = \mathrm{O}(M)$ oder $\mathrm{SO}(M)$. Die Abbildung

$$\begin{array}{rcl} G\times M & \longrightarrow & M \\ (f,m) & \longmapsto & f(m) \end{array}$$

ist eine Linkswirkung von G auf M.

v) Es seien G eine Gruppe und $H \subset G$ eine Untergruppe. Die Abbildung

$$\begin{array}{rcl} H\times G & \longrightarrow & G \\ (h,g) & \longmapsto & h\cdot g \end{array}$$

ist eine Linkswirkung von H auf G und

$$\begin{array}{rcl} G\times H & \longrightarrow & G \\ (g,h) & \longmapsto & g\cdot h \end{array}$$

eine Rechtswirkung. Ein Beispiel ist $\mathbb{Z} \subset \mathbb{R}$, das zu der Wirkung

$$\begin{array}{rcl} \mathbb{Z} \times \mathbb{R} & \longrightarrow & \mathbb{R} \\ (k, x) & \longmapsto & k + x \end{array}$$

führt.

vi) Eine andere Wirkung von $\mathbb{Z}$ auf $\mathbb{R}$ ist durch die Abbildung

$$\begin{array}{rcl} \mathbb{Z} \times \mathbb{R} & \longrightarrow & \mathbb{R} \\ (k, x) & \longmapsto & (-1)^k \cdot x \end{array}$$

gegeben.

Wir entwickeln jetzt weitere Begriffe und Resultate für Gruppenwirkungen. Wir beschränken uns dabei meist auf Linkswirkungen. Die Leserin bzw. der Leser möge die Übertragung auf Rechtswirkungen selbstständig durchführen.

II.6.4 Definitionen. Es seien G eine Gruppe, M eine nichtleere Menge, $\sigma\colon G \times M \longrightarrow M$ eine Wirkung von G auf M und $x \in M$.

i) Die *Bahn* oder der *Orbit* von x ist die Menge

$$G \cdot x := \{\, g \cdot x \in M \mid g \in G \,\}.$$

ii) Die *Standgruppe* oder der *Stabilisator* von x ist

$$G_x := \{\, g \in G \mid g \cdot x = x \,\}.$$

II.6.5 Bemerkung. Die Standgruppe G_x ist eine Untergruppe von G.

II.6.6 Beispiele. i) Es seien k ein Körper, $G = \mathrm{GL}_n(k)$, $M = k^n$ und

$$\begin{array}{rcl} \sigma\colon \mathrm{GL}_n(k) \times k^n & \longrightarrow & k^n \\ (g, v) & \longmapsto & g \cdot v. \end{array}$$

Wir betrachten $x = e_1$. Die Bahn von e_1 ist $k^n \setminus \{0\}$: Für $v = (v_1, ..., v_n)^t \in k^n \setminus \{0\}$ sei $i \in \{\, 1, ..., n \,\}$ ein Index mit $v_i \neq 0$. Dann ist $v, e_1, ..., e_{i-1}, e_{i+1}, ..., e_n$ eine Basis für k^n, und man hat

$$v = (v|e_1|\cdots|e_{i-1}|e_{i+1}|\cdots|e_n) \cdot v = \left(\begin{array}{c|c|c|c|c|c|c} v_1 & & & & & & \\ \vdots & e_1 & \cdots & e_{i-1} & e_{i+1} & \cdots & e_n \\ v_n & & & & & & \end{array}\right) \cdot e_1.$$

Die Standgruppe von e_1 ist

$$\mathrm{GL}_n(k)_{e_1} = \left\{ \left(\begin{array}{c|ccc} 1 & \lambda_2 & \cdots & \lambda_n \\ \hline 0 & & & \\ \vdots & & g & \\ 0 & & & \end{array}\right) \;\middle|\; \lambda_2, ..., \lambda_n \in k,\ g \in \mathrm{GL}_{n-1}(k) \right\}.$$

Die Bahn des Nullvektors 0 ist $\{0\}$ und sein Stabilisator ist $\mathrm{GL}_n(k)$. Der Vektorraum k^n zerfällt somit in zwei $\mathrm{GL}_n(k)$-Bahnen.

ii) Es seien k ein Körper, $0 < l < n$, $G = \mathrm{GL}_n(k)$, $M = \mathrm{Gr}(l,n)$ und

$$\begin{array}{rcl} \sigma\colon \mathrm{GL}_n(k) \times \mathrm{Gr}(l,n) & \longrightarrow & \mathrm{Gr}(l,n) \\ (g,V) & \longmapsto & g \cdot V. \end{array}$$

Weiter sei $W = \langle e_1, ..., e_l \rangle$. Man findet $\mathrm{GL}_n(k) \cdot W = \mathrm{Gr}(l,n)$ (Übung) und für die Standgruppe

$$\mathrm{GL}_n(k)_W = \left\{ \left(\begin{array}{c|c} g_1 & m \\ \hline 0 & g_2 \end{array} \right) \middle| g_1 \in \mathrm{GL}_l(k),\ g_2 \in \mathrm{GL}_{n-l}(k),\ m \in \mathrm{Mat}(l, n-l; k) \right\}.$$

Insbesondere gilt für $l = 1$ und $W = \langle e_1 \rangle$

$$\mathrm{GL}_n(k)_W = \left\{ \left(\begin{array}{c|ccc} \lambda_1 & \lambda_2 & \cdots & \lambda_n \\ \hline 0 & & & \\ \vdots & & g & \\ 0 & & & \end{array} \right) \middle| \lambda_1 \in k^\star,\ \lambda_2, ..., \lambda_n \in k,\ g \in \mathrm{GL}_{n-1}(k) \right\}.$$

iii) Es seien $n \geq 1$, $G = S_n$, $M = \{1, ..., n\}$ und

$$\begin{array}{rcl} S_n \times \{1, ..., n\} & \longrightarrow & \{1, ..., n\} \\ (\sigma, i) & \longmapsto & \sigma(i). \end{array}$$

Es gilt $S_n \cdot n = \{1, ..., n\}$, denn man hat z.B. $k = (k\ n) \cdot n$, $k = 1, ..., n-1$. Die Standgruppe von n ist

$$(S_n)_n = \left\{ \left(\begin{array}{cccc} 1 & \cdots & n-1 & n \\ \sigma(1) & \cdots & \sigma(n-1) & n \end{array} \right) \middle| \sigma \in S_{n-1} \right\} \cong S_{n-1}.$$

II.6.7 Definition. Es seien G eine Gruppe, M eine Menge und $\sigma\colon G \times M \longrightarrow M$ eine Wirkung von G auf M. Für $x, y \in M$ schreiben wir

$$x \sim y \quad :\Longleftrightarrow \quad \exists g \in G : x = g \cdot y \quad \Longleftrightarrow \quad x \in G \cdot y.$$

II.6.8 Lemma. *Die Relation „$\sim$“ auf $M \times M$ ist eine Äquivalenzrelation.*

Beweis. Für die **Reflexivität** beachte man, dass

$$\forall x \in M : \quad x = e \cdot x.$$

Die zeigt $x \sim x$, $x \in M$.

Die **Symmetrie** ergibt sich folgendermaßen: Es seien $x, y \in M$, so dass $x \sim y$. Es gibt also ein Element $g \in G$ mit $x = g \cdot y$. Es folgt

$$g^{-1} \cdot x = g^{-1} \cdot (g \cdot y) = (g^{-1} \cdot g) \cdot y = e \cdot y = y$$

und somit $y \sim x$.

Abschließend ist die **Transitivität** nachzuweisen. Gegeben seien also $x, y, z \in M$ mit $x \sim y$ und $y \sim z$. Daher können wir Elemente $g, h \in G$ mit $x = g \cdot y$ und $y = h \cdot z$ finden. Die Gleichung

$$x = g \cdot y = g \cdot (h \cdot z) = (g \cdot h) \cdot z$$

liefert $x \sim z$. □

II.6.9 Bemerkung. Die Äquivalenzklassen für „$\sim$“ sind gerade die Bahnen.

II.6.10 Beispiele. i) Es seien G eine Gruppe, $H \subset G$ eine Untergruppe und

$$\begin{aligned} \sigma\colon H \times G &\longrightarrow G \\ (h, g) &\longmapsto h \cdot g. \end{aligned}$$

Die Äquivalenzklasse von $g \in G$ ist die sogenannte *Rechtsnebenklasse*

$$H \cdot g = \{\, h \cdot g \in G \mid h \in H \,\}.$$

Die Menge aller Rechtsnebenklassen wird mit $H\backslash G$ bezeichnet.[17]

ii) Für G und H wie in i) müssen wir auch die Rechtswirkung

$$\begin{aligned} \varrho\colon G \times H &\longrightarrow H \\ (g, h) &\longmapsto g \cdot h \end{aligned}$$

betrachten. Wir erhalten auch hier eine Äquivalenzrelation. Die Äquivalenzklassen sind die *Linksnebenklassen*

$$[g] := g \cdot H = \{\, g \cdot h \in G \mid h \in H \,\}, \quad g \in G.$$

Wir schreiben G/H für die Menge der Linksnebenklassen.

iii) Es sei $n \in \mathbb{Z}$. Wir betrachten $G = \mathbb{Z}$ und $H := n \cdot \mathbb{Z}$. Da $\mathbb{Z}$ abelsch ist, liefern die in i) und ii) definierten Wirkungen dieselbe Äquivalenzrelation auf $\mathbb{Z}$. In den Bezeichnungen von ii) überprüft man

$$\forall k, k' \in \mathbb{Z}: \quad [k] = [k'] \quad \Longleftrightarrow \quad k \equiv k' \bmod n.$$

iv) In der Situation von i) und ii) ist

$$\begin{aligned} \lambda\colon G \times G/H &\longrightarrow G/H \\ (g, [g']) &\longmapsto [g \cdot g'] = (g \cdot g') \cdot H \end{aligned}$$

eine Linkswirkung von G auf G/H. Es gilt $G \cdot [e] = G/H$ und $G_{[e]} = H$.

II.6.11 Beobachtung. *In Beispiel* II.6.10, iv), *gilt*

$$\forall g \in G: \quad G_{[g]} = g \cdot H \cdot g^{-1}.$$

Beweis. Zunächst überprüfen wir die Inklusion „$\supset$“: Sei $h \in H$. Dann gilt

$$(g \cdot h \cdot g^{-1}) \cdot [g] = \big[(g \cdot h \cdot g^{-1}) \cdot g\big] = [g \cdot h] = [g].$$

Für den Beweis von „$\subset$“ sei $g' \in G_{[g]}$. Wir berechnen

$$(g^{-1} \cdot g' \cdot g) \cdot [e] = \big[(g^{-1} \cdot g') \cdot g\big] = (g^{-1} \cdot g') \cdot [g] = g^{-1} \cdot (g' \cdot [g]) = g^{-1} \cdot [g] = [g^{-1} \cdot g] = [e].$$

Dies zeigt $g^{-1} \cdot g' \cdot g \in G_{[e]} = H$, so dass es ein $h \in H$ mit $g^{-1} \cdot g' \cdot g = h$ gibt. Damit folgt $g' = g \cdot h \cdot g^{-1} \in g \cdot H \cdot g^{-1}$. □

[17] Bitte sorgfältig von der Mengendifferenz unterscheiden!

Diese Beobachtung legt für eine Gruppe G die Betrachtung folgender Abbildung nahe:

$$\begin{aligned} c\colon G\times G &\longrightarrow G\\ (g,h) &\longmapsto g\cdot h\cdot g^{-1}. \end{aligned}$$

II.6.12 Lemma. *Die Abbildung c ist eine Linkswirkung von G auf G.*

Beweis. Übung. □

II.6.13 Definition. Wir nennen c die Linkswirkung von G auf sich durch *Konjugation*.

II.6.14 Bemerkung. Für $g\in G$ ist

$$\begin{aligned} c_g\colon G &\longrightarrow G\\ h &\longmapsto g\cdot h\cdot g^{-1} \end{aligned}$$

ein **Gruppenautomorphismus**, i.e. ein Gruppenisomorphismus von G auf sich. Sei

$$\mathrm{Aut}(G)=\{\,\varphi\colon G\longrightarrow G\,|\,\varphi \text{ ist ein Gruppenautomorphismus}\,\}.$$

Dies ist eine Untergruppe von $S(G)$. Die Wirkung c entspricht dem Homomorphismus

$$\begin{aligned} \widetilde{c}\colon G &\longrightarrow \mathrm{Aut}(G)\subset S(G)\\ g &\longmapsto c_g. \end{aligned}$$

II.6.15 Definition. Das Bild von $\widetilde{c}$ wird mit $\mathrm{Inn}(G)$ bezeichnet. Ein Element $\varphi\in\mathrm{Inn}(G)$ wird *innerer Automorphismus* genannt, ein Element $\varphi\in\mathrm{Aut}(G)\setminus\mathrm{Inn}(G)$ *äußerer Automorphismus*.

II.6.16 Bemerkung. Ein Homomorphismus $\varphi\colon G\longrightarrow G$ ist genau dann ein innerer Homomorphismus, wenn es ein Element $g\in G$ gibt, so dass

$$\forall h\in G:\quad \varphi(h)=g\cdot h\cdot g^{-1}.$$

Die zuvor eingeführten Objekte erhalten im Fall der Wirkung c durch Konjugation besondere Namen:

II.6.17 Definitionen. Es seien G eine Gruppe und $c\colon G\times G\longrightarrow G$ die Linkswirkung von G auf sich durch Konjugation.

i) Zwei Elemente $x,y\in G$ sind *konjugiert*, wenn ein $g\in G$ mit

$$y=c_g(x)=g\cdot x\cdot g^{-1}$$

existiert.

ii) Für ein Element $x\in G$ ist seine *Konjugationsklasse* durch

$$\begin{aligned} \varkappa(x) &:= \{\,g\cdot x\cdot g^{-1}\in G\,|\,g\in G\,\}\\ &= \{\,y\in G\,|\,y \text{ ist konjugiert zu } x\,\} \end{aligned}$$

gegeben.

iii) Der *Zentralisator* von $x \in G$ ist die Untergruppe

$$\begin{aligned} C_G(x) &:= \{ g \in G \mid c_g(x) = x \} \\ &= \{ g \in G \mid g \cdot x \cdot g^{-1} = x \} \\ &= \{ g \in G \mid g \cdot x = x \cdot g \} \end{aligned}$$

aller Elemente in G, die mit x kommutieren.

iv) Das *Zentrum* von G ist die Untergruppe

$$\begin{aligned} Z(G) &:= \operatorname{Ker}(\widetilde{c}) \\ &= \{ g \in G \mid \forall x \in G : g \cdot x = x \cdot g \} \\ &= \bigcap_{x \in G} C_G(x). \end{aligned}$$

II.6.18 Bemerkungen. i) Abelsche Gruppen sind einfacher als nichtabelsche Gruppen. Das Zentrum einer Gruppe G ist ein Maß dafür, „wie abelsch“ G ist. Wenn das Zentrum groß ist, dann ist G „nahe dran“, abelsch zu sein. Ist es klein, z.B. $Z(G) = \{e\}$, dann ist G sehr weit entfernt davon, abelsch zu sein.

ii) Für eine Gruppe G und ein Element $x \in G$ ist $C_G(x)$ die größte Untergruppe von G, die x in ihrem Zentrum enthält.

Es seien G eine Gruppe und

$$\mathfrak{U} := \{ H \subset G \mid H \text{ ist eine Untergruppe} \}.$$

Für jedes Element $g \in G$ ist $c_g \colon G \longrightarrow G$ ein Gruppenautomorphismus. Folglich ist $c_g(H)$ für jede Untergruppe H von G wieder eine Untergruppe von G (Lemma II.4.4). Als „abstrakte“ Gruppen sind H und $c_g(H)$ isomorph. Wir erhalten die Linkswirkung

$$\begin{aligned} c_{\mathfrak{U}} \colon G \times \mathfrak{U} &\longrightarrow \mathfrak{U} \\ (g, H) &\longmapsto c_g(H). \end{aligned}$$

II.6.19 Definition. Es sei G eine Gruppe. Die Untergruppen H und H' von G sind *konjugiert*, wenn ein Element $g \in G$ mit

$$H = c_g(H') = g \cdot H' \cdot g^{-1}$$

vorhanden ist.

II.6.20 Aufgabe (Gruppenwirkungen). Für die folgenden Beispiele einer Gruppe G, einer Menge M, eines Elements $g \in G$ und eines Elements $x \in M$ ist das Element $g \cdot x$ anzugeben. Dabei sei die Gruppenwirkung $\sigma \colon G \times M \longrightarrow M$ die in der Vorlesung eingeführte.

a) $G := S_7$, $M := \{ 1, ..., 7 \}$, $g := (1\ 3\ 6) \cdot (3\ 5)$, $x := 5$.

b) $G := \mathrm{O}_2(\mathbb{R})$, $M := \mathbb{R}^2$, g die Drehung um den Winkel $\pi/4$, $x := \begin{pmatrix} 1 \\ 1 \end{pmatrix}$.

c) $G = \mathrm{GL}_2(\mathbb{R})$, $M := \mathbb{R}^2$, $g := \begin{pmatrix} 3 & -5 \\ 2 & 11 \end{pmatrix}$, $x := \begin{pmatrix} 4 \\ -3 \end{pmatrix}$.

II.6.21 Aufgabe (Wirkungen von $\mathbb{R}$ auf $\mathbb{C}$). a) Zeigen Sie, dass durch

$$\begin{aligned} \sigma\colon \mathbb{R}\times\mathbb{C} &\longrightarrow \mathbb{C} \\ (t,z) &\longmapsto \exp(t)\cdot z \end{aligned}$$

eine Linkswirkung von $\mathbb{R}$ auf $\mathbb{C}$ gegeben ist. Geben Sie für jede komplexe Zahl z die Bahn $\mathbb{R}\cdot z$ und die Standgruppe $\mathbb{R}_z$ an. Fertigen Sie eine Skizze der Bahnen an.

b) Es sei

$$\begin{aligned} \sigma\colon \mathbb{R}\times\mathbb{C} &\longrightarrow \mathbb{C} \\ (t,z) &\longmapsto \exp(i\cdot t)\cdot z. \end{aligned}$$

Weisen Sie nach, dass σ eine Linkswirkung von $\mathbb{R}$ auf $\mathbb{C}$ ist, und geben Sie für jede komplexe Zahl z die Bahn $\mathbb{R}\cdot z$ und die Standgruppe $\mathbb{R}_z$ an. Skizzieren Sie die Bahnen.

II.6.22 Aufgabe (Wirkung einer Untergruppe von S_8). Es sei

$$\sigma := (1\ 2\ 3)\cdot(5\ 6\ 7\ 8) \in S_8.$$

a) Bestimmen Sie die Ordnung von σ.

b) Es seien $G := \langle\sigma\rangle \subset S_8$ und

$$\begin{aligned} \Gamma\colon G\times\{1,2,3,4,5,6,7,8\} &\longrightarrow \{1,2,3,4,5,6,7,8\} \\ (\sigma^i, j) &\longmapsto \sigma^i(j). \end{aligned}$$

Geben Sie für jedes der Elemente 1, 4 und 5 seine G-Bahn und seine Standgruppe in G an.

II.6.23 Aufgabe (Links- vs. Rechtswirkungen). Es seien G eine Gruppe, M eine Menge,

$$\sigma\colon G\times M \longrightarrow M$$

eine Linkswirkung von G auf M und

$$\varrho\colon M\times G \longrightarrow G$$

eine Rechtswirkung. Weiter seien

$$\begin{aligned} \sigma^\star\colon M\times G &\longrightarrow M \\ (m,g) &\longmapsto \sigma(g^{-1},m) \end{aligned}$$

und

$$\begin{aligned} \varrho^\star\colon G\times M &\longrightarrow M \\ (g,m) &\longmapsto \varrho(m,g^{-1}). \end{aligned}$$

Zeigen Sie, dass $\sigma^\star$ bzw. $\varrho^\star$ eine Rechts- bzw. Linkswirkung von G auf M ist. Vergleichen Sie die Bahnen und Standgruppen bzgl. σ mit denen bzgl. $\sigma^\star$.

II.6.24 Aufgabe (Das Zentrum). a) Es seien k ein Körper und $n \geq 1$. Bestimmen Sie das Zentrum von $\mathrm{GL}_n(k)$.

b) Geben Sie für $n \geq 1$ das Zentrum der symmetrischen Gruppe S_n an.

II.6.25 Aufgabe (Innere und äußere Automorphismen). a) Zeigen Sie, dass eine Gruppe G genau dann abelsch ist, wenn alle ihre inneren Automorphismen trivial sind.

b) Geben Sie ein Beispiel für eine Gruppe G und einen **äußeren** Automorphismus $\varphi\colon G \longrightarrow G$ an.

Konjugationsklassen

Die Zerlegung einer Gruppe in ihre Konjugationsklassen ist ein wertvolles Hilfsmittel zur Untersuchung einer Gruppe. Man sucht für jede Konjugationsklasse einen Repräsentanten, an dem man möglichst viel Information ablesen kann.

In der linearen Algebra beschäftigt man sich mit der Linkswirkung

$$\begin{aligned} c\colon \mathrm{GL}_n(\mathbb{C}) \times M_n(\mathbb{C}) &\longrightarrow M_n(\mathbb{C}) \\ (g, m) &\longmapsto g \cdot m \cdot g^{-1}. \end{aligned}$$

Zwei Matrizen m und m' sind *ähnlich*, wenn ein $g \in \mathrm{GL}_n(\mathbb{C})$ mit

$$m = g \cdot m' \cdot g^{-1}$$

existiert.

Die **Jordansche Normalform**[18] liefert in jeder Bahn einen Repräsentanten. Gegeben seien $\lambda \in \mathbb{C}$, $1 \le k$ und $1 \le k_1 \le \cdots \le k_s$. Man setze

$$J_k(\lambda) := \begin{pmatrix} \lambda & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda \end{pmatrix} \in M_k(\mathbb{C})$$

und

$$J_{k_1,\ldots,k_s}(\lambda) := \left(\begin{array}{c|c|c} J_{k_1}(\lambda) & 0 & \\ \hline 0 & \ddots & 0 \\ \hline & \ddots & 0 \\ 0 & \hline 0 & J_{k_s}(\lambda) \end{array}\right) \in M_{k_1+\cdots+k_s}(\mathbb{C}).$$

Seien $m \in M_n(\mathbb{C})$ und $\lambda_1, \ldots, \lambda_t$ die verschiedenen Eigenwerte von m. Dann gibt es Zahlen $k_{i1} \le \cdots \le k_{is_i}$, $i = 1, \ldots, t$, mit $\sum_{i=1}^{t} \sum_{j=1}^{s_i} k_{ij} = n$, so dass m der Matrix

$$\left(\begin{array}{c|c|c} J_{k_{11},\ldots,k_{1s_1}}(\lambda_1) & 0 & \\ \hline 0 & \ddots & 0 \\ \hline & \ddots & 0 \\ 0 & \hline 0 & J_{k_{t1},\ldots,k_{ts_t}}(\lambda_t) \end{array}\right) \tag{II.4}$$

ähnlich ist. Eine Matrix wie in (II.4) ist genau dann invertierbar, wenn $\lambda_i \neq 0$, $i = 1, \ldots, t$. Die Konjugationsklassen in $\mathrm{GL}_n(\mathbb{C})$ werden also durch Blockmatrizen parametrisiert, die sich aus Jordan-Blöcken zu nichttrivialen Eigenwerten zusammensetzen.

Im Folgenden beschreiben wir die Konjugationsklassen in der symmetrischen Gruppe S_n, $n \ge 1$. Es seien $(i_1 \ \cdots \ i_k) \in S_n$ ein Zykel der Länge k und $\sigma \in S_n$. Dann gilt

$$\sigma \cdot (i_1 \ \cdots \ i_k) \cdot \sigma^{-1} = (\sigma(i_1) \ \cdots \ \sigma(i_k)). \tag{II.5}$$

[18] Marie Ennemond Camille Jordan (1838 - 1922), französischer Mathematiker.

Jede zu $(i_1 \ \cdots \ i_k)$ konjugierte Permutation ist wiederum ein Zykel der Länge k. Außerdem sieht man mit (II.5), dass zwei Zykel der Länge k konjugiert sind.

Es seien weiter $\varphi \in S_n$ und $c_1, ..., c_s \in S_n$ paarweise disjunkte Zykel, so dass

$$\varphi = c_1 \cdot \cdots \cdot c_s.$$

Für $\sigma \in S_n$ haben wir

$$\sigma \cdot \varphi \cdot \sigma^{-1} = (\sigma \cdot c_1 \cdot \sigma^{-1}) \cdot \cdots \cdot (\sigma \cdot c_s \cdot \sigma^{-1}).$$

Daran erkennen wir

II.6.26 Lemma. *Zwei konjugierte Permutationen haben denselben Zykeltyp.*

II.6.27 Satz. *Für gegebene Permutationen $\varphi, \varphi' \in S_n$ sind folgende Aussagen äquivalent:*

i) *Die Permutationen φ und φ' sind konjugiert.*

ii) *Die Permutationen φ und φ' haben denselben Zykeltyp.*

Beweis. Die Implikation „i)$\Longrightarrow$ii)“ haben wir bereits begründet. Für „ii)$\Longrightarrow$i)“ seien $\underline{n}_\varphi = (n_1, ..., n_s) = \underline{n}_{\varphi'}$ der Zykeltyp und $n_{s+1} := n - (n_1 + \cdots + n_s)$. Es seien c_i bzw. d_i Zykel der Länge n_i, $i = 1, ..., s$, so dass c_i und c_j bzw. d_i und d_j für $1 \le i < j \le s$ paarweise disjunkt sind und

$$\varphi = c_1 \cdot \cdots \cdot c_s \quad \text{und} \quad \varphi' = d_1 \cdot \cdots \cdot d_s$$

gilt. Wir schreiben

$$c_i = (l_1^i \ \cdots \ l_{n_i}^i) \quad \text{bzw.} \quad d_i = (m_1^i \ \cdots \ m_{n_i}^i), \quad i = 1, ..., s.$$

Weiter gibt es Zahlen $l_1^{s+1} < \cdots < l_{n_{s+1}}^{s+1}$ bzw. $m_1^{s+1} < \cdots < m_{n_{s+1}}^{s+1}$, so dass

$$\begin{aligned} \{\, 1, ..., n \,\} &= \{\, l_1^1, ..., l_{n_1}^1 \,\} \sqcup \cdots \sqcup \{\, l_1^s, ..., l_{n_s}^s \,\} \sqcup \{\, l_1^{s+1}, ..., l_{n_{s+1}}^{s+1} \,\} \\ &= \{\, m_1^1, ..., m_{n_1}^1 \,\} \sqcup \cdots \sqcup \{\, m_1^s, ..., m_{n_s}^s \,\} \sqcup \{\, m_1^{s+1}, ..., m_{n_{s+1}}^{s+1} \,\}. \end{aligned}$$

Es gibt somit genau eine Permutation $\sigma \in S_n$ mit

$$\sigma(l_j^i) = m_j^i, \quad j = 1, ..., n_i, \ i = 1, ..., s+1.$$

Gleichung (II.5) zeigt

$$(m_1^i \ \cdots \ m_{n_i}^i) = \sigma \cdot (l_1^i \ \cdots \ l_{n_i}^i) \cdot \sigma^{-1}, \quad i = 1, ..., s,$$

und somit $\sigma \cdot \varphi \cdot \sigma^{-1} = \varphi'$. □

II.6.28 Aufgabe (Vorzeichen und Ordnung eines Zykels). a) Es sei $c \in S_n$ ein Zykel der Länge k. Berechnen Sie das Vorzeichen $\mathrm{Sign}(c)$.

b) Welche Ordnung hat ein Zykel $c \in S_n$ der Länge k?

c) Es seien $\sigma \in S_n$ eine Permutation und $\underline{n} = (n_1, ..., n_s)$ ihr Zykeltyp. Welche Ordnung hat σ?

II.7 Der Satz von Lagrange und Anwendungen

Es seien M eine nichtleere Menge, G eine Gruppe und $\sigma\colon G \times M \longrightarrow M$ eine Wirkung von G auf M.

II.7.1 Lemma. *Für $x \in M$ und $g \in G$ gilt*

$$G_{g\cdot x} = g \cdot G_x \cdot g^{-1}$$

und damit insbesondere

$$G_{g\cdot x} \cong G_x.$$

Beweis. Übung (vgl. Beobachtung II.6.11). □

II.7.2 Satz. *In der obigen Situation seien G und M endlich. Dann gilt*

$$\#G = (\#G_x) \cdot (\#G \cdot x).$$

Beweis. Wir führen die Bahnabbildung

$$\begin{array}{rccc} \mathrm{Orb}_x\colon & G & \longrightarrow & G \cdot x \\ & g & \longmapsto & g \cdot x \end{array}$$

ein. Sie ist offenbar surjektiv. Es seien $s := \#G \cdot x$ und $G \cdot x = \{ x_1, ..., x_s \}$. Es folgt

$$G = \bigsqcup_{i=1}^{s} \mathrm{Orb}_x^{-1}(x_i)$$

und deswegen

$$\#G = \sum_{i=1}^{s} \#\mathrm{Orb}_x^{-1}(x_i). \tag{II.6}$$

Wir fixieren Elemente $g_1, ..., g_s \in G$ mit $x_i = g_i \cdot x$, $i = 1, ..., s$. Damit gilt

$$\begin{aligned} \mathrm{Orb}_x^{-1}(x_i) &= \{ h \in G \mid h \cdot x = g_i \cdot x \} \\ &= \{ h \in G \mid g_i^{-1} \cdot h \cdot x = x \} \\ &= \{ h \in G \mid g_i^{-1} \cdot h \in G_x \} \\ &= g_i \cdot G_x, \quad i = 1, ..., s. \end{aligned}$$

Es folgt

$$\#\mathrm{Orb}_x^{-1}(x_i) = \#(g_i \cdot G_x) = \#G_x, \quad i = 1, ..., s.$$

Die letzte Gleichung folgt aus Lemma II.2.1. Somit wird aus (II.6)

$$\#G = s \cdot \#G_x = (\#G \cdot x) \cdot (\#G_x).$$

Dies ist die behauptete Gleichung. □

II.7.3 Bemerkung. Die Abbildung

$$\begin{array}{rcl} G/G_x & \longrightarrow & G \cdot x \\ g \cdot G_x & \longmapsto & g \cdot x \end{array}$$

ist wohldefiniert und bijektiv. Auf Grund des Satzes gilt

$$\#G = \#(G/G_x) \cdot \#G_x.$$

II.7.4 Folgerung (Satz von Lagrange[19]). *Es seien G eine endliche Gruppe und H eine Untergruppe. Dann gilt*

$$\#G = \#H \cdot \#(G/H).$$

Insbesondere hat man

$$\#H | \#G.$$

Beweis. Wir betrachten die Abbildung

$$\begin{array}{rcl} G \times (G/H) & \longrightarrow & G/H \\ (g, [h]) & \longmapsto & [g \cdot h] \end{array}$$

aus Beispiel II.6.10, iv). Es gilt $G \cdot [e] = G/H$ und $G_{[e]} = H$. Also ist die Behauptung ein Spezialfall von Satz II.7.2. □

II.7.5 Folgerung. *Es seien G eine endliche Gruppe und $g \in G$. Dann gilt*

$$\mathrm{Ord}(g) | \#G.$$

Beweis. Es sei $n = \mathrm{Ord}(g) = \min\{\, k \geq 1 \mid g^k = e \,\}$. Dann ist

$$\langle g \rangle = \{\, e, g, g^2, ..., g^{n-1} \,\}$$

eine zyklische Untergruppe von G mit n Elementen. Nach Folgerung II.7.4 gilt $n | \#G$. □

II.7.6 Folgerung. *Es seien p eine Primzahl und G eine endliche Gruppe der Ordnung p. Dann ist G zyklisch (und damit isomorph zu $\mathbb{Z}_p$).*

Beweis. Es sei $g \in G \setminus \{e\}$. Dann haben wir

- ⋆ $\mathrm{Ord}(g) > 1$,
- ⋆ $\mathrm{Ord}(g) | p$.

Das bedeutet $\mathrm{Ord}(g) = p = \#G$ und folglich $\langle g \rangle = G$. □

II.7.7 Bemerkung. Wir haben jetzt alle endlichen Gruppen bis einschließlich Ordnung 5 klassifiziert:

Ordnung	1	2	3	4	5
Gruppen	$\{e\}$	$\mathbb{Z}_2$	$\mathbb{Z}_3$	$\mathbb{Z}_4,\ \mathbb{Z}_2 \times \mathbb{Z}_2$	$\mathbb{Z}_5$

Sie sind sämtlich abelsch.

[19] Joseph-Louis de Lagrange (geb. als Giuseppe Lodovico Lagrangia; 1736 - 1813), italienischer Mathematiker und Astronom.

Nun beweisen wir eine interessante Verallgemeinerung der letzten Folgerung:

II.7.8 Satz. *Es seien p eine Primzahl, $n \geq 1$ und G eine endliche Gruppe der Ordnung p^n. Dann ist das Zentrum von G nichttrivial, d.h.*

$$\#Z(G) > 1.$$

Beweis. Es seien $C_1, ..., C_s$ die verschiedenen Konjugationsklassen in G. Wir nummerieren so, dass $C_1 = \varkappa(e) = \{e\}$. Dann gilt:

- $\star$ $\#C_i > 1 \Longrightarrow p|\#C_i$, $i = 2, ..., s$. (Das folgt aus Satz II.7.2, weil C_i eine Bahn ist, $i = 2, ..., s$.)
- $\star$ $G = C_1 \sqcup \cdots \sqcup C_s$ und daher $\#C_1 + \cdots + \#C_s = 1 + \#C_2 + \cdots + \#C_s$.

Da $p|\#G$ aber $p \nmid 1$, muss es einen Index $i_0 \in \{2, ..., s\}$ mit $p \nmid \#C_{i_0}$ geben. Nach der obigen Diskussion bedeutet das $\#C_{i_0} = 1$. Sei $x \in G \setminus \{e\}$ mit $C_{i_0} = \varkappa(x) = \{x\}$. Die Gleichung $\varkappa(x) = \{x\}$ bedeutet $x \in Z(G)$. □

II.7.9 Aufgabe. Es seien $m, n > 0$ positive ganze Zahlen, so dass

$$\mathrm{ggT}(m, n) = 1.$$

Zeigen Sie, dass das Element $(1, 1) \in \mathbb{Z}_m \times \mathbb{Z}_n$ Ordnung $m \cdot n$ hat und folgern Sie

$$\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{m \cdot n}.$$

Die Anzahl der Bahnen

II.7.10 Definition. Es seien M eine nichtleere Menge, G eine Gruppe, $\sigma\colon G \times M \longrightarrow M$ eine Wirkung von G auf M und $g \in G$. Dann ist

$$M^g := \mathrm{Fix}(g) := \{\, x \in M \mid g \cdot x = x \,\}$$

die *Fixpunktmenge* von g.

II.7.11 Satz. *In der obigen Situation seien G und M endlich. Dann haben wir*

$$\textit{Anzahl der Bahnen in } M = \frac{1}{\#G} \cdot \sum_{x \in M} \#G_x = \frac{1}{\#G} \cdot \sum_{g \in G} \#M^g.$$

Beweis. **Schritt 1.** Aus Satz II.7.2 wissen wir, dass für jeden Punkt $x \in M$

$$\#G = (\#G \cdot x) \cdot (\#G_x). \tag{II.7}$$

Seien s die Anzahl der Bahnen und $x_1, ..., x_s \in M$, so dass $G \cdot x_1$, ..., $G \cdot x_s$ diese Bahnen sind. Mit

$$M = G \cdot x_1 \sqcup \cdots \sqcup G \cdot x_s$$

leiten wir

$$s \cdot \#G = \sum_{i=1}^{s} (\#G \cdot x_i) \cdot (\#G_{x_i}) = \sum_{x \in M} \#G_x.$$

aus (II.7) ab. (Bei der letzten Umformung haben wir die Tatsache benutzt, dass $G_x \cong G_y$, wenn x und y in derselben Bahn liegen (s. Lemma II.7.1).) Diese Gleichung zeigt bereits

$$s = \frac{1}{\#G} \cdot \sum_{x \in M} G_x.$$

Schritt 2. Es sei

$$\begin{aligned} \Delta &= \{(g,x) \in G \times M \mid g \cdot x = x\} \\ &= \{(g,x) \in G \times M \mid g \in G_x\} \\ &= \{(g,x) \in G \times M \mid x \in M^g\}. \end{aligned}$$

Mit den beiden letzten Beschreibungen von Δ gelangen wir zu der Identität

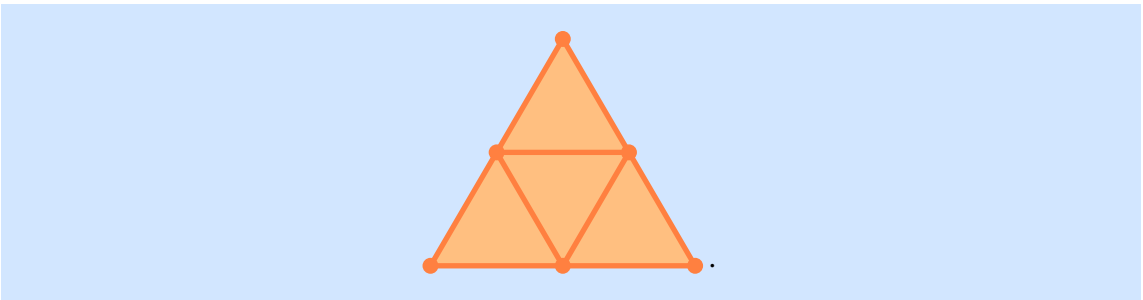
$$\#\Delta = \sum_{x \in M} \#G_x = \sum_{g \in G} \#M^g.$$

Zusammen mit Schritt 1 ergibt sich die Aussage des Satzes. □

II.7.12 Aufgabe (Wichteln). An einer Weihnachtsfeier nehmen n Personen teil. Jede bringt ein Geschenk mit. Am Ende der Feier werden die Geschenke zufällig an die TeilnehmerInnen verteilt. Wieviele Personen erhalten im Durchschnitt ihr eigenes Geschenk?
(Es handelt sich um eine Frage zu den Fixpunktmengen einer geeigneten Gruppenwirkung.)

Färbungsprobleme

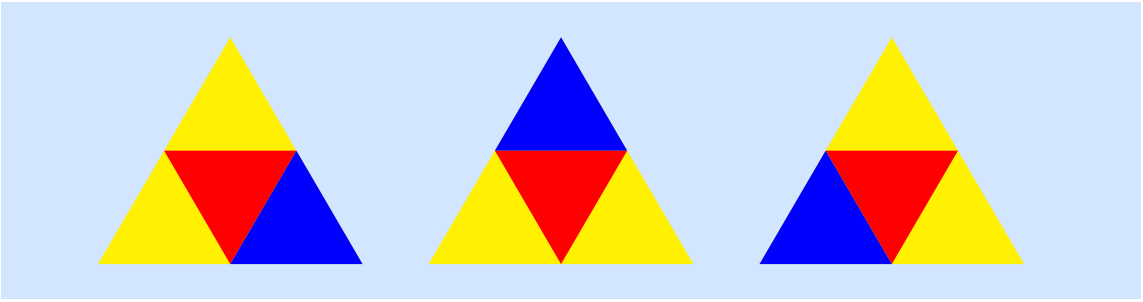
Ein gleichseitiges Dreieck werde in vier gleichgroße Dreiecke unterteilt:



Frage. Wieviele **wesentlich verschiedenene** Möglichkeiten gibt es, die vier Dreiecke in den Farben blau, gelb und rot einzufärben?

Dabei nennen wir zwei Färbungen *wesentlich verschieden*, wenn sie nicht durch eine Drehung ineinander überführt werden können.

Um diese Problemstellung zu verstehen, kann man sich das Dreieck als Fliese vorstellen. Dann macht es z.B. offenkundig keinen Sinn, zwischen den Färbungen

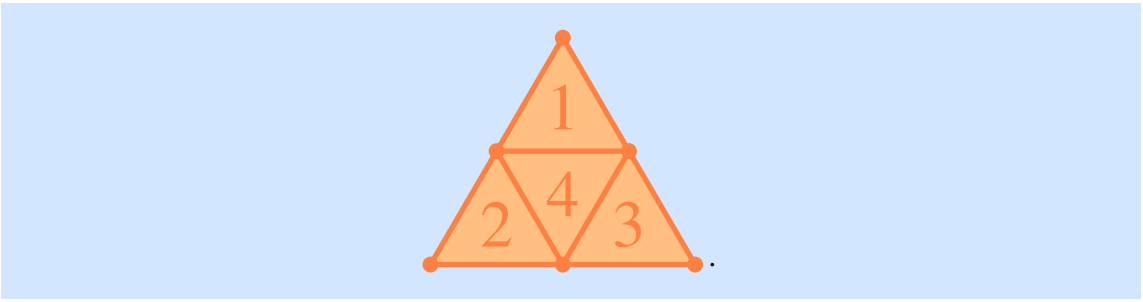


zu unterscheiden.

Wir modellieren das Färbungsproblem als Wirkung von $\mathbb{Z}_3 = \{0, 1, 2\}$ auf der Menge

$$M = \{ f : \{1, 2, 3, 4\} \longrightarrow \{B, G, R\} \}.$$

Dabei seien die Felder des Dreiecks folgendermaßen nummeriert:



Man beachte

$$\#G = 3 \quad \text{und} \quad \#M = 3^4 = 81.$$

Wir stellen folgende Tabelle auf

g	M^g	$\#M^g$
0	M	81
1	Alle Färbungen, bei denen 1, 2 und 3 dieselbe Farbe haben	9
2	dto.	9

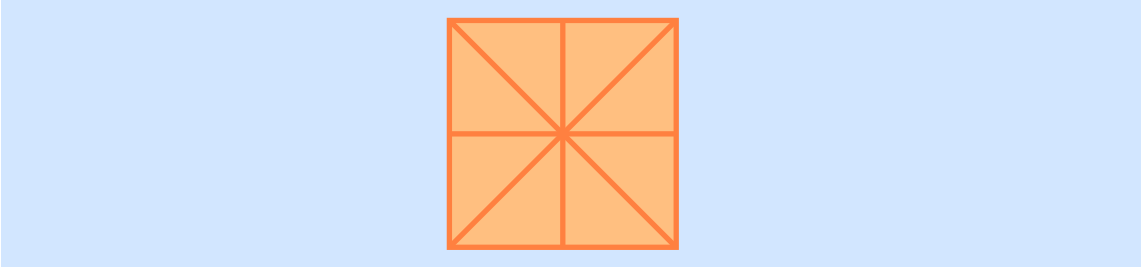
.

Mit Satz II.7.11 finden wir

$$s = \frac{1}{3} \cdot (81 + 9 + 9) = 33$$

als Anzahl der wesentlich verschiedenen Färbungen.

Jetzt wollen wir



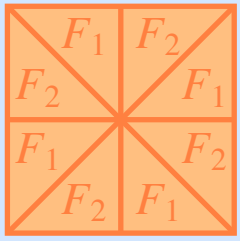
färben. Diesmal sehen wir zwei Färbungen als *wesentlich verschieden* an, wenn sie nicht durch eine Drehung **oder eine Spiegelung** ineinander transformiert werden können. Um dies mit unserer Anschauung in Einklang zu bringen, stellen wir uns eine aus Glas gefertigte Fliese vor. Diese können wir nicht nur in der Ebene drehen, sondern auch spiegeln, indem wir sie umdrehen. Wir lassen in unseren Betrachtungen eine beliebige Zahl n von Farben zu. Die wirkende Gruppe ist $G = D_4$ mit $\#G = 8$ und

$$M = \{ f : \{ 1, 2, 3, 4, 5, 6, 7, 8 \} \longrightarrow \{ 1, ..., n \} \}$$

mit $\#M = n^8$. Wir zählen die Fixpunkte für die verschiedenen Elemente von G ab. Dabei seien r die Drehung um den Winkel $\pi/2$ und s die Spiegelung an der x-Achse.

i) Für das Neutralelement e sind alle Färbungen Fixpunkte, also $\#M^e = n^8$.

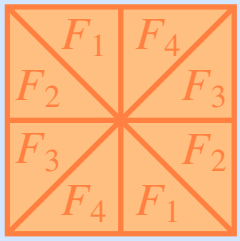
ii) Für die beiden Drehungen $g = r$ und $g = r^3$ muss die Fliese auf folgende Weise eingefärbt werden:



.

Folglich gilt $\#M^g = n^2$.

iii) Für die Drehung $g = r^2$ der Ordnung 2 muss wie folgt gefärbt werden:



.

Somit gilt $\#M^g = n^4$.

iv) Für die Spiegelungen $g \in \{ s, r \cdot s, r^2 \cdot s, r^3 \cdot s \}$ finden wir jeweils n^4 Elemente in M^g.

Zusammengenommen erhalten wir

$$s = \frac{1}{8} \cdot (n^8 + 5 \cdot n^4 + 2 \cdot n^2)$$

wesentlich verschiedene Färbungen. Wir können weitere Detailfragen stellen, z.B.

Frage. Wieviele wesentlich verschiedene Färbungen gibt es mit sechs blauen und zwei gelben Feldern?

Wie zuvor bilden wir M mit $n = 2$. Wir müssen die beiden Felder auswählen, die gelb gefärbt werden. Deshalb definieren wir

$$P := \{ N \subset \{ 1, 2, 3, 4, 5, 6, 7, 8 \} \mid \#N = 2 \}.$$

Man beachte

$$\#P = \binom{8}{2} = \frac{8 \cdot 7}{2} = 28.$$

In den oben untersuchenten Fällen i) - iv) erhalten wir folgende Werte für $\#P^g$:

i)	ii)	iii)	iv)
28	0	4	4

Es ergeben sich

$$s = \frac{1}{8} \cdot (28 + 5 \cdot 4) = 6$$

wesentlich verschiedene Färbungen mit sechs blauen und zwei gelben Feldern.

Als drittes Beispiel betrachten wir die möglichen Färbungen der Seiten eines regulären Tetraeders unter der Wirkung der speziellen Symmetriegruppe $\mathrm{SO}(T)$. Wir legen also die Gruppe $G = \mathrm{SO}(T)$ mit 12 Elementen und die Menge

$$M = \{ f : \{1, 2, 3, 4\} \longrightarrow \{1, ..., n\} \}$$

mit n^4 Elementen zugrunde. Wir gehen für die Berechnung von $\#M^g$ die verschiedenen Elemente von G durch (vgl. Beispiel II.1.9, ii).

i) Für $g = e$ haben wir $\#M^g = n^4$.

ii) Für eine der acht Drehungen der Ordnung 3 müssen die drei Seiten, die die Ecke, durch die die Drehachse verläuft, enthalten, mit derselben Farbe gefärbt werden. Daher finden wir n^2 Elemente in M^g.

iii) Es sei g eine der drei Drehungen der Ordnung zwei. Ihre Drehachse verläuft durch die Mittelpunkte zweier gegenüberliegender Kanten K_1 und K_2. Die beiden Seiten, die K_1 enthalten, und die beiden, die K_2 enthalten, müssen jeweils in derselben Farbe eingefärbt werden. Wir finden n^2 Elemente in M^g.

Mit den gesammelten Informationen ermitteln wir die Zahl

$$s = \frac{1}{12} \cdot (n^4 + 11 \cdot n^2)$$

als Anzahl der wesentlich verschiedenen Färbungen.

II.7.13 Bemerkungen. i) Geometrische Probleme wie dasjenige des Tetraeders treten auch in der Chemie auf. Dort möchte man die Anzahl der möglichen Moleküle, die sich aus vorgegebenen Atomen zusammensetzen, bestimmen (s. [8], S. 164ff).

ii) In den obigen Berechnungen haben wir die zweite Formel für s in Satz II.7.11 verwendet, denn auf Grund der einfachen Geometrie der Probleme war es uns leicht möglich, die Mengen M^g, $g \in G$, abzuzählen.

II.7.14 Aufgabe (Ein Färbungsproblem). Eine Kette soll aus sechs Perlen gefertigt werden. Die Perlen stehen in den Farben 1, ..., n zur Verfügung.

a) Welche Symmetriegruppe benutzt man sinnvollerweise, um verschiedene Ketten zu identifizieren?

b) Bestimmen Sie die Anzahl der wesentlich verschiedenen Ketten, die man herstellen kann.

c) Geben Sie die Anzahl der wesentlich verschiedenen Ketten an, die aus drei weißen und drei schwarzen Perlen bestehen.

II.8 Endliche Drehgruppen

Im Folgenden beschreiben wir die endlichen Untergruppen von O(2) und SO(3). Die bereits mehrfach beobachtete Übersetzung von algebraischen Rechnungen in geometrische Strukturen tritt hier besonders deutlich zu Tage. Im Fall von SO(3) erhalten wir dabei eine gruppentheoretische Herleitung der Klassifikation der platonischen Körper.

Endliche Untergruppen von O(2)

II.8.1 Satz. *Es sei $G \subset \mathrm{O}(2)$ eine endliche Untergruppe. Dann gibt es ein $n \geq 1$, so dass G zu $\mathbb{Z}_n$ oder zu D_n isomorph ist.*

Beweis. **Fall 1.** Wir setzen zunächst $G \subset \mathrm{SO}(2)$ voraus. Nach Satz II.1.6 sind alle Elemente von G Drehungen. Seien $n = \#G$ und $g \in G$. Wir haben bereits $\mathrm{Ord}(g)|n$ bewiesen (Folgerung II.7.5). Es folgt

$$g^n = (g^{\mathrm{Ord}(g)})^{\frac{n}{\mathrm{Ord}(g)}} = e^{\frac{n}{\mathrm{Ord}(g)}} = e.$$

Dem Element g können wir somit diejenige Zahl $k(g) \in \{1, ..., n\}$ zuweisen, für die g die Drehung um den Winkel $2\pi \cdot k(g)/n$ ist. Seien weiter

$$k := \min\{\, k(g) \mid g \in G \,\}$$

und g_0 die Drehung um den Winkel $2\pi \cdot k/n$. Für $g \in G$ schreiben wir

$$k(g) = l \cdot k + r \quad \text{mit } l \geq 1 \text{ und } r \in \{0, ..., k-1\}.$$

Das Element $g_0^{-l} \cdot g \in G$ ist die Drehung um den Winkel $2\pi \cdot r/n$. Die Definition von k zeigt wegen $0 \leq r < k$, dass $r = 0$ und folglich $g = g_0^l$. Damit ist $G = \langle g_0 \rangle \cong \mathbb{Z}_n$ bewiesen.

Fall 2. Wir nehmen $G \not\subset \mathrm{SO}(2)$ an und fixieren $s \in G \setminus \mathrm{SO}(2)$. Weiter sei r ein Erzeuger der Untergruppe $G \cap \mathrm{SO}(2)$ von G. Man überlegt sich sofort, dass

$$G = \{\, e, ..., r^{n-1}, s, r \cdot s, ..., r^{n-1} \cdot s \,\}, \quad n := \mathrm{Ord}(r).$$

Für $n = 1$ folgt $G \cong \mathbb{Z}_2$ und andernfalls $G \cong D_n$. □

Endliche Untergruppen von SO(3)

II.8.2 Satz. *Es sei $G \subset \mathrm{SO}(3)$ eine endliche Untergruppe. Dann ist G zu einer der folgenden Gruppen isomorph:*

- ⋆ $\mathbb{Z}_n$, $n \geq 1$,
- ⋆ D_n, $n \geq 2$,
- ⋆ $\mathrm{SO}(T)$, $T \subset \mathbb{R}^3$ *ein reguläres Tetraeder,*
- ⋆ $\mathrm{SO}(O)$, $O \subset \mathbb{R}^3$ *ein reguläres Oktaeder,*
- ⋆ $\mathrm{SO}(I)$, $I \subset \mathbb{R}^3$ *ein reguläres Ikosaeder.*

II.8.3 Bemerkung. Die spezielle Symmetriegruppe $\mathrm{SO}(O)$ ist isomorph zur speziellen Symmetriegruppe $\mathrm{SO}(W)$ eines Würfels $W \subset \mathbb{R}^3$. Ebenso ist $\mathrm{SO}(I)$ zur speziellen Symmetriegruppe $\mathrm{SO}(D)$ eines regulären Dodekaeders $D \subset \mathbb{R}^3$ isomorph (vgl. Bemerkung und Beispiel II.8.9, ii).

Im Beweis des obigen Satzes werden wir zunächst eine endliche Menge M konstruieren, auf der G in geeigneter Weise wirkt, und dann Satz II.7.11 anwenden. Auf diese Weise werden wir Aussagen über die Geometrie der Bahnen treffen können. Dabei spielen auch die Norm $\|\cdot\|$ auf $\mathbb{R}^3$ und die Tatsache, dass $\mathrm{SO}(3)$ diese Norm invariant lässt, eine wichtige Rolle. Wir verwenden also:

$$\star \quad \begin{array}{rcl} \|\cdot\|\colon \mathbb{R}^3 & \longrightarrow & \mathbb{R}^3 \\ (x,y,z) & \longmapsto & \sqrt{x^2+y^2+z^2}\,, \end{array}$$

$\star$ $S^2 = \{\,(x,y,z) \in \mathbb{R}^3 \mid \|(x,y,z)\| = 1\,\}$.

Es sei $\varrho \in \mathrm{SO}(3) \setminus \{e\}$. Dann ist ϱ nach Satz II.1.7 eine Drehung um eine eindeutig bestimmte Gerade $\gamma_\varrho \subset \mathbb{R}^3$ durch den Nullpunkt.

II.8.4 Hilfssatz. *Es seien $G \subset \mathrm{SO}(3)$ eine Untergruppe und $q \in \mathbb{R}^3 \setminus \{0\}$.*

i) *Es gilt $G_{-q} = G_q$.*

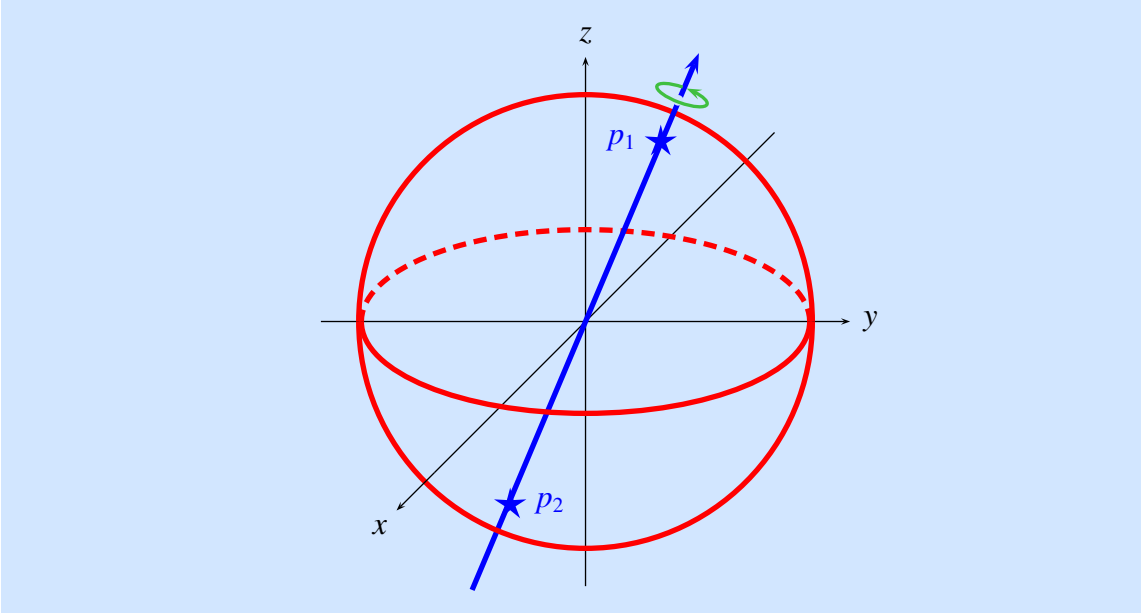
ii) *Wenn die Standgruppe G_q endlich ist, dann ist sie zyklisch. Für jeden Punkt $p \in \mathbb{R}^3$, der nicht auf der Gerade durch 0 und q liegt, ist die Bahn $(G_q) \cdot p$ ein regelmäßiges n-Eck in einer Ebene, die senkrecht auf der Geraden durch 0 und q steht, $n := \#G_q$.*

Beweis. i) Die Standgruppe von q besteht aus denjenigen Drehungen $\varrho \in G$, deren Drehachse γ_ϱ die Gerade durch 0 und q ist. Diese Gerade ist auch als die Gerade durch q und $-q$ oder durch 0 und $-q$ gekennzeichnet. Damit folgt die Behauptung.

ii) Nach i) ist G_q eine endliche Gruppe von Drehungen mit derselben Drehachse, und zwar der Geraden durch 0 und q. Die Elemente von G_q sind daher durch die Angabe des Drehwinkels bestimmt. Die Aussage kann deshalb wie Fall 1 im Beweis von Satz II.8.1 gezeigt werden. Es sei $n := \#G_q$. Wir fixieren eine Orientierung der Geraden γ durch 0 und q. Damit wird der mathematisch positive Drehsinn um γ (vgl. Abbildung II.1) festgelegt. Es sei ϱ die Drehung um γ um den Winkel $2\pi/n$ im mathematisch positiven Sinn. Diese Drehung erzeugt G_q. Ein Punkt $p \notin \gamma$ definiert eine Ebene E, die p enthält und senkrecht auf γ steht. Die Bahn $(G_q) \cdot p$ ist nun offensichtlich ein regelmäßiges n-Eck in der Ebene E. □

II.8.5 Bemerkung. In ii) haben je zwei Punkte der Bahn $(G_q) \cdot p$ denselben Abstand von q.

Es seien $G \subset \mathrm{SO}(3)$ eine Untergruppe und $\varrho \in G \setminus \{e\}$. Die Gerade γ_ϱ schneidet die Sphäre S^2 in genau zwei Punkten. Wir nennen $p \in \mathbb{R}^3$ einen *Pol* von ϱ, wenn $p \in \gamma_\varrho \cap S^2$.



Es sei weiter

$$M := \{\, p \in S^2 \mid \exists \varrho \in G \setminus \{e\},\ \text{so dass } p \text{ ein Pol von } \varrho \text{ ist} \,\}.$$

II.8.6 Hilfssatz. *Es seien $p \in M$ und $g \in G$. Dann gilt auch $g \cdot p \in M$.*

Beweis. Sei $\varrho \in G \setminus \{e\}$, so dass p ein Pol von ϱ ist. Wir berechnen

$$(g \cdot \varrho \cdot g^{-1}) \cdot (g \cdot p) = (g \cdot \varrho) \cdot p = g \cdot (\varrho \cdot p) = g \cdot p.$$

Wir halten fest:

- ⋆ Der Punkt $g \cdot p$ ist ein Fixpunkt von $\varrho' = g \cdot \varrho \cdot g^{-1} \in G \setminus \{e\}$. Das bedeutet $g \cdot p \in \gamma_{\varrho'}$.
- ⋆ Wegen $g \in \mathrm{SO}(3)$ gilt $\|g \cdot p\| = \|p\| = 1$, so dass $g \cdot p \in S^2$.

Diese beiden Eigenschaften zeigen $g \cdot p \in \gamma_{\varrho'} \cap S^2$, so dass $g \cdot p$ ein Pol von $\varrho' \in G$ ist und somit der Menge M angehört. □

Beweis von Satz II.8.2. Die Gruppe G wirkt auf Grund von Hilfssatz II.8.6 auf der Menge M. Es seien s die Anzahl aller G-Bahnen in M und $p_1, ..., p_s \in M$ Repräsentanten dieser Bahnen. Man beachte ferner, dass jedes Element $g \in G \setminus \{e\}$ genau zwei Punkte von M fixiert. Mit Satz II.7.11 schließen wir:

$$s = \frac{1}{\#G} \cdot (2 \cdot \#G - 2 + \#M) = \frac{1}{\#G} \cdot \left(2 \cdot \#G - 2 + \sum_{i=1}^{s} \#(G \cdot p_i) \right). \tag{II.8}$$

Wir schreiben dies mit Satz II.7.2 um zu

$$2 - \frac{2}{\#G} = s - \sum_{i=1}^{s} \frac{\#(G \cdot p_i)}{\#G} = s - \sum_{i=1}^{s} \frac{1}{\#G_{p_i}} = \sum_{i=1}^{s} \left(1 - \frac{1}{\#G_{p_i}} \right). \tag{II.9}$$

Für $G \neq \{e\}$ gilt

$$1 \leq 2 - \frac{2}{\#G} < 2. \tag{II.10}$$

Nach Konstruktion wird jeder Punkt p von M von einem nichttrivialen Element in G fixiert, so dass $\#G_p \geq 2$. Es ergibt sich

$$\frac{1}{2} \leq 1 - \frac{1}{\#G_{p_i}} < 1, \quad i = 1, ..., s. \tag{II.11}$$

Aus (II.9), (II.10) und (II.11) leiten wir

$$s \in \{ 2, 3 \}$$

ab.

Fall 1: $s = 2$. Gleichung (II.8) wird zu

$$2 = \#(G \cdot p_1) + \#(G \cdot p_2),$$

also zu $\#(G \cdot p_1) = 1 = \#(G \cdot p_2)$, und besagt, dass p_1 und p_2 von jedem Element aus G fixiert werden. Alle nichttrivialen Elemente von G haben somit dieselbe Drehachse, nämlich die Gerade durch p_1 und p_2, so dass $G = G_{p_1} = G_{p_2}$. Hilfssatz II.8.4, ii), zeigt $G \cong \mathbb{Z}_n$ für $n := \#G$.

Fall 2: $s = 3$. Aus der Gleichung

$$1 + \frac{2}{\#G} = \frac{1}{\#G_{p_1}} + \frac{1}{\#G_{p_2}} + \frac{1}{\#G_{p_3}}$$

folgt

$$\left(\frac{1}{\#G_{p_1}}, \frac{1}{\#G_{p_2}}, \frac{1}{\#G_{p_3}}\right) \in \left\{ \underbrace{\left(\frac{1}{2}, \frac{1}{2}, \frac{1}{n}\right),\ n \geq 2}_{\text{a)}}, \underbrace{\left(\frac{1}{2}, \frac{1}{3}, \frac{1}{3}\right)}_{\text{b)}}, \underbrace{\left(\frac{1}{2}, \frac{1}{3}, \frac{1}{4}\right)}_{\text{c)}}, \underbrace{\left(\frac{1}{2}, \frac{1}{3}, \frac{1}{5}\right)}_{\text{d)}} \right\}.$$

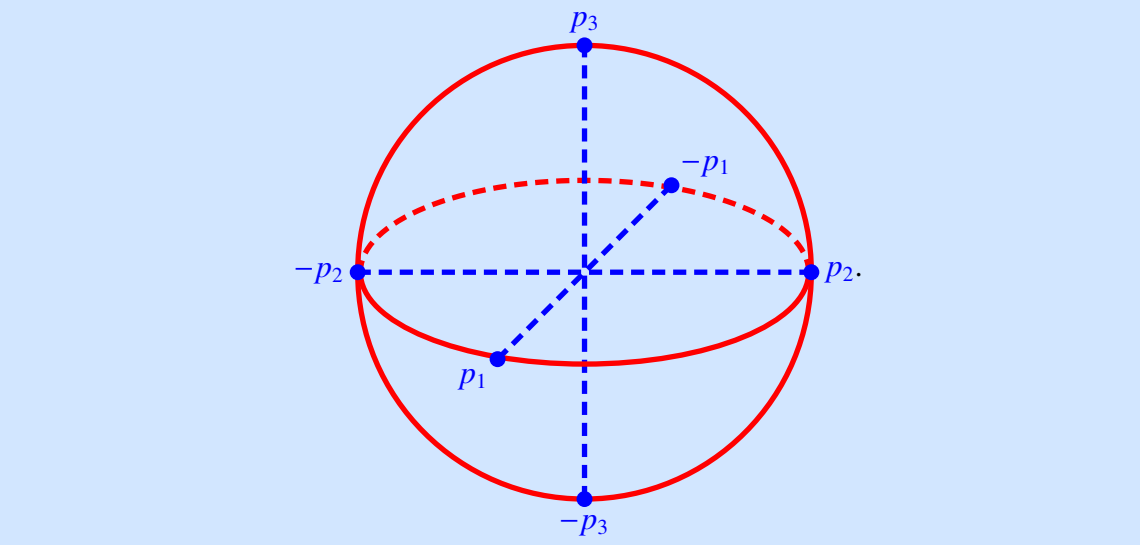
Wir gehen nun die in der obigen Formel bezeichneten Fälle durch.

Fall 2 a). Es sei zunächst $\boldsymbol{n = 2}$. Es folgt $\#G = 4$. Die Gruppe G kann kein Element der Ordnung 4 enthalten, weil dann $\#M = 2$ gelten würde und $s = 3$ unmöglich wäre. Damit ist G isomorph zur Kleinschen Vierergruppe $\mathbb{Z}_2 \times \mathbb{Z}_2 \cong D_2$. Wir können die zugehörige Geometrie noch genauer beschreiben.

Behauptung. *Man hat $G \cdot p_i = \{\pm p_i\}$, $i = 1, 2, 3$.*

Wir zeigen dies für p_1. Die Bahn von p_1 umfasst zwei Elemente, p_1 und einen weiteren Punkt p'. Die Standgruppen von p_1 und p' sind konjugiert (Lemma II.7.1). Da G abelsch ist, sind G_{p_1} und $G_{p'}$ gleich. Dies beinhaltet $p_1 = -p'$. √

Die Drehachsen der drei nichttrivialen Elemente von G stehen also paarweise aufeinander senkrecht, so dass sich folgendes Bild ergibt:

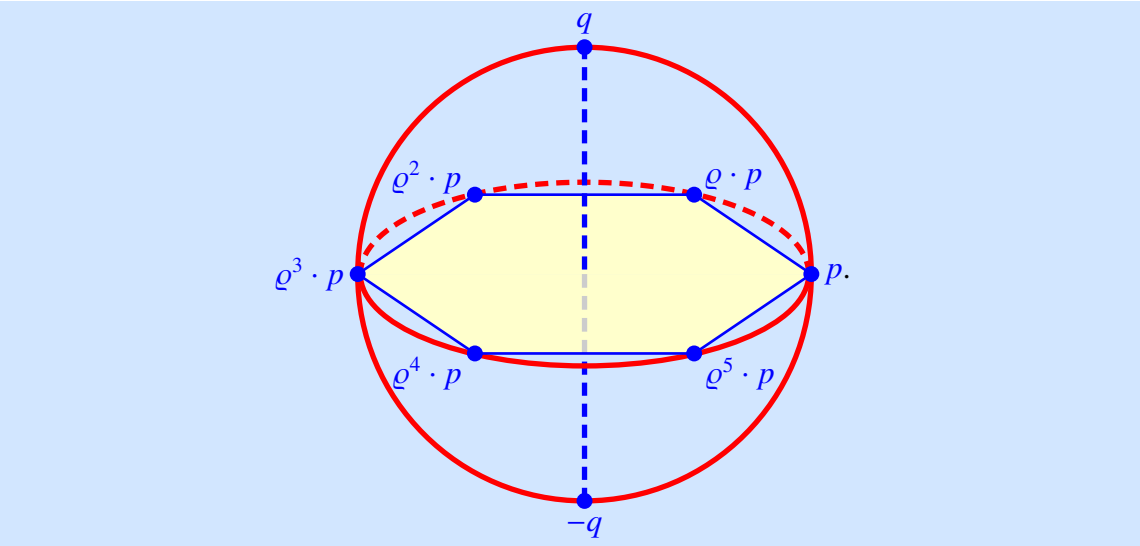


II.8.7 Bemerkung. Wir erkennen, dass G in der speziellen Symmetriegruppe eines Würfels enthalten ist.

Für $\boldsymbol{n \geq 3}$ haben wir $\#G = 2n$. Es seien $p := p_1$ und $q := p_3$. Die Standgruppe G_q ist zyklisch von der Ordnung n (Hilfssatz II.8.4, ii). Sei ϱ ein Erzeuger für G_q. Wir schauen uns die Punkte p, $\varrho \cdot p$, ..., $\varrho^{n-1} \cdot p$ an. Diese bilden nach dem besagten Hilfssatz ein regelmäßiges n-Eck P in einer Ebene, die senkreckt auf der Geraden durch $-q$ und q steht. Außerdem stellen sie die Bahn $G \cdot p$ dar. Das nichttriviale Element $\varrho' \in G_p$ bildet folglich P auf sich ab. Wir erkennen, dass P auf dem Äquator der Sphäre S^2 mit q als Nord- und $-q$ als Südpol liegt. Das Element ϱ' hat Ordnung zwei und ist damit eine Drehung um den Winkel π. Diese Betrachtungen zeigen

$$D_n \cong \langle \varrho, \varrho' \rangle \subset G.$$

Aus $\#D_n = 2n = \#G$ folgt wie gewünscht $\langle \varrho, \varrho' \rangle = G$.

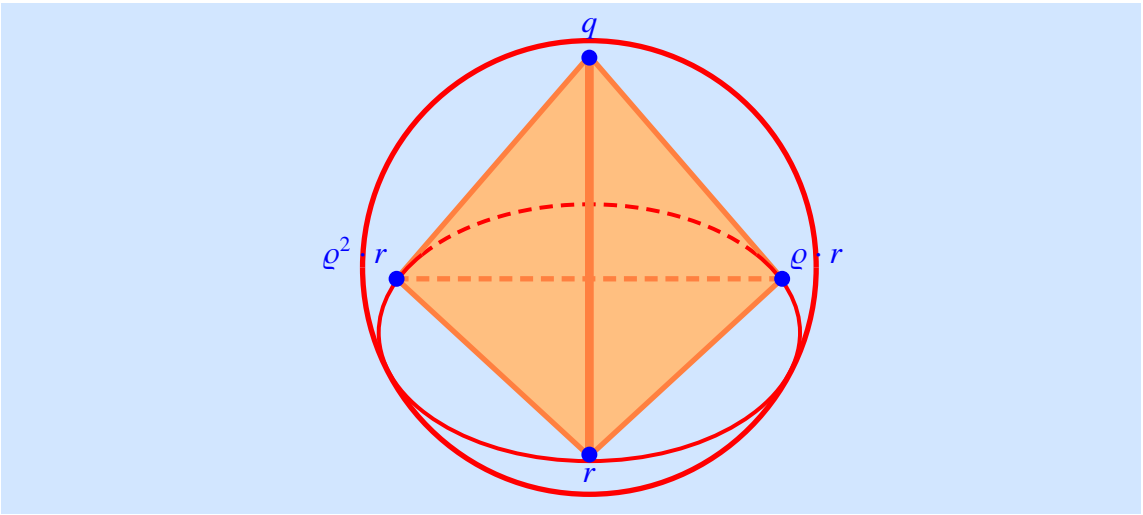


Fall 2 b). In diesem Fall gilt $\#G = 12$. Wir setzen $q := p_3$. Wegen $\#G_q = 3$ umfasst die Bahn $G \cdot q$ nach Satz II.7.2 vier Punkte. Inbesondere können wir $p \in (G \cdot q) \setminus \{\pm q\}$ wählen. Für einen Erzeuger ϱ von $G_q \cong \mathbb{Z}_3$ bilden die Punkte r, $\varrho \cdot r$ und $\varrho^2 \cdot r$ nach Hilfssatz II.8.4

ein gleichseitiges Dreieck. Dieselbe Betrachtung kann anstatt für q für jeden Punkt in der Bahn $G \cdot q$ durchgeführt werden. Wir schließen, dass

$$q,\ r,\ \varrho \cdot r,\ \varrho^2 \cdot r$$

die Eckpunkte eines regulären Tetraeders T sind.

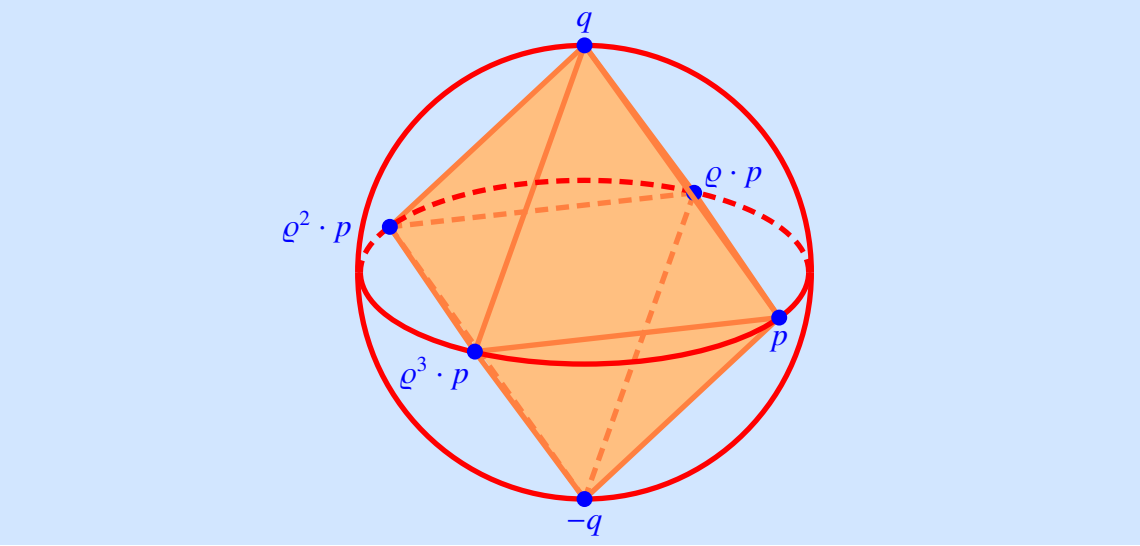


Da diese Punkte eine G-Bahn bilden, folgt $G \subset \mathrm{SO}(T)$. Wegen $\#G = 12 = \#\mathrm{SO}(T)$ ergibt sich sogar Gleichheit.

Fall 2 c). Hier haben wir $\#G = 24$. Sei $q := p_3$. Die Standgruppe G_q enthält vier Elemente und die Bahn $G \cdot q$ demnach sechs. Es sei $r \in (G \cdot q) \setminus \{\pm q\}$. Gemäß Hilfssatz II.8.4 fixieren wir einen Erzeuger ϱ für $G_q \cong \mathbb{Z}_4$. Die vier Punkte r, $\varrho \cdot r$, $\varrho^2 \cdot r$ und $\varrho^3 \cdot r$ sind die Ecken eines Quadrats Q in einer Ebene E, die senkrecht auf der Geraden γ_ϱ steht. Dabei wissen wir noch nicht, dass E den Ursprung enthält. Die Punkte in der Bahn $G_r \cdot q$ sind Ecken eines Quadrats Q' in einer Ebene E'. Der Durchschnitt $(G_q \cdot r) \cap (G_r \cdot q)$ umfasst zwei Elemente d_1 und d_2. Da alle Elemente in $G_r \cdot q$ denselben Abstand von r haben, handelt es sich bei d_1 und d_2 um gegenüberliegende Ecken des Quadrats Q. Es folgt, dass E' die Gerade durch q und den Mittelpunkt von Q enthält und damit auch den Ursprung. Dasselbe gilt folglich für E. Man erkennt, dass $-r \in G \cdot q$ und ebenso $-q \in G \cdot q$, d.h.

$$G \cdot q = \{\, q, -q, r, \varrho \cdot r, \varrho^2 \cdot r, \varrho^3 \cdot r \,\}.$$

Ferner sehen wir auf diese Weise, dass die Punkte der Bahn $G \cdot q$ die Ecken eines regulären Oktaeders O bilden.



Damit ist $G \subset \mathrm{SO}(O)$ gezeigt. Man überlegt sich leicht, dass $\mathrm{SO}(O)$ genau 24 Elemente enthält und deshalb $G = \mathrm{SO}(O)$ gilt.

Fall 2 d). Die Gruppe G enthält dann 60 Elemente, die Standgruppe G_q fünf und die Bahn $G \cdot q$ zwölf, $q := p_3$. Wir wählen einen Punkt $r \in (G \cdot q) \setminus \{\pm q\}$, der den kleinsten Abstand zu q unter den Punkten von $(G \cdot q) \setminus \{\pm q\}$ einnimmt, und einen Erzeuger ϱ für G_q.

Die fünf Punkte r, $\varrho \cdot r$, $\varrho^2 \cdot r$, $\varrho^3 \cdot r$ und $\varrho^4 \cdot r$ sind die Eckpunkte eines regelmäßigen Fünfecks. Aus Bemerkung II.8.5 ergibt sich weiter, dass alle diese Punkte denselben Abstand zu q haben.

Sei weiter $s \in (G \cdot q) \setminus \{\pm q, r, \varrho \cdot r, \ldots, \varrho^4 \cdot r\}$. Die fünf Punkte s, $\varrho \cdot s$, $\varrho^2 \cdot s$, $\varrho^3 \cdot s$ und $\varrho^4 \cdot s$ bilden ein regelmäßiges Fünfeck und haben alle denselben Abstand zu q.

Wir haben

$$2 > \|q - s\| \geq \|q - r\| > 0.$$

Die erste Ungleichung gilt wegen $s \neq -q$. Wenn $\|q - s\| = \|q - r\|$ gälte, dann lägen r, $\varrho \cdot r$, $\varrho^2 \cdot r$, $\varrho^3 \cdot r$, $\varrho^4 \cdot r$, s, $\varrho \cdot s$, $\varrho^2 \cdot s$, $\varrho^3 \cdot s$ und $\varrho^4 \cdot s$ alle auf demselben Kreis: Wieder sind alle

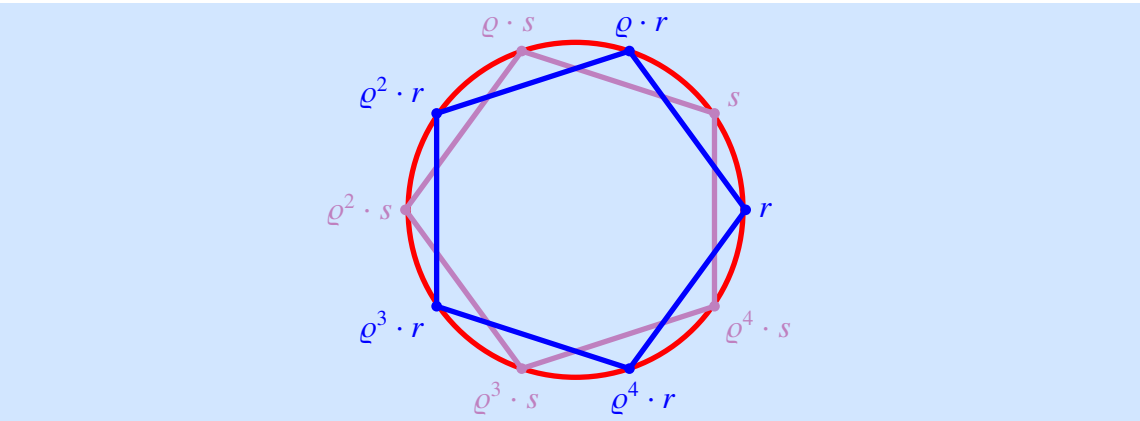
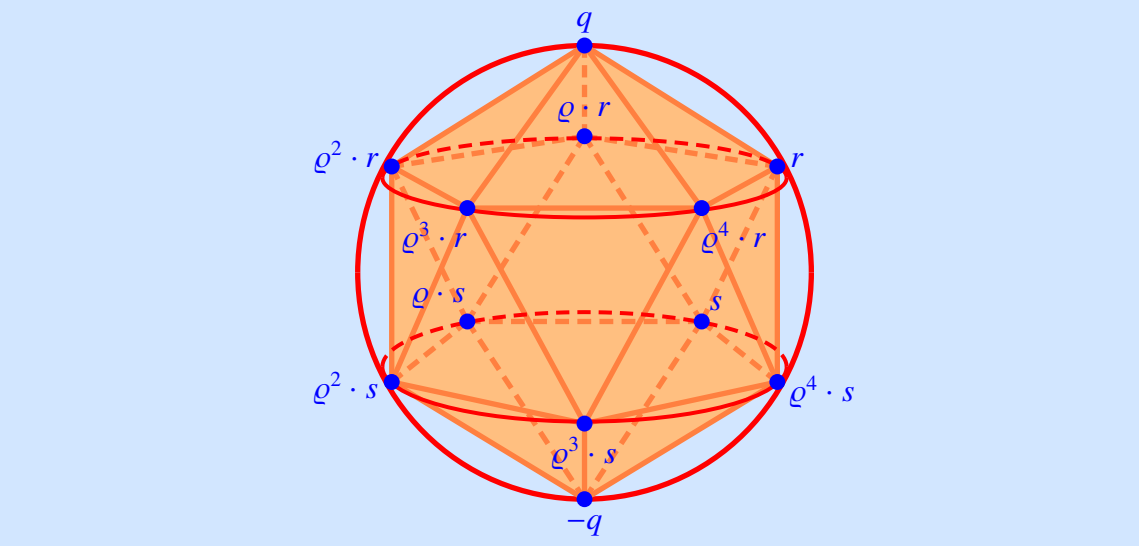


Abbildung II.3: Die unmögliche Konfiguration

Punkte der Bahn $G \cdot q$ gleichberechtigt, so dass die obigen Untersuchungen zeigen, dass es unter den elf Punkten von $(G \cdot q) \setminus \{r\}$ fünf mit demselben minimalem Abstand zu r

gibt. In der in Abbildung II.3 gezeigten Konfiguration gibt es aber höchstens vier davon. Dieser Widerspruch zeigt $\|q - s\| > \|q - r\|$.

Mit unseren Überlegungen folgt, dass die Elemente der Bahn $G \cdot q$ die Eckpunkte eines regulären Ikosaeders I sind.



Somit haben wir $G \subset \mathrm{SO}(I)$. Der Leser bzw. die Leserin möge selbstständig die spezielle Symmetriegruppe eines Ikosaeders untersuchen und zu dem Schluss gelangen, dass diese 60 Elemente umfasst. Damit finden wir schließlich $G = \mathrm{SO}(I)$. □

II.8.8 Bemerkung. i) Wir sind oftmals von der Anschauung eines gegebenen Körpers ausgegangen und haben mit dieser seine Symmetriegruppe beschrieben. Im Beweis von Satz II.8.2 sind wir den umgekehrten Weg gegangen. Wir haben mit einer gewissen Gruppe G begonnen und mit Hilfe der Algebra das Objekt gefunden, dessen Symmetriegruppe G ist. Im vorgestellten Satz haben wir somit eine wunderschöne Entsprechung von Algebra und Geometrie vorgefunden.

ii) Die Diskussionen im obigen Beweis zeigen, wie die in Satz II.8.2 genannten Gruppen als Untergruppen von $\mathrm{SO}_3(\mathbb{R})$ aufgefasst werden können. Der Beweis zeigt weiter, dass wir in der Formulierung des Satzes „ist zu ... isomorph“ durch „ist zu ... konjugiert“ ersetzen können.

Über Polyeder

In den bisherigen Ausführungen haben wir nur ein vages anschauliches Bild der sogenannten fünf **platonischen Körper** Tetraeder, Hexaeder (=Würfel), Oktaeder, Dodekaeder und Ikosaeder benutzt bzw. angenommen, dass die Leserin bzw. der Leser bereits mit diesen Objekten vertraut ist. Jetzt wollen wir die formalen Grundlagen anreißen. Wir werden nicht bei allen Argumenten ins Detail gehen. Dazu würden wir etwas mehr konvexe Geometrie benötigen ([10], [24]).

Eine Teilmenge $H \subset \mathbb{R}^3$ ist ein (*abgeschlossener*) *Halbraum*, wenn es eine nichttriviale Linearform $l\colon \mathbb{R}^3 \longrightarrow \mathbb{R}$ und eine Zahl $c \in \mathbb{R}$ gibt, so dass

$$H = \{\, p \in \mathbb{R}^3 \mid l(p) \geq c \,\}.$$

Wir definieren dazu

$$H^- : \{\, p \in \mathbb{R}^3 \mid l(p) \leq c \,\}.$$

Es sei $M \subset \mathbb{R}^3$ eine **endliche** Teilmenge. Die *konvexe Hülle* von M ist der Durchschnitt aller Halbräume, die M enthalten:

$$\mathrm{Konv}(M) := \bigcap_{\substack{H \subset \mathbb{R}^3 \\ H \text{ Halbraum}}} H.$$

Die Menge $\mathrm{Konv}(M)$ ist konvex (im Sinne von [17], S. 62). Sie ist die kleinste konvexe Menge, die M enthält.[20]

Ein *Polyeder* ist nun eine Teilmenge $P \subset \mathbb{R}^3$ mit folgenden Eigenschaften:

- ⋆ P ist die konvexe Hülle einer endlichen Teilmenge $M \subset \mathbb{R}^3$.
- ⋆ P ist dreidimensional, d.h. es gibt keine Ebene im $\mathbb{R}^3$, die P enthält.

Es seien $P \subset \mathbb{R}^3$ ein Polyeder. Eine Teilmenge $P' \subset P$ ist eine *Seite* von P, wenn es einen Halbraum $H \subset \mathbb{R}^3$ mit

$$P \subset H^- \quad \text{und} \quad P' = P \cap H$$

gibt.

Für den Durchschnitt $P \cap H$ von P mit einem Halbraum $H = \{\, p \in \mathbb{R}^3 \mid l(p) \geq c \,\}$, so dass $P \subset H^-$, bestehen folgende Möglichkeiten

- ⋆ $P \cap H = \varnothing$.
- ⋆ $P \cap H = \{p\}$. In diesem Fall ist p eine *Ecke* von p.
- ⋆ $P \cap H = K$ ist eine Strecke positiver Länge auf einer Geraden. Dann heißt K *Kante* von P.
- ⋆ $P \cap H = S$ ist ein zweidimensionales Vieleck in der Ebene $\{\, p \in \mathbb{R}^3 \mid l(p) = c \,\}$. In diesem Fall ist S eine *Seite* von P.

Mit diesen Begriffen definieren wir eine *Fahne* in P als ein Tripel (E, K, S), das sich aus einer Ecke E, einer Kante K und einer Seite S von P zusammensetzt, so dass

$$E \in K \subset S.$$

Es sei

$$\mathfrak{F}(P) = \{\, F \mid F \text{ ist Fahne von } P \,\}.$$

Die Symmetriegruppe $\mathrm{O}(P)$ wirkt offensichtlich auf der Menge $\mathfrak{F}(P)$ der Fahnen in P.

Das Polyeder P ist *regulär*, wenn es zu je zwei Fahnen F und F' ein Element $g \in \mathrm{O}(P)$ mit

$$F = g \cdot F'$$

gibt.

[20] Die obige Definition der konvexen Hülle greift nur für endliche Mengen. Im Allgemeinen definiert man die konvexe Hülle einer Teilmenge $M \subset \mathbb{R}^3$ als die kleinste konvexe Teilmenge, die M enthält. Der Durchschnitt aller Halbräume, die M enthalten, ist der Abschluss der konvexen Hülle von M. Man betrachte z.B. den offenen Ball $M := \{\, p \in \mathbb{R}^3 \mid \|p\| < 1 \,\}$. Er ist bereits konvex ([17], S. 62f), stimmt also mit seiner konvexen Hülle überein. Der Durchschnitt aller Halbräume, die M enthalten, ist der abgeschlossene Ball $\overline{M} = \{\, p \in \mathbb{R}^3 \mid \|p\| \leq 1 \,\}$ (vgl. [17], Beispiel 1.6.2, i).

II.8.9 Bemerkung und Beispiel. i) Jedes Polyeder P besitzt ein **duales Polyeder** $P^\vee$: Bezeichne $M^\vee$ die Menge der Seitenmittelpunkte von P, so ist $P^\vee := \mathrm{Konv}(M^\vee)$. Jeder Seite S von P ist damit eine Ecke $S^\vee$ von $P^\vee$ zugeordnet. Weiter entspricht jeder Ecke E von P eine Seite $E^\vee$ von $P^\vee$. Dabei gilt genau dann $E \in S$, wenn $E^\vee \ni S^\vee$. Man enthält somit auch eine Korrespondenz zwischen den Kanten von P und denjenigen von $P^\vee$: Die Kante $K \subset P$ mit den Ecken E und E' entspricht der Kante $K^\vee = E^\vee \cap E'^\vee$ von $P^\vee$.

ii) Es seien P ein Tetraeder, Hexaeder, Oktaeder, Dodekaeder oder Ikosaeder, bei dem alle Kanten dieselbe Länge haben. Dann ist P ein reguläres Polyeder. Das Hexaeder ist dual zum Oktaeder und das Dodekaeder zum Ikosaeder. Das Tetraeder ist „selbstdual".

II.8.10 Lemma. *Zu je zwei Ecken E, $\widetilde{E}$ eines regulären Polyeders gibt es ein Element $\varrho \in \mathrm{SO}(P)$ in der **speziellen** Symmetriegruppe von P, so dass*

$$E = \varrho \cdot \widetilde{E}.$$

Beweis. Es gibt ein Element $g \in \mathrm{O}(P)$ mit $E = g \cdot \widetilde{E}$, und wir müssen nur den Fall behandeln, dass $\mathrm{Det}(g) = -1$ gilt. Seien $S \subset P$ eine Seite von P, die E enthält. Es gibt dann genau zwei Kanten K' und K'' in S, die E enthalten. Die Kante K' bzw. K'' enthält neben E noch einen weiteren Eckpunkt E' bzw. E''. Die Fahne (E, K', S) kann durch ein Element $h \in \mathrm{O}(P)$ in die Fahne (E'', K'', S) überführt werden. Die Leserin bzw. der Leser möge sich der Tatsache vergewissern, dass h die Orientierung von $\mathbb{R}^3$ erhält, d.h. $h \in \mathrm{SO}(P)$. Des Weiteren findet man ein Element $k \in \mathrm{O}(P)$, das die Fahne (E'', K'', S) auf die Fahne (E, K'', S) abbildet. Hier folgt $\mathrm{Det}(k) = -1$. Folglich ist

$$\varrho := k \cdot h \cdot g$$

ein Element in $\mathrm{SO}(P)$, dass $\widetilde{E}$ auf E abbildet. □

II.8.11 Satz. *Tetraeder, Hexaeder, Oktaeder, Dodekaeder und Ikosaeder sind die einzigen regulären Polyeder.*

Beweis. Es seien $G := \mathrm{SO}(P)$ und $\mathfrak{E}$ die Menge der Ecken von P. Ein Element $\varrho \in G$ ist durch seine Wirkung auf den Ecken bestimmt (Übung), so dass G isomorph zu einer Untergruppe von $S(\mathfrak{E})$ und damit endlich ist. Für jede Ecke E von P ist der Stabilisator G_E nichttrivial, genauer gesagt haben wir:

Behauptung. *Für jede Ecke E von P gilt $\#G_E \geq 3$.*

Dazu seien $E \in P$ eine Ecke und $S \subset P$ eine Seite, die E enthält. Es gibt zwei Kanten K_1 und K_2 in S, die E enthalten. Da P nicht in der Ebene, die durch S bestimmt wird, liegt, ist eine der Strecken, die E mit einem Punkt aus $P \setminus S$ verbindet, eine weitere Kante von P. Ferner grenzt jede Kante von P an genau zwei Seiten von P.[21] Eine Verallgemeinerung des Arguments aus Lemma II.8.10 zeigt, dass es zu je zwei Paaren (E, K) und (E', K'), die aus Ecken E bzw. E' und Kanten K bzw. K' mit $E \in K$ bzw. $E' \in K'$ bestehen, ein Element $g \in G$ mit $(E, K) = g \cdot (E', K')$ gibt.

Es seien K_1, K_2 und K_3 drei verschiedene Kanten, die E enthalten. Es gibt Elemente $g_2, g_3 \in G$ mit $(E, K_i) = g_i \cdot (E, K_1)$, $i = 2, 3$. Diese gehören der Standgruppe G_E an, so dass $\{ e, g_2, g_3 \} \subset G_E$. √

[21] Diese Aussage entspricht der Tatsache, dass jede Kante von P genau zwei Ecken von P enthält (Bemerkung und Beispiel II.8.9).

Also ist $\mathfrak{E}$ eine Teilmenge der Menge M der Pole von G. Nach Lemma II.8.10 ist $\mathfrak{E}$ die Bahn eines Pols $p \in M$. Der Beweis von Satz II.8.2[22] impliziert die Behauptung in Fall 2 b), in Fall 2 c), wenn es eine Ecke E mit $\#G_E = 4$ gibt, und in Fall 2 d), wenn es eine Ecke E mit $\#G = 5$ gibt. Gilt $\#G_E = 3$ in Fall 2 c), dann überprüft man mit Überlegungen wie in 2 d), dass P ein Würfel ist. Für $\#G = 60$ und eine Ecke E mit $\#G_E = 3$ führen ähnliche Überlegungen zum Dodekaeder. □

II.8.12 Bemerkung. Die Punkte aus der Polmenge für G in den Fällen 2 c) und 2 d), die eine zweielementige Standgruppe haben, gehören zu den Drehungen um Achsen durch die Mittelpunkte zweier gegenüberliegender Kanten und deshalb nicht zu den Ecken eines regulären Polyeders.

II.9 Faktorgruppen

In der linearen Algebra lernt man folgende Konstruktion kennen ([20], §30; [5], Abschnitt 2.2.7): Gegeben ein Körper k, ein k-Vektorraum V und ein Untervektorraum $U \subset V$, dann existiert auf der Menge V/U der Linksnebenklassen die Struktur eines k-Vektorraums, so dass die Projektion $V \longrightarrow V/U$, $v \longmapsto [v]$, linear ist. Wir wollen nun die analoge Konstruktion in der Gruppentheorie untersuchen.

Problem. Gegeben seien eine Gruppe G und eine Untergruppe $H \subset G$. Wann trägt die Menge G/H der Linksnebenklassen die Struktur einer Gruppe, so dass

$$\begin{array}{rcl} \pi\colon G & \longrightarrow & G/H \\ g & \longmapsto & [g] \end{array}$$

ein Gruppenhomomorphismus ist?

Da π surjektiv ist, kann die Gruppenstruktur auf G/H nur von der Form

$$\forall g, g' \in G: \quad [g] \cdot [g'] = [g \cdot g'] \tag{II.12}$$

sein. Also formulieren wir das obige Problem folgendermaßen um:

Problem. Wann ist Formel (II.12) wohldefiniert?

Wir müssen also herausfinden, wann für alle $g, g' \in G$ und $h, h' \in H$

$$[g \cdot h \cdot g' \cdot h'] = [g \cdot g']$$

gilt, d.h.

$$g'^{-1} \cdot g^{-1} \cdot g \cdot h \cdot g' \cdot h' = g'^{-1} \cdot h \cdot g' \cdot h' \in H. \tag{II.13}$$

II.9.1 Beobachtung. *Die Bedingung, dass* (II.13) *für alle $g, g' \in G$, $h, h' \in H$ gilt, ist äquivalent zu der Aussage*

$$\forall g \in G,\ h \in H: \quad g \cdot h \cdot g^{-1} \in H. \tag{II.14}$$

[22] Fall 1 und 2 a) scheiden aus. Warum?

Vereinbarung. Wir schreiben Aussage (II.14) in der Form

$$\forall g \in G: \quad g \cdot H \cdot g^{-1} \subset H.$$

Beweis von Beobachtung II.9.1. Die Implikation „$\Longleftarrow$“ ist trivial, weil H eine Untergruppe ist. Für die Richtung „$\Longrightarrow$“ wähle man $g' := g^{-1}$ und $h' = e$ in (II.13). □

II.9.2 Beobachtung. *Die Bedingung*

$$\forall g \in G: \quad g \cdot H \cdot g^{-1} \subset H$$

ist äquivalent zu der Bedingung

$$\forall g \in G: \quad g \cdot H \cdot g^{-1} = H.$$

Beweis. Die zweite Bedingung impliziert offenbar die erste. Für die Umkehrung beachte man, dass

$$H = g \cdot (g^{-1} \cdot H \cdot g) \cdot g^{-1} \subset g \cdot H \cdot g^{-1}$$

für $g \in G$ gilt. □

II.9.3 Definition. Es seien G eine Gruppe und H eine Untergruppe. Man sagt, dass H ein *Normalteiler* von G ist, wenn

$$\forall g \in G: \quad g \cdot H \cdot g^{-1} = H$$

gilt.
Schreibweise. $H \lhd G$.

II.9.4 Satz. *Es seien G eine Gruppe und $H \subset G$ ein Normalteiler. Durch*

$$\begin{array}{rcl} \cdot\colon G/H \times G/H & \longrightarrow & G/H \\ ([g],[g']) & \longmapsto & [g \cdot g'] \end{array}$$

wird auf G/H die Struktur einer Gruppe definiert. Die Abbildung

$$\begin{array}{rcl} \pi\colon G & \longrightarrow & G/H \\ g & \longmapsto & [g] \end{array}$$

ist ein surjektiver Gruppenhomomorphismus, und es gilt

$$\mathrm{Ker}(\pi) = H.$$

II.9.5 Definition. Wir nennen G/H die *Faktor-* oder *Quotientengruppe* von G nach H.

Beweis von Satz II.9.4. Nach Definition eines Normalteilers ist die Multiplikation auf G/H wohldefiniert. Alle anderen Aussagen ergeben sich aus der vorangegangenen Diskussion oder sind offensichtlich. □

II.9.6 Beispiele. i) Wenn G abelsch ist, dann ist jede Untergruppe $H \subset G$ ein Normalteiler.

ii) Für jede Gruppe G ist das Zentrum (Definition II.6.17)

$$Z(G) = \{\, h \in G \mid \forall g \in G : g \cdot h \cdot g^{-1} = h \,\}$$

ein Normalteiler. Ferner ist jede Untergruppe $H \subset Z(G)$ ebenfalls ein Normalteiler von G.

iii) Es seien $n \geq 3$, S_n die symmetrische Gruppe und

$$H := \langle (1\ 2) \rangle = \{\, e, (1\ 2) \,\} \cong \mathbb{Z}_2.$$

Dann ist H **kein** Normalteiler in G, denn man hat z.B.

$$(1\ 3) \cdot (1\ 2) \cdot (1\ 3) = (2\ 3) \notin H.$$

iv) Es seien G, G' Gruppen und $\varphi\colon G \longrightarrow G'$ ein Gruppenhomomorphismus. Dann ist $\mathrm{Ker}(\varphi)$ ein Normalteiler von G. In der Tat hat man

$$\varphi(g \cdot h \cdot g^{-1}) = \varphi(g) \cdot \varphi(h) \cdot \varphi(g^{-1}) = \varphi(g) \cdot e \cdot \varphi(g)^{-1} = e$$

für $g \in G$ und $h \in \mathrm{Ker}(\varphi)$.

So ist z.B. für einen Körper k die Untergruppe $\mathrm{SL}_n(k) = \mathrm{Ker}(\mathrm{Det}\colon\ \mathrm{GL}_n(k) \longrightarrow k^\star)$ ein Normalteiler von $\mathrm{GL}_n(k)$. Die Gruppe $A_n = \mathrm{Ker}(\mathrm{Sign}\colon S_n \longrightarrow \{\pm 1\})$ ist ein Normalteiler von S_n (s. auch Teil v).

v) Es seien G eine Gruppe und $H \subset G$ eine Untergruppe. Gilt $\#(G/H) = 2$, dann ist H ein Normalteiler in G. Zum Beweis zeigen wir, dass

$$\forall g \in G : \quad g \cdot H = H \cdot g.$$

Für $g \in H$ haben wir natürlich $g \cdot H = H = H \cdot g$. Falls $g \in G \setminus H$, so gilt $g \cdot H \neq H$ und $H \cdot g \neq H$. Auf der anderen Seite ist G die disjunkte Vereinigung der Links- bzw. Rechtsnebenklassen, d.h.

$$G = H \sqcup g \cdot H \quad \text{bzw.} \quad G = H \sqcup H \cdot g.$$

Daraus folgern wir unmittelbar $g \cdot H = G \setminus H = H \cdot g$.

Es seien $n \geq 2$ und D_n die entsprechende Diedergruppe. Sie enthält die Rotation r um den Winkel $2\pi/n$. Für $H = \langle r \rangle$ und die Spiegelung $s \in D_n$ an der x-Achse hat man $D_n/H = \{\, [e], [s] \,\}$, so dass H normal in D_n ist.

vi) In D_6 betrachten wir die Rotation r um den Winkel $\pi/3$. Wir behaupten, dass $H := \langle r^3 \rangle \cong \mathbb{Z}_2$ ein Normalteiler von D_6 ist. In D_6 gilt Relation (II.1), d.h. $s \cdot r \cdot s = r^{-1}$. Sie impliziert $s \cdot r^3 \cdot s = r^{-3} = r^3$. Damit folgt leicht die Behauptung.[23]

vii) In der alternierenden Gruppe A_4 betrachten wir die Teilmenge

$$H := \{\, e, (1\ 2) \cdot (3\ 4), (1\ 3) \cdot (2\ 4), (1\ 4) \cdot (2\ 3) \,\}$$

aller Permutationen vom Zykeltyp $(2, 2)$.

Wir bemerken zunächst, dass H eine Untergruppe von G ist. Offensichtlich gilt $e \in H$. Jedes Element $g \in H$ erfüllt $g^2 = e$, so dass $g^{-1} = g \in H$. Dass für $g, h \in H$ auch $g \cdot h \in H$, überprüft man durch Nachrechnen.

Da Konjugation den Zykeltyp nicht ändert (Lemma II.6.26), ist H ein Normalteiler von A_4.

[23] Genauer gesagt zeigt unser Argument, dass $H \subset Z(D_6)$. Man kann sich weiter vergewissern, dass $H = Z(G)$ gilt.

II.9.7 Satz (Universelle Eigenschaften der Faktorgruppe). *Es seien G, G' Gruppen, $H \lhd G$ ein Normalteiler von G und $\varphi\colon G \longrightarrow G'$ ein Homomorphismus. Gilt*

$$H \subset \operatorname{Ker}(\varphi),$$

dann existiert genau ein Homomorphismus

$$\overline{\varphi}\colon G/H \longrightarrow G',$$

so dass

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & G' \\ {\scriptstyle\pi}\downarrow & \nearrow_{\overline{\varphi}} & \\ G/H & & \end{array}$$

kommutiert. Dabei ist $\pi\colon G \longrightarrow G/H$, $g \longmapsto [g]$.

II.9.8 Bemerkung. Es sei G eine Gruppe. Zu einem Normalteiler $H \lhd G$ haben wir eine Gruppe G/H und einen Homomorphismus $\pi\colon G \longrightarrow G/H$ mit $\operatorname{Ker}(\pi) = H$ und damit insbesondere $H \subset \operatorname{Ker}(\varphi)$ konstruiert. Der Satz besagt, dass das Paar $(G/H, \pi)$ **universell mit dieser Eigenschaft** ist: Jeder andere Homomorphismus $\varphi\colon G \longrightarrow G'$ mit $H \subset \operatorname{Ker}(\varphi)$ faktorisiert in eindeutiger Weise über π, d.h. es gibt genau einen Homomorphismus $\overline{\varphi}\colon G/H \longrightarrow G'$ mit $\varphi = \overline{\varphi} \circ \pi$. Durch diese universelle Eigenschaft ist $(G/H, \pi)$ eindeutig festgelegt: Es seien Q eine Gruppe und $\varrho\colon G \longrightarrow Q$ ein Homomorphismus mit $H \subset \operatorname{Ker}(\varrho)$, so dass es für jeden Homomorphismus $\varphi\colon G \longrightarrow G'$ mit $H \subset \operatorname{Ker}(\varphi)$ genau einen Homomorphismus $\overline{\varphi}\colon Q \longrightarrow G'$ mit $\varphi = \overline{\varphi} \circ \varrho$ gibt. Dann finden wir insbesondere eindeutig bestimmte Homomorphismen $\overline{\varrho}\colon G/H \longrightarrow Q$ und $\overline{\pi}\colon Q \longrightarrow G/H$, so dass die Diagramme

$$\begin{array}{ccc} G & \xrightarrow{\varrho} & Q \\ {\scriptstyle\pi}\downarrow & \nearrow_{\overline{\varrho}} & \\ G/H & & \end{array} \quad \text{und} \quad \begin{array}{ccc} G & \xrightarrow{\pi} & G/H \\ {\scriptstyle\varrho}\downarrow & \nearrow_{\overline{\pi}} & \\ Q & & \end{array}$$

kommutieren. Damit erhalten wir die Diagramme

$$\begin{array}{ccc} G & \xrightarrow{\pi} & G/H \\ {\scriptstyle\pi}\downarrow & \nearrow_{\overline{\pi}\circ\overline{\varrho}} & \\ G/H & & \end{array} \quad \text{und} \quad \begin{array}{ccc} G & \xrightarrow{\varrho} & Q \\ {\scriptstyle\varrho}\downarrow & \nearrow_{\overline{\varrho}\circ\overline{\pi}} & \\ Q & & \end{array}.$$

Die universellen Eigenschaften von $(G/H, \pi)$ und (Q, ϱ) implizieren

$$\mathrm{id}_{G/H} = \overline{\pi} \circ \overline{\varrho} \quad \text{und} \quad \mathrm{id}_Q = \overline{\varrho} \circ \overline{\pi}.$$

Die Gruppen G/H und Q sind damit isomorph und ihre universellen Eigenschaften bestimmen einen Isomorphismus $\psi\colon G/H \longrightarrow Q$.[24] Um mit $(G/H, \pi)$ zu arbeiten, muss man nur die obige universelle Eigenschaft kennen und nicht seine Konstruktion. Im besprochenen Fall treten die Vorzüge dieser Sichtweise noch nicht klar zu Tage, in anderen Beispielen wie dem Tensorprodukt ([13], Chapter XVI, §1) von Moduln ist das deutlicher zu erkennen. Die Leser oder Leserinnen, die ihre Kenntnisse in der Algebra vertiefen, werden noch zahlreichen universellen Konstruktionen und Eigenschaften begegnen.

[24] Man sagt, das Paar $(G/H, \pi)$ ist **bis auf eindeutige Isomorphie eindeutig**.

Beweis von Satz II.9.7. Die genannte Bedingung für $\overline{\varphi}$ verlangt:

$$\forall g \in G: \quad \overline{\varphi}([g]) = \overline{\varphi}(\pi(g)) = \varphi(g). \tag{II.15}$$

Aus dieser Gleichung lesen wir die Eindeutigkeit von $\overline{\varphi}$ ab.

Wir zeigen, dass die Vorschrift in (II.15) wohldefiniert ist. Dazu seien $g, g' \in G$ Elemente mit $[g] = [g']$. Dann existiert ein $h \in H$ mit $g = g' \cdot h$. Wegen $H \subset \operatorname{Ker}(\varphi)$ finden wir

$$\varphi(g) = \varphi(g' \cdot h) = \varphi(g') \cdot \varphi(h) = \varphi(g') \cdot e = \varphi(g').$$

Die Gleichung $\varphi = \overline{\varphi} \circ \pi$ gilt nach Definition von $\overline{\varphi}$. Schließlich muss noch gezeigt werden, dass $\overline{\varphi}$ ein Gruppenhomomorphismus ist. Dazu berechnen wir

$$\forall g, g' \in G: \quad \overline{\varphi}([g] \cdot [g']) = \overline{\varphi}([g \cdot g']) = \varphi(g \cdot g') = \varphi(g) \cdot \varphi(g') = \overline{\varphi}([g]) \cdot \overline{\varphi}([g'])$$

und beenden damit den Beweis des Satzes. □

Als Illustration dieses Satzes stellen wir eine allgemeine Konstruktion vor. Es seien G eine Gruppe, G' eine **abelsche** Gruppe und $\varphi\colon G \longrightarrow G'$ ein Homomorphismus. Für $g, h \in G$ haben wir

$$\varphi(g \cdot h \cdot g^{-1} \cdot h^{-1}) = \varphi(g) \cdot \varphi(h) \cdot \varphi(g)^{-1} \cdot \varphi(h)^{-1} = \varphi(g) \cdot \varphi(g)^{-1} \cdot \varphi(h) \cdot \varphi(h)^{-1} = e. \tag{II.16}$$

II.9.9 Definitionen. Es sei G eine Gruppe.

i) Für $g, h \in G$ heißt $g \cdot h \cdot g^{-1} \cdot h^{-1}$ der *Kommutator* von g und h.

ii) Es sei

$$K(G) := \{\, g \cdot h \cdot g^{-1} \cdot h^{-1} \mid g, h \in G \,\}.$$

Die von $K(G)$ erzeugte Untergruppe

$$[G, G] := \langle K(G) \rangle$$

ist die *Kommutator-Untergruppe* von G.

II.9.10 Bemerkung. Eine abelsche Gruppe ist dadurch ausgezeichnet, dass $g \cdot h \cdot g^{-1} \cdot h^{-1} = e$ für alle $g, h \in G$ gilt, also dass $[G, G] = \{e\}$. Deshalb ist die „Größe“ von $[G, G]$ ebenfalls ein Maß dafür, wie stark sich G von einer abelschen Gruppe unterscheidet.

II.9.11 Lemma. *Die Untergruppe* $[G, G]$ *ist ein Normalteiler von* G.

Beweis. **Schritt 1.** Man überprüft sofort, dass

$$\forall g \in G: \quad g \cdot K(G) \cdot g^{-1} \subset K(G)$$

gilt. Wie im Beweis von Beobachtung II.9.2 leiten wir daraus ab, dass

$$\forall g \in G: \quad g \cdot K(G) \cdot g^{-1} = K(G).$$

Schritt 2. Für jedes Element $g \in G$ ist $g \cdot [G, G] \cdot g^{-1}$ eine Untergruppe. Nach Schritt 1 enthält sie $K(G)$. Aus Satz II.4.10 folgt

$$[G, G] \subset g \cdot [G, G] \cdot g^{-1}.$$

Wie zuvor schließen wir, dass

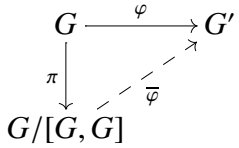
$$g \cdot [G, G] \cdot g^{-1} \subset g \cdot (g^{-1} \cdot [G, G] \cdot g) \cdot g^{-1} = [G, G]$$

für $g \in G$ gilt. □

Aus den Definitionen ergibt sich unmittelbar, dass $G/[G,G]$ eine abelsche Gruppe ist. Diese Konstruktion erfüllt sogar eine **universelle Eigenschaft**:

II.9.12 Lemma. *Es sei G eine Gruppe.*

i) *Für jede **abelsche** Gruppe G' und jeden Homomorphismus $\varphi\colon G \longrightarrow G'$ existiert genau ein Homomorphismus $\overline{\varphi}\colon G/[G,G] \longrightarrow G'$, so dass das Diagramm*



kommutiert.

ii) *Es sei $H \lhd G$ ein Normalteiler, so dass G/H abelsch ist. Dann gilt $[G,G] \subset H$.*

Beweis. i) In (II.16) haben wir $K(G) \subset \mathrm{Ker}(\varphi)$ nachgerechnet. Es folgt $[G,G] \subset \mathrm{Ker}(\varphi)$. Die Aussage ist damit eine Konsequenz aus Satz II.9.7.

ii) Sei

$$\begin{aligned} \varrho\colon G &\longrightarrow G/H \\ g &\longmapsto [g]. \end{aligned}$$

Wie in i) gesehen hat man $[G,G] \subset \mathrm{Ker}(\varrho) = H$. □

Das Lemma besagt, dass $[G,G]$ der kleinste Normalteiler ist, für den die Faktorgruppe abelsch ist.

II.9.13 Definition. Die Gruppe $G/[G,G]$ nennt man die *Verabelung* von G.

II.9.14 Aufgabe (Kommutierende Normalteiler). Es seien G eine Gruppe und H, J Normalteiler von G, so dass $H \cap J = \{e\}$.

a) Beweisen Sie

$$\forall h \in H,\ j \in J: \quad h \cdot j = j \cdot h.$$

b) Nun sei G eine endliche Gruppe, und es gelte zusätzlich $\#G = \#H \cdot \#J$. Zeigen Sie

$$G \cong H \times J.$$

II.9.15 Aufgabe (Untergruppen von Primzahlindex). Geben Sie für jede Primzahl $p > 2$ endliche Gruppen G und H an, so dass $\#(G/H) = p$ und H kein Normalteiler von G ist.

II.9.16 Aufgabe (Die orthogonale Gruppe). a) Zeigen Sie, dass die orthogonale Gruppe $\mathrm{O}(2)$ von Spiegelungen erzeugt wird.

b) Es sei $N \trianglelefteq \mathrm{O}(2)$ eine normale Untergruppe, die eine Spiegelung enthält. Beweisen Sie $N = \mathrm{O}(2)$.

c) Es seien $r \in \mathrm{O}(2)$ eine Drehung und $G = \langle r \rangle$. Weisen Sie nach, dass N eine normale Untergruppe ist.

d) Wann ist die Untergruppe G aus Teil c) endlich?

II.9.17 Aufgabe (Die alternierende Gruppe A_4). a) Zeigen Sie, dass e zusammen mit den Permutationen vom Zykeltyp $(2,2)$ eine normale Untergruppe $H \lhd A_4$ bildet.

b) Geben Sie einen Homomorphismus $\varphi\colon A_4 \longrightarrow \mathbb{Z}_3$ mit $\mathrm{Ker}(\varphi) = H$ an, H die Untergruppe aus Teil a).

II.9.18 Aufgabe (Die Kommutatoruntergruppe von S_n). Beweisen Sie, dass für $n \geq 2$

$$[S_n, S_n] = A_n.$$

II.9.19 Aufgabe (Die Kommutatoruntergruppe von GL_n). Es seien k ein Körper und $n \geq 2$. Falls $n = 2$, gelte $\#k \geq 3$. Zeigen Sie

$$[\mathrm{GL}_n(k), \mathrm{GL}_n(k)] = \mathrm{SL}_n(k).$$

II.10 Die Isomorphiesätze

Die Isomorphiesätze stellen Isomorphismen zwischen gewissen Gruppen, die auf verschiedene Weise konstruiert wurden, her. Mit dem ersten Isomorphiesatz werden wir z.B. die Isomorphieklassen zahlreicher Faktorgruppen identifizieren. Im Allgemeinen kann eine der beiden Gruppen, die im jeweiligen Isomorphiesatz auftreten, in Bezug auf eine gewisse Eigenschaft leichter zu untersuchen sein als die andere. Mit dem entsprechenden Isomorphiesatz kann man Eigenschaften der einen Gruppe aber auf die andere übertragen.

II.10.1 Der erste Isomorphiesatz. *Es seien G, G' Gruppen und $\varphi\colon G \longrightarrow G'$ ein Homomorphismus. Dann induziert φ einen* ***Isomorphismus***

$$\widetilde{\varphi}\colon G/\mathrm{Ker}(\varphi) \longrightarrow \mathrm{Im}(\varphi).$$

Beweis. Nach Satz II.9.7 haben wir einen Homomorphismus

$$\overline{\varphi}\colon G/\mathrm{Ker}(\varphi) \longrightarrow G'.$$

Da $\varphi = \overline{\varphi} \circ \pi$ und π surjektiv ist, folgt

$$\mathrm{Im}(\overline{\varphi}) = \mathrm{Im}(\varphi).$$

Auf diese Weise gelangen wir zu der Surjektion

$$\begin{array}{rcl} \widetilde{\varphi}\colon G/\mathrm{Ker}(\varphi) & \longrightarrow & \mathrm{Im}(\varphi) \\ [g] & \longmapsto & \overline{\varphi}([g]). \end{array}$$

Es sei $[g] \in G/\mathrm{Ker}(\varphi)$ ein Element mit $\widetilde{\varphi}([g]) = e$. Aus $\widetilde{\varphi}([g]) = \overline{\varphi}([g]) = \varphi(g)$ leiten wir $e \in \mathrm{Ker}(\varphi)$ und damit $[g] = [e]$ ab. Damit haben wir $\mathrm{Ker}(\widetilde{\varphi}) = \{[e]\}$ nachgewiesen. Lemma II.4.5 zeigt, dass $\widetilde{\varphi}$ injektiv ist. □

II.10.2 Beispiele. i) Wir betrachten für $n \geq 1$

$$\begin{array}{rcl} \varphi\colon \mathbb{Z} & \longrightarrow & \mathbb{Z}_n \\ k & \longmapsto & [k]_n. \end{array}$$

Diese Abbildung ist surjektiv, und wir haben $\mathrm{Ker}(\varphi) = n \cdot \mathbb{Z}$ (vgl. Beispiel II.4.3, ii), so dass

$$\mathbb{Z}/(n \cdot \mathbb{Z}) \cong \mathbb{Z}_n$$

ii) Es seien $n \geq 1$ und k ein Körper. Der Homomorphismus $\mathrm{Det}\colon \mathrm{GL}_n(k) \longrightarrow k^\star$ ist surjektiv, und der Kern ist nach Definition (Beispiel II.4.6, i) die spezielle lineare Gruppe $\mathrm{SL}_n(k)$. Wir schließen, dass

$$\mathrm{GL}_n(k)/\mathrm{SL}_n(k) \cong k^\star.$$

iii) Der Homomorphismus $\mathrm{Sign}\colon S_n \longrightarrow \{\pm 1\}$ ist surjektiv. Der Kern ist die alternierende Gruppe A_n (Definition II.5.22). Wir schließen

$$S_n/A_n \cong \{\pm 1\} \cong \mathbb{Z}_2.$$

iv) Wir definieren (in den Bezeichnungen von Beispiel II.4.16, ii)

$$\begin{array}{rcll} \varphi\colon D_6 & \longrightarrow & D_3 & \\ r^i & \longmapsto & \varrho^i, & \varrho \text{ die Drehung um } \frac{2\cdot\pi}{3} \\ r^i \cdot s & \longmapsto & \varrho^i \cdot s, & i = 0, ..., 5. \end{array}$$

Die Gleichung

$$\varphi(s \cdot r) = \varphi(r^5 \cdot s) = \varrho^5 \cdot s = \varrho^2 \cdot s = s \cdot \varrho = \varphi(s) \cdot \varphi(r)$$

impliziert, dass φ ein Homomorphismus ist (Übung). Da φ surjektiv ist, erkennen wir

$$D_6/\langle r^3 \rangle \cong D_3.$$

II.10.3 Der zweite Isomorphiesatz. *Es seien G eine Gruppe und H, J Untergruppen von G. Wenn J ein Normalteiler von G ist, dann ist*

- ⋆ $H \cdot J := \{\, h \cdot j \in G \mid h \in H,\ j \in J \,\}$ *eine Untergruppe von G,*
- ⋆ $H \cap J$ *ein Normalteiler von H,*

und die Gruppen[25]

$$(H \cdot J)/J \quad \textit{und} \quad H/(H \cap J)$$

sind isomorph.

Beweis. Wir zeigen mit dem Kriterium aus Lemma II.4.5, dass $H \cdot J$ eine Untergruppe ist. Zunächst gilt $e \in H$ und $e \in J$, so dass $e = e \cdot e \in H \cdot J$ und $H \cdot J \neq \emptyset$. Für $h, h' \in H$ und $j, j' \in J$ berechnen wir

$$\begin{aligned} (h \cdot j)^{-1} \cdot (h' \cdot j') &= j^{-1} \cdot h^{-1} \cdot h' \cdot j' = h^{-1} \cdot (\underbrace{h \cdot j^{-1} \cdot h^{-1}}_{=: j'' \in J}) \cdot h' \cdot j' \\ &= h^{-1} \cdot h' \cdot (\underbrace{h'^{-1} \cdot j'' \cdot h'}_{=: j''' \in J}) \cdot j' = (\underbrace{h^{-1} \cdot h'}_{\in H}) \cdot (\underbrace{j''' \cdot j'}_{\in J}) \in H \cdot J. \end{aligned}$$

Wir verknüpfen die Inklusion $\iota\colon H \longrightarrow H \cdot J$ und die Surjektion $\pi\colon H \cdot J \longrightarrow (H \cdot J)/J$ zu der Abbildung

$$\widetilde{\iota}\colon H \longrightarrow (H \cdot J)/J.$$

Diese Abbildung ist offenkundig surjektiv und hat den Kern $H \cap J$. Somit ist $H \cap J$ ein Normalteiler von H (Beispiel II.9.6, iv), und die behauptete Isomorphie

$$(H \cdot J)/J \cong H/(H \cap J)$$

folgt aus dem ersten Isomorphiesatz II.10.1. □

[25] Da J ein Normalteiler von G ist, ist J auch ein Normalteiler von $H \cdot J$.

Der zweite Isomorphiesatz wird beim Beweis der Sylowsätze im folgenden Abschnitt zum Einsatz kommen.

II.10.4 Der dritte Isomorphiesatz. *Es seien G eine Gruppe und H, J Normalteiler von G. Wenn $H \subset J$, dann ist J/H ein Normalteiler von G/H.*[26]

Beweis. Es sei $\pi\colon G \longrightarrow G/J$ die "Standardsurjektion". Wegen $H \subset J = \mathrm{Ker}(\pi)$ induziert π nach dem ersten Isomorphiesatz II.10.1 eine Surjektion

$$\overline{\pi}\colon G/H \longrightarrow G/J.$$

Der Kern von $\overline{\pi}$ ist offenbar J/H, und wir schließen abermals mit dem ersten Isomorphiesatz. □

II.11 Die Sylowsätze

Die Sylowsätze,[27] die in diesem Abschnitt entwickelt werden, sind Hilfsmittel zur Klassifikation endlicher Gruppen. Sie illustrieren die bereits formulierte Idee, eine Gruppe mit Hilfe ihrer Untergruppen zu analysieren.

In diesem Abschnitt seien stets G eine endliche Gruppe, $n := \#G$ ihre Ordnung und p eine Primzahl, die n teilt. Wir setzen

$$k := \max\{\varkappa \in \mathbb{N} \mid p^{\varkappa} | n\}$$

und

$$m := \frac{n}{p^k}.$$

Dann gilt $p \nmid m$, d.h. $\mathrm{ggT}(p, m) = 1$.

II.11.1 Der erste Sylowsatz. *Die Untergruppe G enthält eine Untergruppe H der Ordnung p^k.*

II.11.2 Definition. Eine Untergruppe H von G mit p^k Elementen ist eine *p-Sylow-Untergruppe* von G.

II.11.3 Hilfssatz. *Für $l \in \{1, ..., k\}$ gilt*

$$p^{k-l+1} \nmid \binom{n}{p^l}.$$

Beweis. Wir schreiben

$$\binom{n}{p^l} = \frac{n!}{(n-p^l)! \cdot p^l!} = \frac{n}{p^l} \cdot \frac{(n-1)!}{((n-1)-(p^l-1))! \cdot (p^l-1)!} = p^{k-l} \cdot m \cdot \binom{n-1}{p^l-1}.$$

Wegen $p \nmid m$ ist

$$p \nmid \binom{n-1}{p^l-1}$$

[26] Die Gruppe $J/H = \{[j] = j \cdot H \mid j \in J\}$ ist eine Untergruppe von $G/H = \{[g] = g \cdot H \mid g \in G\}$.

[27] Peter Ludwig Mejdell Sylow (1832 - 1918), norwegischer Mathematiker

zu zeigen. Für $\lambda \in \{ 1, ..., p^l - 1 \}$ sei

$$\mu_\lambda := \max\{ \nu \in \mathbb{N} \mid p^\nu | \lambda \}.$$

Es gilt

$$0 \leq \mu_\lambda < l, \quad \lambda = 1, ..., p^l - 1. \tag{II.17}$$

Wir setzen weiter

$$\tau_\lambda := \frac{\lambda}{p^{\mu_\lambda}}, \quad \lambda = 1, ..., p^l - 1.$$

Damit finden wir

$$\frac{n - \lambda}{p^l - \lambda} = \frac{p^k \cdot m - \lambda}{p^l - \lambda} = \frac{p^{k-\mu_\lambda} \cdot m - \tau_\lambda}{p^{l-\mu_\lambda} - \tau_\lambda}, \quad \lambda = 1, ..., p^l - 1.$$

Es sei

$$a := \prod_{\lambda=1}^{p^l-1} (-\tau_\lambda).$$

Dann existieren ganze Zahlen $b, c \in \mathbb{Z}$, so dass

$$\beta := \binom{n-1}{p^l-1} = \frac{(n-1) \cdot \cdots \cdot (n-p^l+1)}{(p^l-1) \cdot \cdots \cdot (p^l-p^l+1)} = \prod_{\lambda=1}^{p^l-1} \frac{n-\lambda}{p^l-\lambda} = \frac{a + p \cdot b}{a + p \cdot c}$$

bzw.

$$\beta \cdot (a + p \cdot c) = a + p \cdot b. \tag{II.18}$$

Wegen $p \nmid \tau_\lambda$, $\lambda = 1, ..., p^l - 1$, gilt $p \nmid a$. Deshalb teilt p die Zahl $a + p \cdot b$ nicht und kann auf Grund von (II.18) auch nicht β teilen. □

Um jetzt den ersten Sylowsatz zu beweisen, lassen wir die Gruppe G auf einer geeigneten Menge $\mathfrak{M}$ wirken und erhalten H als Standgruppe eines geeigneten Elements in dieser Menge.

Beweis von Satz II.11.1. Wir betrachten die Menge

$$\mathfrak{M} := \{ M \subset G \mid \#M = p^k \}$$

der Teil**mengen** von G mit p^k Elementen. Es gilt

$$\#\mathfrak{M} = \binom{n}{p^k} = \binom{p^k \cdot m}{p^k}.$$

Wir arbeiten mit der Linkswirkung

$$\begin{aligned} \sigma \colon G \times \mathfrak{M} &\longrightarrow \mathfrak{M} \\ (g, M) &\longmapsto g \cdot M = \{ g \cdot m \in G \mid m \in M \}. \end{aligned}$$

Der Fall $l = k$ in Hilfssatz II.11.3 liefert

$$p \nmid \binom{n}{p^k}.$$

Die Menge $\mathfrak{M}$ ist die disjunkte Vereinigung ihrer verschiedenen G-Bahnen. Daher muss es eine G-Bahn in $\mathfrak{M}$ geben, deren Ordnung nicht durch p geteilt wird, d.h. es existiert ein Element $M \in \mathfrak{M}$, so dass

$$p \nmid \#(G \cdot M).$$

Nach Satz II.7.2 gilt

$$\#G = \#(G_M) \cdot \#(G \cdot M),$$

so dass

$$p^k | \#G_M \tag{II.19}$$

folgt. Für $g \in G_M$ gilt $g \cdot M = M$, so dass insbesondere

$$\forall g \in G_M \forall m \in M : \quad g \cdot m \in M.$$

Sei $m_0 \in M$. Dann haben wir $G_M \cdot m_0 \subset M \subset G$. Da die Rechtsmultiplikation mit dem Gruppenelement m_0 injektiv ist (Lemma II.2.1), schließen wir

$$\#G_M = \#(G_M \cdot m_0) \leq \#M = p^k. \tag{II.20}$$

Aus (II.19) und (II.20) leiten wir $\#G_M = p^k$ ab. □

II.11.4 Folgerung (Der Satz von Cauchy[28]). *Die Gruppe G enthält ein Element der Ordnung p.*

Beweis. Auf Grund des ersten Sylowsatzes II.11.1 können wir ohne Beschränkung der Allgemeinheit $\#G = p^k$ annehmen. Für $g \in G \setminus \{e\}$ gilt nach Folgerung II.7.5

$$1 < \mathrm{Ord}(g) | p^k.$$

Es existiert folglich ein $l \in \{1, ..., k\}$ mit $\mathrm{Ord}(g) = p^l$. Das Element $g^{p^{l-1}}$ hat Ordnung p. □

II.11.5 Der zweite Sylowsatz. *Je zwei p-Sylowgruppen H, H' von G sind konjugiert, d.h. es existiert ein $g \in G$ mit*

$$H = g \cdot H' \cdot g^{-1}.$$

II.11.6 Der dritte Sylowsatz. *Die Anzahl t der p-Sylowgruppen von G ist kongruent* 1 *modulo p und ein Teiler von m:*

$$t \equiv 1 \bmod p, \quad t | m.$$

Diesmal betrachten wir die Menge

$$\mathfrak{H} := \{ H \subset G \,|\, H \text{ ist } p\text{-Sylowuntergruppe} \},$$

die nach dem ersten Sylowsatz II.11.1 nichtleer ist. Die Gruppe G wirkt durch Konjugation von links auf $\mathfrak{H}$:

$$\begin{array}{rccl} \tau \colon & G \times \mathfrak{H} & \longrightarrow & \mathfrak{H} \\ & (g, H) & \longmapsto & g \cdot H \cdot g^{-1} = \{ g \cdot h \cdot g^{-1} \,|\, h \in H \}. \end{array}$$

Wir nummerieren die Elemente von $\mathfrak{H}$:

$$\mathfrak{H} = \{ H_1, ..., H_t \}, \quad t := \#\mathfrak{H}.$$

[28] Augustin Louis Cauchy (1789 - 1857), französischer Mathematiker.

II.11.7 Hilfssatz. *Für $h \in H_1$ und $j \in \{1, ..., t\}$ gilt*

$$h \cdot H_j \cdot h^{-1} = H_j \quad \Longleftrightarrow \quad h \in H_1 \cap H_j.$$

Beweis. Die Richtung „$\Longleftarrow$“ ist klar, weil H_j eine Untergruppe ist.

Für „$\Longrightarrow$“ sei

$$K_j = \{ h \in H_1 \mid h \cdot H_j \cdot h^{-1} = H_j \}$$

der Durchschnitt der Standgruppe von H_j (bzgl. τ) mit H_1. Wie im Beweis des zweiten Isomorphiesatzes II.10.3 zeigt man, dass $K_j \cdot H_j$ eine Untergruppe von G ist. Ferner ist H_j offenbar normal in $K_j \cdot H_j$.

Aus dem besagten zweiten Isomorphiesatz[29] (mit $K_j \cdot H_j$ in der Rolle von G und K_j bzw. H_j in der Rolle von H bzw. J) folgern wir:

$$(K_j \cdot H_j)/H_j \cong K_j/(K_j \cap H_j).$$

Mit dem Satz von Lagrange (Folgerung II.7.4) erhalten wir

$$\#(K_j \cdot H_j) = \#H_j \cdot \#(K_j/(K_j \cap H_j)).$$

Da K_j eine Untergruppe von H_j ist, sind $\#K_j$ und $\#(K_j \cap H_j)$ Potenzen von p. Es folgt

$$\#(K_j \cdot H_j) = p^l$$

für ein $l \geq k$. Auf der anderen Seite ist $K_j \cdot H_j$ eine Untergruppe von G und erfüllt damit

$$\#(K_j \cdot H_j) | \#G.$$

Aus der Definition von k folgt somit $l = k$. Wegen $H_j \subset K_j \cdot H_j$ und $\#H_j = p^k = \#(K_j \cdot H_j)$ haben wir $H_j = K_j \cdot H_j$ und deshalb $K_j \subset H_j$. □

Beweis des dritten Sylowsatzes II.11.6 *(Teil 1).* Wir schränken die Wirkung τ auf H_1 ein und erhalten die Wirkung

$$\begin{array}{rcl} \tau' \colon H_1 \times \mathfrak{H} & \longrightarrow & \mathfrak{H} \\ (g, H) & \longmapsto & g \cdot H \cdot g^{-1}. \end{array}$$

Wir untersuchen die Anzahl der Elemente in den verschiedenen H_1-Bahnen in $\mathfrak{H}$. Die Bahn von H_1 enthält nur ein Element, und zwar H_1. Für $j \neq 1$ ist die Standgruppe von H_j nach Hilfssatz II.11.7 die Gruppe $H_1 \cap H_j$ und damit eine echte Untergruppe von H_1, so dass die Anzahl ihrer Elemente von der Form p^l mit $0 \leq l \leq k-1$ ist. Die Bahn von H_j enthält somit p^{k-l} Elemente. Wegen $k - l \geq 1$ ist die Anzahl der Elemente in der Bahn von H_j durch p teilbar, $j = 2, ..., t$.

Die Menge $\mathfrak{H}$ zerfällt also in H_1-Bahnen, von denen eine ein Element und alle anderen eine durch p teilbare Anzahl von Elementen umfassen. Das zeigt $t \equiv 1 \bmod p$. □

[29] Hier sieht man deutlich, dass die zweite Beschreibung günstiger für die Berechnung der Ordnung ist.

Beweis des zweiten Sylowsatzes II.11.5. Wir haben zu zeigen, dass $\mathfrak{H}$ aus einer einzigen G-Bahn besteht. Die G-Bahn von H_1 ist eine disjunkte Vereinigung von H_1-Bahnen, darunter die Bahn $\{H_1\}$. Wie zuvor folgt

$$\#(G \cdot H_1) \equiv 1 \bmod p. \tag{II.21}$$

Sei $r \in \{2, ..., t\}$, so dass $H_r \notin G \cdot H_1$. Jetzt schränken wir die Wirkung τ auf H_r ein und erhalten

$$\begin{array}{rcl} \tau'' \colon H_r \times \mathfrak{H} & \longrightarrow & \mathfrak{H} \\ (g, H) & \longmapsto & g \cdot H \cdot g^{-1}. \end{array}$$

Wir können die Bahn $G \cdot H_1$ auch als disjunkte Vereinigung von H_r-Bahnen schreiben. Da $H_r \notin G \cdot H_1$, ist die Bahn $\{H_r\}$ nicht darunter. Der oben geführte Beweis des dritten Sylowsatzes zeigt, dass die Anzahl der Elemente in jeder in $G \cdot H_1$ vorkommenden H_r-Bahn durch p teilbar ist, so dass

$$p | \#(G \cdot H_1).$$

Dies widerspricht (II.21). Daher ist jede der p-Sylowuntergruppen H_1, ..., H_t in der G-Bahn von H_1 enthalten und daher zu H_1 konjugiert. □

Beweis des dritten Sylowsatzes II.11.6 *(Teil 2).* Aus der Formel

$$\#G = \#G_{H_1} \cdot \#(G \cdot H_1) = \#G_{H_1} \cdot t$$

folgt

$$t | \#G, \quad \text{d.h.} \quad t | (p^k \cdot m).$$

Wegen $\mathrm{ggT}(p^k, t) = 1$ heißt das $t | m$. □

II.11.8 Aufgabe (Gruppen der Ordnung 1000). Beweisen Sie, dass eine endliche Gruppe G der Ordnung 1000 einen Normalteiler H mit $\{e\} \subsetneq H \subsetneq G$ besitzt.

II.11.9 Aufgabe (Zyklische Gruppen). Es seien $p < q$ Primzahlen, so dass $q \not\equiv 1 \bmod p$, und G eine endliche Gruppe der Ordnung $p \cdot q$.

a) Geben Sie mindestens vier Beispiele für Paare (p, q) mit den obigen Eigenschaften an.

b) Beweisen Sie, dass G einen Normalteiler der Ordnung p und einen Normalteiler der Ordnung q hat.

c) Zeigen Sie, dass G isomorph zu $\mathbb{Z}_p \times \mathbb{Z}_q$ ist, und folgern Sie, dass G zyklisch ist.

II.12 Klassifikation endlicher Gruppen bis zur Ordnung 14

Nachdem wir uns ausgiebig mit dem Gruppenbegriff auseinandergesetzt haben, wollen wir in diesem und dem folgenden Abschnitt das Klassifikationsproblem untersuchen. Sobald man eine mathematische Struktur definiert und einen Isomorphiebegriff eingeführt hat, stellt sich die Frage nach der Klassifikation der entsprechenden Objekte bis auf Isomorphie. Man möchte dabei eine Liste von Objekten erstellen, so dass jedes Objekt, das

die betrachtete mathematische Struktur trägt, zu genau einem Objekt aus der Liste isomorph ist. Man lernt Beispiele dafür in der linearen Algebra kennen: Es sei k ein Körper. Dann ist jeder **endlichdimensionale** k-Vektorraum zu genau einem Vektorraum aus der Liste k^n, $n \in \mathbb{N}$, isomorph. (Dabei sei $k^0 = \{0\}$.) Auch der Satz über die Jordansche Normalform ist ein Klassifikationssatz. Er beschreibt die Isomorphieklassen endlichdimensionaler Moduln über dem Polynomring $k[t]$, k ein **algebraisch abgeschlossener** Körper.

Es gibt einen allgemeinen Klassifikationssatz in der Gruppentheorie, der die **Bausteine** für alle endlichen Gruppen beschreibt. Um die Bausteine zu verstehen, geht man von folgender Vorstellung aus: Es seien G eine Gruppe und $H \lhd G$ ein **Normalteiler**. Dann ist G/H wieder eine Gruppe (s. Abschnitt II.9). Wir notieren dies als sogenannte **kurze exakte Sequenz**:

$$\{1\} \longrightarrow H \longrightarrow G \longrightarrow G/H \longrightarrow \{1\}.$$

Bei solch einer kurzen exakten Sequenz stellt man sich die Gruppe G aus den Gruppen H und G/H „aufgebaut“ vor. Die Bauvorschrift kann dabei allerdings kompliziert sein.[30] Bei den ganzen Zahlen haben wir diejenigen Zahlen, die sich nicht auf nichttriviale Weise als Produkt kleinerer ganzer Zahlen schreiben lassen, als **Primzahlen** bezeichnet. Die Gruppen, die sich nicht auf obige Weise in kleinere Gruppen zerlegen lassen, sehen folgendermaßen aus:

II.12.1 Definition. Eine Gruppe heißt *einfach*, wenn sie außer $\{e\}$ und G keine Normalteiler hat.

II.12.2 Beispiel. Eine endliche Gruppe, deren Ordnung eine Primzahl ist, ist einfach.

II.12.3 Aufgabe (Jordan–Hölder[31]-Filtrierung). Zu jeder endlichen Gruppe H gibt es eine Folge

$$\{1\} =: H_0 \subsetneq H_1 \subsetneq \cdots \subsetneq H_{s-1} \subsetneq H_s := H$$

von Untergruppen, so dass H_{i-1} ein Normalteiler von H_i und die Gruppe

$$\overline{H}_i := H_i/H_{i-1}$$

einfach ist, $i = 1, ..., s$.

Bei dieser Jordan–Hölder-Filtrierung ist s eindeutig bestimmt, und zu einer weiteren Jordan–Hölder-Filtrierung

$$\{1\} =: H'_0 \subsetneq H'_1 \subsetneq \cdots \subsetneq H'_{s-1} \subsetneq H'_s := H$$

gibt es eine Permutation $\sigma\colon \{1, ..., s\} \longrightarrow \{1, ..., s\}$,[32] so dass

$$\overline{H}_i \cong \overline{H}'_{\sigma(i)}, \quad i = 1, ..., s.$$

Die Jordan–Hölder-Filtrierung ist also ein gewisses Analogon zur Primfaktorzerlegung. Allerdings kann H i.A. **nicht** aus der Jordan–Hölder-Filtrierung rekonstruiert werden.

[30] Im Allgemeinen wird G **nicht** isomorph zum direkten Produkt $H \times (G/H)$ oder zu einem semidirekten Produkt (s. Definition II.12.8 und Satz II.12.9) $H \rtimes (G/H)$ sein.

[31] Otto Ludwig Hölder (1859 - 1937), deutscher Mathematiker.

[32] Diese Aussagen sind etwas schwieriger zu beweisen, so dass die Leserin bzw. der Leser nicht frustriert zu sein braucht, wenn sie bzw. er das nicht direkt einsieht.

Ein Meilenstein der Mathematikgeschichte ist die Klassifikation der einfachen endlichen Gruppen: Es gibt eine Liste von einfachen endlichen Gruppen,[33] so dass jede einfache endliche Gruppe isomorph zu genau einer Gruppe aus dieser Liste ist. Dieses Ergebnis ist in jeder Hinsicht bemerkenswert. Es waren mehr als 100 Mathematiker daran beteiligt, und der vollständige Beweis umfasst wohl mehr als 10.000 Seiten (s. [4]).

In diesem Abschnitt werden wir bescheidener sein und uns darauf beschränken, alle Gruppen bis zur Ordnung 14 mit Hilfe der bisher bewiesenen Sätze zu klassifizieren. Dabei sind jedoch nur die Gruppen $\mathbb{Z}_1$, $\mathbb{Z}_2$, $\mathbb{Z}_3$, $\mathbb{Z}_5$, $\mathbb{Z}_7$, $\mathbb{Z}_{11}$ und $\mathbb{Z}_{13}$ einfach. Für die restlichen Gruppen G werden wir einen geeigneten Normalteiler H auffinden und G aus H und G/H aufbauen.

Gruppen der Ordnung p^2, p eine Primzahl

II.12.4 Satz. *Es seien p eine Primzahl und G eine endliche Gruppe der Ordnung p^2. Dann ist G entweder zu $\mathbb{Z}_{p^2}$ oder zu $\mathbb{Z}_p \times \mathbb{Z}_p$ isomorph. Insbesondere ist G abelsch.*

Beweis. Entweder enthält G ein Element der Ordnung p^2, so dass $G = \langle g \rangle$ und $G \cong \mathbb{Z}_{p^2}$, oder jedes Element $g \in G \setminus \{e\}$ hat Ordnung p (Folgerung II.7.5). Nach Satz II.7.8 können wir $g \in Z(G) \setminus \{e\}$ wählen. Dann ist $\langle g \rangle$ insbesondere ein Normalteiler von G (Beispiel II.9.6, ii). Sei weiter $h \in G \setminus \langle g \rangle$. Dann gilt:

- $\star$ $\#\langle g \rangle = p = \#\langle h \rangle$.
- $\star$ $\langle g \rangle \cap \langle h \rangle = \{e\}$. (Ansonsten folgte mit Folgerung II.7.4 $\langle g \rangle = \langle h \rangle$ und $h \in \langle g \rangle$.)
- $\star$ $\langle g \rangle \cdot \langle h \rangle$ ist eine Untergruppe von G (Zweiter Isomorphiesatz II.10.3).

Auf Grund des zweiten Punkts gilt $\langle g \rangle \subsetneq \langle g \rangle \cdot \langle h \rangle \subset G$. Da die Ordnung von $\langle g \rangle \cdot \langle h \rangle$ gleichzeitig ein Teiler der Ordnung von G ist, folgt $\#(\langle g \rangle \cdot \langle h \rangle) = p^2$ und $\langle g \rangle \cdot \langle h \rangle = G$.

- $\star$ Wegen $g \in Z(G)$ gilt $g^i \cdot h^j = h^j \cdot g^i$, $i, j \in \{ 0, ..., p-1 \}$.

Somit ist

$$\begin{array}{rcl} \varphi\colon \mathbb{Z}_p \times \mathbb{Z}_p & \longrightarrow & G \\ (i, j) & \longmapsto & g^i \cdot h^j \end{array}$$

ein surjektiver und damit bijektiver Gruppenhomomorphismus. □

Gruppen der Ordnung $2 \cdot p$, p eine Primzahl

II.12.5 Satz. *Es seien $p > 2$ eine Primzahl und G eine endliche Gruppe der Ordnung $2p$. Dann ist G entweder zu $\mathbb{Z}_{2p}$ oder zu D_p isomorph.*

Beweis. Nach dem Satz von Cauchy (Folgerung II.11.4) gibt es ein Element $g \in G$ der Ordnung p und ein Element $h \in G$ der Ordnung 2. Da die Menge $G/\langle g \rangle$ der Rechtsnebenklassen genau zwei Elemente umfasst, ist $\langle g \rangle$ nach Beispiel II.9.6, v), ein Normalteiler

[33] Sie ist allerdings zu umfangreich, um hier reproduziert zu werden (vgl. `http://en.wikipedia.org/wiki/List_of_finite_simple_groups#References`).

von G. Deshalb ist $\langle g\rangle \cdot \langle h\rangle$ eine Untergruppe von G. Da $2 \nmid p = \#\langle g\rangle$, gilt $h \notin \langle g\rangle$. Daraus folgt $\#(\langle g\rangle \cdot \langle h\rangle) = 2p$ und $\langle g\rangle \cdot \langle h\rangle = G$. Außerdem existiert eine Zahl $l \in \{1, ..., p-1\}$ mit

$$h \cdot g \cdot h \overset{h^2=e}{=} h \cdot g \cdot h^{-1} = g^l.$$

Wir haben

$$g = h^2 \cdot g \cdot h^2 = h \cdot g^l \cdot h = (h \cdot g \cdot h)^l = g^{l^2},$$

so dass

$$g^{l^2-1} = e.$$

Mit Folgerung II.7.5 schließen wir

$$p|(l^2-1), \quad \text{d.h.} \quad p|(l-1) \vee p|(l+1).$$

Das bedeutet wegen $1 \leq l \leq p-1$, dass $l = 1$ oder $l = p-1$.

Fall 1. $l = 1$. Das heißt $h \cdot g = g \cdot h$, und deswegen ist

$$\begin{array}{rcl} \varphi\colon \mathbb{Z}_p \times \mathbb{Z}_2 & \longrightarrow & G \\ (i,j) & \longmapsto & g^i \cdot h^j \end{array}$$

ein Isomorphismus. Man beachte, dass das Element $(1,1) \in \mathbb{Z}_p \times \mathbb{Z}_2$ Ordnung $2p$ hat, so dass

$$\mathbb{Z}_p \times \mathbb{Z}_2 \cong \mathbb{Z}_{2p}$$

gilt.

Fall 2. $l = p-1$. Hier haben wir

$$h \cdot g = g^{p-1} \cdot h,$$

und

$$\begin{array}{rcl} \varphi\colon D_p & \longrightarrow & G \\ r^i \cdot s^j & \longmapsto & g^i \cdot h^j, \quad i = 0, ..., p-1,\ j = 0, 1, \end{array}$$

ist ein Isomorphismus. □

Gruppen der Ordnung 8

Die erste Ordnung, die nicht durch die Sätze II.12.4 und II.12.5 abgedeckt ist, ist Ordnung 8. Hier kennen wir bereits die Gruppen

$$\mathbb{Z}_8, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \quad \mathbb{Z}_4 \times \mathbb{Z}_2 \quad \text{und} \quad D_4.$$

Wir werden jetzt mit ähnlichen Methoden wie oben das Klassifikationsproblem für Gruppen der Ordnung 8 studieren und dabei „entdecken“, dass es neben den obigen Gruppen noch eine weitere Gruppe der Ordnung 8 gibt.

Fall 1. Die Gruppe G enthalte ein Element g der Ordnung 8. Dann gilt $G = \langle g\rangle$ und $G \cong \mathbb{Z}_8$.

Fall 2. Jedes Element aus G habe Ordnung 2. Dann ist G abelsch, denn

$$\forall g, h \in G: \quad (g \cdot h) \cdot (g \cdot h) = e \overset{g^2=e}{\Longrightarrow} h \cdot g \cdot h = g \overset{h^2=e}{\Longrightarrow} g \cdot h = h \cdot g.$$

Man wähle $g_1, g_2, g_3 \in G$ mit $g_1 \neq e$, $g_2 \in G \setminus \langle g_1 \rangle$ und $g_3 \in G \setminus (\langle g_1 \rangle \cdot \langle g_2 \rangle)$. Dann ist

$$\begin{aligned} \varphi\colon \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 &\longrightarrow G \\ (i_1, i_2, i_3) &\longmapsto g_1^{i_1} \cdot g_2^{i_2} \cdot g_3^{i_3} \end{aligned}$$

ein Isomorphismus.

Fall 3. Es gebe ein Element $g \in G$ der Ordnung 4 und ein Element $h \in G$ der Ordnung 2 mit $h \notin \langle g \rangle$. Nach Beispiel II.9.6, v), ist $\langle g \rangle$ ein Normalteiler von G. Wir folgern, dass $G = \langle g \rangle \cdot \langle h \rangle$ und dass ein $j \in \{1, 2, 3\}$ mit

$$h \cdot g \cdot h = g^j$$

existiert. Für $j = 1$ bzw. $j = 3$ bedeutet das $h \cdot g = g \cdot h$ bzw. $h \cdot g = g^3 \cdot h$ und $G \cong \mathbb{Z}_4 \times \mathbb{Z}_2$ bzw. $G \cong D_4$ (vgl. Beweis von Satz II.12.5). Der Fall $j = 2$ ist unmöglich, weil Konjugation mit h ein Automorphismus der Gruppe G ist. Somit hat $h \cdot g \cdot h$ dieselbe Ordnung wie g, also 4. Das Element g^2 hat dagegen Ordnung 2.

Fall 4. Es gibt ein Element $g \in G$ der Ordnung 4, und jedes Element der Ordnung 2 ist in $\langle g \rangle$ enthalten. Mit anderen Worten: $l := g^2$ ist das einzige Element der Ordnung 2 in G. Für $h \in G \setminus \langle g \rangle$ hat man

$$G = \{ e, g, g^2, g^3, h, h \cdot g, h \cdot g^2, h \cdot g^3 \}.$$

Behauptung. *Es gilt* $g \cdot h = h \cdot g^3$.

Beweis. Wegen $h \notin \langle g \rangle$ haben wir $g \cdot h \neq e$ und $g \cdot h \neq g^2 = l$. Zudem folgt, dass h Ordnung 4 hat und h^2 Ordnung 2, so dass $h^2 = l$. Ebenso hat $g \cdot h$ Ordnung 4 und $(g \cdot h)^2$ Ordnung 2, i.e.

$$g \cdot h \cdot g \cdot h = l = h^2.$$

Wir schließen

$$g \cdot h \cdot g = h$$

und mit $g^{-1} = g^3$

$$g \cdot h = h \cdot g^3.$$

Damit ist die Behauptung gezeigt. □

Mit der Behauptung können wir die Verknüpfungstabelle von G erstellen:

	e	g	g^2	g^3	h	$h \cdot g$	$h \cdot g^2$	$h \cdot g^3$
e	e	g	g^2	g^3	h	$h \cdot g$	$h \cdot g^2$	$h \cdot g^3$
g	g	g^2	g^3	e	$h \cdot g^3$	h	$h \cdot g$	$h \cdot g^2$
g^2	g^2	g^3	e	g	$h \cdot g^2$	$h \cdot g^3$	h	$h \cdot g$
g^3	g^3	e	g	g^2	$h \cdot g$	$h \cdot g^2$	$h \cdot g^3$	h
h	h	$h \cdot g$	$h \cdot g^2$	$h \cdot g^3$	g^2	g^3	e	g
$h \cdot g$	$h \cdot g$	$h \cdot g^2$	$h \cdot g^3$	h	g	g^2	g^3	e
$h \cdot g^2$	$h \cdot g^2$	$h \cdot g^3$	h	$h \cdot g$	e	g	g^2	g^3
$h \cdot g^3$	$h \cdot g^3$	h	$h \cdot g$	$h \cdot g^2$	g^3	e	g	g^2

. (II.22)

Es stellt sich die Frage, ob die durch obige Tabelle erklärte Verknüpfung das Assoziativgesetz erfüllt. Man könnte das mühsam nachrechnen. Wir sparen uns diese Mühe und zeigen, dass eine Untergruppe Q von $\mathrm{GL}_2(\mathbb{C})$ die obige Verknüpfungstabelle realisiert.[34] Mit $i := \sqrt{-1}$ definieren wir die Matrizen

$$E := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad I := \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \quad J := \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \quad K := \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Wir erstellen die Verknüpfungstabelle

	E	I	J	K
E	E	I	J	K
I	I	$-E$	K	$-J$
J	J	$-K$	$-E$	I
K	K	J	$-I$	$-E$

. (II.23)

II.12.6 Satz. *Die Menge* $Q := \{ \pm E, \pm I, \pm J, \pm K \}$ *ist eine Untergruppe von* $\mathrm{GL}_2(\mathbb{C})$.

Beweis. Das Neutralelement $E \in \mathrm{GL}_2(\mathbb{C})$ ist in Q enthalten. Außerdem haben wir

$$(-E)^{-1} = -E \in Q, \quad (\pm I)^{-1} = \mp I \in Q, \quad (\pm J)^{-1} = \mp J \in Q, \quad (\pm K)^{-1} = \mp K \in Q.$$

Schließlich entnimmt man Tabelle (II.23), dass für $A, B \in \mathrm{GL}_2(\mathbb{C})$ aus $A, B \in Q$ auch $A \cdot B \in Q$ folgt. □

Bei den obigen Rechnungen hat uns neben der Gruppenstruktur von $\mathrm{GL}_2(\mathbb{C})$ auch die lineare Struktur von $M_2(\mathbb{C})$ geholfen.

Wir erkennen, dass es in Q kein Element der Ordnung 8 und genau ein Element der Ordnung 2, nämlich $-E$, gibt. Also verwirklicht diese Gruppe Fall 4 in den obigen Betrachtungen. (Man kann z.B. $g := I$ und $h := J$ setzen, um Verknüpfungstabelle (II.22) zu erhalten.)

Gruppen der Ordnung 12

In diesem Abschnitt werden wir die Sylow-Sätze anwenden, um alle Gruppen der Ordnung 12 aufzufinden. Auch hier werden wir auf eine uns bisher unbekannte Gruppe stoßen.

Es seien G eine Gruppe der Ordnung 12 und t die Anzahl ihrer 3-Sylow-Untergruppen. Nach dem dritten Sylowsatz II.11.6 haben wir

$$t \equiv 1 \bmod 3 \quad \text{und} \quad t|4.$$

Es gibt daher entweder genau eine 3-Sylow-Untergruppe oder genau vier.

Fall 1. Es gebe genau eine 3-Sylow-Untergruppe H. Diese ist dann ein Normalteiler von G. Wir wählen einen Erzeuger g für H. Zudem sei J eine 2-Sylow-Untergruppe. Sie umfasst 4 Elemente. Da 3 und 4 teilerfremd sind, haben wir $H \cap J = \{e\}$ und $G = H \cdot J$.

[34] Das widerspricht zwar unserem Entdeckergeist, spart uns dafür aber viel Zeit und macht uns mit einer weiteren wichtigen Gruppe vertraut.

Fall 1 a). Die Gruppe J sei zyklisch, und h sei ein Erzeuger für J. Für das Element $h \cdot g \cdot h^{-1} \in H$ gibt es zwei Optionen.

i) Es sei $h \cdot g \cdot h^{-1} = g$. Dann ist G abelsch und

$$\begin{aligned} \varphi\colon \mathbb{Z}_3 \times \mathbb{Z}_4 &\longrightarrow G \\ (i, j) &\longmapsto g^i \cdot h^j \end{aligned}$$

ist ein Isomorphismus.

ii) Es gelte $h \cdot g \cdot h^{-1} = g^2$, d.h. $h \cdot g = g^2 \cdot h$. Wie zu Beginn gesehen, gilt

$$G = \{\, g^i \cdot h^j \mid i = 0, 1, 2,\ j = 0, 1, 2, 3 \,\}.$$

Mit der Rechenregel $h \cdot g = g^2 \cdot h$ könnte man die Verknüpfungstafel für G erstellen. Wir lassen sie hier fort. Die Existenz einer Gruppe G, in der die gefundenen Rechenregeln gelten, werden wir am Ende dieses Abschnitts nachweisen.

Fall 1 b). Es gelte $J \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Es seien $h, l \in J \setminus \{e\}$ zwei verschiedene Elemente und $m = h \cdot l$, d.h. $J = \{\, e, h, l, m \,\}$. Es gibt Elemente $a, b \in \{\pm 1\}$ mit

$$h \cdot g \cdot h = g^a, \quad l \cdot g \cdot l = g^b, \quad m \cdot g \cdot m = g^{a \cdot b}.$$

Es eröffnen sich wiederum zwei Möglichkeiten.

i) Es gelte $a = b = a \cdot b = 1$. In diesem Fall sind G abelsch und

$$\begin{aligned} \varphi\colon \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_2 &\longrightarrow G \\ (i, j, k) &\longmapsto g^i \cdot h^j \cdot l^k \end{aligned}$$

ein Isomorphismus.

ii) Bei geeigneter Wahl von h und l gelte $a = 1, b = -1 = a \cdot b$. Dann folgt $g \cdot h = h \cdot g$, und das Element $u := g \cdot h$ hat Ordnung 6. Schließlich finden wir

$$l \cdot u = l \cdot g \cdot h = g^{-1} \cdot l \cdot h = g^{-1} \cdot h \cdot l \overset{h^2 = e}{=} g^{-1} \cdot h^{-1} \cdot l = h^{-1} \cdot g^{-1} \cdot l = u^{-1} \cdot l = u^5 \cdot l.$$

Die Abbildung

$$\begin{aligned} \varphi\colon D_6 &\longrightarrow G \\ r^i \cdot s^j &\longmapsto u^i \cdot l^j, \quad i = 0, ..., 5,\ j = 0, 1, \end{aligned}$$

ist ein Gruppenisomorphismus.

Fall 2. Es gebe 4 zueinander konjugierte 3-Sylow-Untergruppen. Die Vereinigung V dieser 3-Sylow-Untergruppen enthält genau 9 Elemente. Deshalb ist $J := (G \setminus V) \cup \{e\}$ die einzige 2-Sylow-Untergruppe. Insbesondere ist J ein Normalteiler von G. Für das Folgende seien H eine 3-Sylow-Untergruppe und g ein Erzeuger für H. Es gilt wieder $G = H \cdot J$.

Behauptung. *Es gilt $J \cong \mathbb{Z}_2 \times \mathbb{Z}_2$.*

Beweis. Wenn die Behauptung falsch wäre, wäre J zyklisch von der Ordnung 4. In diesem Fall sei $h \in J$ ein Erzeuger. Das Element $g \cdot h \cdot g^{-1}$ ist ein Element der Ordnung 4 in J. Daher gilt entweder $g \cdot h \cdot g^{-1} = h$ oder $g \cdot h \cdot g^{-1} = h^3$. Der erste Fall ist unmöglich, weil

G dann abelsch wäre und nur eine einzige 3-Sylow-Untergruppe enthielte.[35] Es gilt also $g \cdot h \cdot g^{-1} = h^3$, und wir berechnen

$$h \overset{g^3=e}{=} g^3 \cdot h \cdot g^{-3} = g^2 \cdot h^3 \cdot g^{-2} = g \cdot h^9 \cdot g^{-1} = h^{27} \overset{h^4=e}{=} h^3.$$

Das ist wegen $\mathrm{Ord}(h) = 4$ unmöglich. □

Wir schreiben $J = \{e, h, l, m\}$. Dabei gilt $h^2 = l^2 = m^2 = e$ und $h \cdot l = m$. Wegen $G = H \cdot J$ erzeugen g, h und l die Gruppe G. Konjugation mit g induziert eine Permutation von $\{h, l, m\}$. Wegen $\mathrm{Ord}(g) = 3$ ist diese Permutation entweder die Identität oder ein 3-Zykel. Die Identität scheidet aus, weil G sonst abelsch wäre. Wir können h, l und m so wählen, dass

$$g \cdot h \cdot g^{-1} = l, \quad g \cdot l \cdot g^{-1} = m, \quad g \cdot m \cdot g^{-1} = h.$$

Man kann nun explizit überprüfen (Übung), dass

$$\begin{array}{rcl} \psi\colon G & \longrightarrow & A_4 \\ h & \longmapsto & (1\ 2) \cdot (3\ 4) \\ l & \longmapsto & (1\ 3) \cdot (2\ 4) \\ g & \longmapsto & (2\ 3\ 4) \end{array}$$

einen Isomorphismus induziert.

II.12.7 Aufgabe. Es sei G die Tetraedergruppe aus Beispiel II.1.9, ii). Sie hat Ordnung 12. Zu welcher der bisher genannten Gruppen ist sie isomorph?

Das semidirekte Produkt

Wir müssen noch ein Modell für die in Fall 1 a) gefundene Gruppe angeben. Dazu verwenden wir eine allgemeine Konstruktionsmethode für Gruppen.

II.12.8 Definition. Es seien G, H Gruppen und $\varphi\colon H \longrightarrow \mathrm{Aut}(G)$ ein Homomorphismus. Auf der Menge $G \times H$ wird folgende Verknüpfung erklärt:

$$\forall g_1, g_2 \in G,\ h_1, h_2 \in H: \quad (g_1, h_1) \cdot (g_2, h_2) := (g_1 \cdot \varphi(h_1)(g_2), h_1 \cdot h_2).$$

II.12.9 Satz. *Die Menge $G \times H$ zusammen mit der Verknüpfung aus Definition* II.12.8 *ist eine Gruppe.*

Beweis. i) Das **Neutralelement** ist (e, e). Für $g \in G$ und $h \in H$ berechnen wir

$$\begin{array}{rcl} (e, e) \cdot (g, h) & = & (e \cdot \varphi(e)(g), e \cdot h) \overset{\varphi(e)=\mathrm{id}_G}{=} (g, h), \\ (g, h) \cdot (e, e) & = & (g \cdot \varphi(h)(e), h \cdot e) = (g, h). \end{array}$$

Dabei haben wir benutzt, dass $\varphi(h)\colon G \longrightarrow G$ ein Gruppenautomorphismus ist und somit $\varphi(h)(e) = e$ gilt (Lemma II.3.4, i).

[35] In einer abelschen Gruppe ist Konjugation trivial. Zwei Untergruppen sind deswegen genau dann konjugiert, wenn sie gleich sind. Da je zwei 3-Sylow-Untergruppen konjugiert sind, kann es in einer abelschen Gruppe nur eine davon geben.

ii) Für $(g,h) \in G \times H$ ist das **inverse Element**

$$(g,h)^{-1} = \Big((\varphi(h^{-1})(g))^{-1}, h^{-1}\Big).$$

In der Tat haben wir

$$\begin{aligned}(g,h)^{-1} \cdot (g,h) &= \Big((\varphi(h^{-1})(g))^{-1} \cdot (\varphi(h^{-1})(g)), h^{-1} \cdot h\Big) = (e,e),\\ (g,h) \cdot (g,h)^{-1} &= \Big(g \cdot \varphi(h)(\varphi(h^{-1})(g^{-1})), h \cdot h^{-1}\Big)\\ &= (g \cdot \varphi(h \cdot h^{-1})(g^{-1}), e) = (g \cdot g^{-1}, e) = (e,e).\end{aligned}$$

iii) Für das **Assoziativgesetz** berechnen wir

$$\begin{aligned}(g_1,h_1) \cdot ((g_2,h_2) \cdot (g_3,h_3)) &= (g_1,h_1) \cdot (g_2 \cdot \varphi(h_2)(g_3), h_2 \cdot h_3)\\ &= (g_1 \cdot \varphi(h_1)(g_2 \cdot \varphi(h_2)(g_3)), h_1 \cdot (h_2 \cdot h_3))\\ &= (g_1 \cdot \varphi(h_1)(g_2) \cdot \varphi(h_1 \cdot h_2)(g_3), (h_1 \cdot h_2) \cdot h_3)\\ &= (g_1 \cdot \varphi(h_1)(g_2), h_1 \cdot h_2) \cdot (g_3,h_3)\\ &= ((g_1,h_1) \cdot (g_2,h_2)) \cdot (g_3,h_3)\end{aligned}$$

für $g_1, g_2, g_3 \in G$ und $h_1, h_2, h_3 \in H$. □

II.12.10 Definition. Die in Definition II.12.8 und Satz II.12.9 gefundene Gruppe heißt das *semidirekte Produkt* von G und H (bzgl. φ).
Schreibweise. $G \rtimes H$ oder $G \underset{\varphi}{\rtimes} H$.

II.12.11 Bemerkung. Die Untergruppe

$$G \cong \{\,(g,e) \mid g \in G\,\}$$

ist ein Normalteiler von $G \rtimes H$.[36]

II.12.12 Beispiel. Wir arbeiten mit dem Homomorphismus

$$\begin{aligned}\varphi\colon \mathbb{Z}_4 &\longrightarrow \mathrm{Aut}(\mathbb{Z}_3)\\ 1 &\longmapsto (i \longmapsto -i = 2i).\end{aligned}$$

Das Element $g := (1,0)$ hat Ordnung 3, und $h := (0,1)$ Ordnung 4. Weiter gilt

$$h \cdot g \cdot h^{-1} = (0,1) \cdot (1,0) \cdot (0,-1) = (0,1) \cdot (1,-1) = (-1,0) = (2,0) = g^2.$$

Damit ist $\mathbb{H}_{12} := \mathbb{Z}_3 \rtimes \mathbb{Z}_4$ eine Gruppe wie in Fall 1 a) beschrieben. Man nennt $\mathbb{H}_{12}$ eine *dizyklische Gruppe*.

II.12.13 Bemerkung. Die Klassifikationsresultate in diesem Abschnitt beruhen darauf, dass wir geeignete Normalteiler in den betreffenden Gruppen entdeckt haben. Bis auf die zyklischen Gruppen von Primzahlordnung sind wir also noch keinen einfachen Gruppen begegnet. In der Tat umfasst eine einfache, nichtzyklische endliche Gruppe mindestens 60 Elemente. Die alternierende Gruppe A_5 ist einfach (s. [12], Satz 11.44) und bis auf Isomorphie die einzige einfache Gruppe der Ordnung 60, d.h. jede einfache Gruppe der Ordnung 60 ist zu A_5 isomorph.

[36] Das erklärt das Symbol „⋊“.

II.13 Der Hauptsatz über endlich erzeugte abelsche Gruppen

Im Falle abelscher Gruppen haben wir einen wesentlich allgemeineren Klassifikationssatz zur Verfügung, den wir überdies mit relativ einfachen Methoden herleiten können.

II.13.1 Definition. Es sei G eine Gruppe. Sie ist *endlich erzeugt*, wenn es Elemente $x_1, ..., x_s \in G$ gibt, so dass $G = \langle x_1, ..., x_s \rangle$.

Ab jetzt sei G eine endlich erzeugte **abelsche** Gruppe. Weiter seien **erzeugende Elemente** $x_1, ..., x_s \in G$ gegeben, d.h. $G = \langle x_1, ..., x_s \rangle$. Da G abelsch ist, kann jedes Element von G dann in der Form

$$g = x_1^{k_1} \cdot \cdots \cdot x_s^{k_s} \tag{II.24}$$

für geeignete ganze Zahlen $k_1, ..., k_s \in \mathbb{Z}$ geschrieben werden.

II.13.2 Bemerkungen. i) Zum System $x_1, ..., x_s$ von erzeugenden Elementen gehört der surjektive Gruppenhomomorphismus

$$\begin{aligned} \varphi\colon \mathbb{Z}^s := \underbrace{\mathbb{Z} \times \cdots \times \mathbb{Z}}_{s \text{ Faktoren}} &\longrightarrow G \\ (k_1, ..., k_s) &\longmapsto x_1^{k_1} \cdot \cdots \cdot x_s^{k_s}. \end{aligned}$$

ii) Die Darstellung in (II.24) ist im Allgemeinen nicht eindeutig. Die Nichteindeutigkeit entspricht der Tatsache, dass φ nicht injektiv zu sein braucht.

II.13.3 Definition. Ein Ausdruck der Form

$$e = x_1^{k_1} \cdot \cdots \cdot x_s^{k_s}, \quad k_i \in \mathbb{Z},\ i = 1, ..., s,$$

heißt *Relation* zwischen den Erzeugern $x_1, ..., x_s$. Für

$$k_1 = \cdots = k_s = 0$$

sprechen wir von der *trivialen Relation*.

II.13.4 Bemerkung. In Bemerkung II.13.2, i), gilt genau dann

$$e = x_1^{k_1} \cdot \cdots \cdot x_s^{k_s},$$

wenn

$$(k_1, ..., k_s) \in \ker(\varphi).$$

II.13.5 Der Hauptsatz über endlich erzeugte abelsche Gruppen. *Es sei G eine endlich erzeugte abelsche Gruppe. Dann existieren eindeutig bestimmte natürliche Zahlen $r, t \in \mathbb{N}$ und ganze Zahlen $m_1, ..., m_t$, so dass*

$$1 < m_1, \quad m_i | m_{i+1}, \quad i = 1, ..., t-1,$$

und es einen Isomorphismus

$$\varphi\colon \mathbb{Z}^r \times \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_t} \longrightarrow G$$

gibt.

II.13.6 Definitionen. Es sei G eine endlich erzeugte abelsche Gruppe.
i) Die Zahl r heißt der *Rang* von G.
ii) Die Zahlen $m_1, ..., m_t$ sind die *Torsionskoeffizienten* von G.
iii) Falls $t = 0$ gilt, dann nennt man G *freie abelsche Gruppe*.

II.13.7 Folgerungen. i) *Für jede* ***endliche*** *abelsche Gruppe G gibt es eindeutig bestimmte ganze Zahlen $t \geq 0$ und $1 < m_1|m_2|\cdots|m_t$, so dass*

$$G \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_t}.$$

ii) *Es sei G eine endlich erzeugte abelsche Gruppe, so dass e das einzige Element endlicher Ordnung in G ist. Dann ist G eine freie abelsche Gruppe.*

Aus dem Hauptsatz über endlich erzeugte abelsche Gruppen folgt, dass man ein System von Erzeugern $x_1, ..., x_s \in G$ so wählen kann, dass $\mathrm{Ker}(\varphi)$ in Bemerkung II.13.2, i), von Elementen der Form[37] $(0, ..., 0, k_i, 0, ..., 0)$, k_i an der i-ten Stelle, $i = 1, ..., s$, erzeugt wird. Es wird ein wichtiger Schritt im Beweis des Hauptsatzes sein, eine Relation

$$x_1^{k_1} \cdot \cdots \cdot x_s^{k_s} = e$$

in eine Relation der Form

$$z_1^{m_1} = e$$

umzuschreiben.

II.13.8 Beispiele. i) Wir betrachten $G := \mathbb{Z}_6 \times \mathbb{Z}_{10}$. Wir haben $\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$, so dass

$$\mathbb{Z}_6 \times \mathbb{Z}_{10} \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_{10}.$$

Weiter gilt nach Aufgabe II.7.9, dass $\mathbb{Z}_3 \times \mathbb{Z}_{10} \cong \mathbb{Z}_{30}$ und daher

$$\mathbb{Z}_6 \times \mathbb{Z}_{10} \cong \mathbb{Z}_2 \times \mathbb{Z}_{30}.$$

Hier gilt schließlich $2|30$.

ii) Es gibt genau zwei Isomorphieklassen von abelschen Gruppen der Ordnung 12, und zwar

$$\mathbb{Z}_2 \times \mathbb{Z}_6 \quad \text{und} \quad \mathbb{Z}_{12}.$$

iii) Es sei $G \subset \mathbb{C}^\star$ die von -1 und $i/2$ erzeugte Untergruppe. Wir behaupten, dass

$$\begin{array}{rcl} \varphi\colon \mathbb{Z}_2 \times \mathbb{Z} & \longrightarrow & G \\ (k, l) & \longmapsto & (-1)^k \cdot \left(\dfrac{i}{2}\right)^l \end{array}$$

ein Isomorphismus ist. Nach Definition ist φ surjektiv (vgl. Bemerkung II.13.2). Sei $(k, l) \in \ker(\varphi)$. Dann gilt

$$1 = \left|\varphi(k, l)\right| = \frac{1}{2^l}$$

und deshalb $l = 0$. Ferner gilt genau dann $\varphi(k, 0) = 1$, wenn $k = 0$, $k \in \mathbb{Z}_2$.

[37] entsprechend $x_i^{k_i}$

Beweis von Satz II.13.5. *Teil 1: Existenz von r, t und $m_1, ..., m_t$.* Im Beweis benutzen wir die *minimale Länge*

$$s := \min\{\, \sigma \in \mathbb{N} \mid \exists x_1, ..., x_\sigma \in G : \langle\, x_1, ..., x_\sigma \,\rangle = G \,\}$$

eines Erzeugendensystems von G.

Behauptung 1. *Es gibt ganze Zahlen $r, t \geq 0$ und $1 < m_1|m_2|\cdots|m_t$, so dass*

- ⋆ $G \cong \mathbb{Z}^r \times \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_t}$,
- ⋆ $s = r + t$.

Hierbei ist die Konvention $\mathbb{Z}^0 = \{0\}$. Diese Aussage beweisen wir durch Induktion über s. Für $\boldsymbol{s = 0}$ gilt $G = \{0\}$, und die Aussage ist klar.

Im restlichen Beweis $\boldsymbol{s - 1 \longrightarrow s}$ betrachten wir zunächst den Fall, dass es ein Erzeugendensystem $x_1, ..., x_s$ für G gibt, für das nur die triviale Relation besteht. Dann ist

$$\begin{array}{rcl} \varphi\colon \mathbb{Z}^s & \longrightarrow & G \\ (k_1, ..., k_s) & \longmapsto & x_1^{k_1} \cdot \cdots \cdot x_s^{k_s} \end{array}$$

ein Isomorphismus, und es ist nichts zu zeigen.

In den verbleibenden Fällen gibt es für jedes Erzeugendensystem minimaler Länge eine nichttriviale Relation. Wir setzen dann[38]

$$m_1 := \min\{\, m \geq 1 \mid \exists x_1, ..., x_s \in G,\ l_2, ..., l_s \in \mathbb{Z} : \langle\, x_1, ..., x_s \,\rangle = G,\ x_1^m \cdot x_2^{l_2} \cdot \cdots \cdot x_s^{l_s} = e \,\}.$$

Es seien $x_1, ..., x_s \in G$ Erzeuger und $l_2, ..., l_s$ ganze Zahlen, so dass die Relation

$$x_1^{m_1} \cdot x_2^{l_2} \cdot \cdots \cdot x_s^{l_s} = e \tag{II.25}$$

besteht.

Behauptung 2. *Es gilt $m_1|l_2$.*

Zum Beweis führen wir die Division mit Rest $l_2 = q \cdot m_1 + u$ mit $q \in \mathbb{Z}$ und $0 \leq u < m_1$ durch. Dann finden wir

$$e = x_1^{m_1} \cdot x_2^{q \cdot m_1 + u} \cdot x_3^{l_3} \cdot \cdots \cdot x_s^{l_s} = (x_1 \cdot x_2^q)^{m_1} \cdot x_2^u \cdot x_3^{l_3} \cdot \cdots \cdot x_s^{l_s}.$$

Es gilt

$$G = \langle\, x_1, ..., x_s \,\rangle = \langle\, x_1 \cdot x_2^q, x_2, ..., x_s \,\rangle.$$

Die Inklusion „$\supset$“ ist dabei klar. Für „$\subset$“ beachte man $x_1 = (x_1 \cdot x_2^q) \cdot x_2^{-q}$. Aus der Definition von m_1 folgt $u = 0$. √

Da wir $x_2, ..., x_s$ beliebig nummerieren können, folgt aus Behauptung 2, dass $m_1|l_i$, $i = 2, ..., s$. Seien $q_2, ..., q_s \in \mathbb{Z}$, so dass $l_i = m_1 \cdot q_i$, $i = 2, ..., s$. Mit $z_1 := x_1 \cdot x_2^{q_2} \cdot \cdots \cdot x_s^{q_s}$ gilt

$$G = \langle\, x_1, x_2, ..., x_s \,\rangle = \langle\, z_1, x_2, ..., x_s \,\rangle,$$

[38] Die betrachtete Menge ist nicht leer: Nach Voraussetzung gibt es $x_1, ..., x_s \in G$ sowie $m, m_2, ..., m_s \in \mathbb{Z}$ mit $m \neq 0$ und $e = x_1^m \cdot x_2^{m_2} \cdot \cdots \cdot x_s^{m_s}$. Dann haben wir auch $e = x_1^{-m} \cdot x_2^{-m_2} \cdot \cdots \cdot x_s^{-m_s}$.

und Relation (II.25) wird zu

$$z_1^{m_1} = e. \tag{II.26}$$

Nun seien

$$H := \langle z_1 \rangle \cong \mathbb{Z}_{m_1} \quad \text{und} \quad G_1 := \langle\, x_2, ..., x_s \,\rangle.$$

Dann gilt

- ⋆ $H \cdot G_1 = G$,
- ⋆ $H \cap G_1 = \{e\}$[39]
- ⋆ und deswegen $G \cong H \times G_1$.

Die minimale Länge eines Erzeugendensystems für G_1 ist offenbar $s - 1$. Nach Induktionsvoraussetzung existieren $r, t \geq 0$ und ganze Zahlen $0 < m_2|m_3| \cdots |m_t$ mit

- ⋆ $G_1 \cong \mathbb{Z}^r \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_t}$,
- ⋆ $s - 1 = r + t - 1$.

Es ist noch zu begründen, dass

$$m_1|m_2.$$

In der Tat finden wir ein Erzeugendensystem $\langle\, z_2, ..., z_s \,\rangle$ für G_1 mit $z_2^{m_2} = e$. Dann ist $\langle\, z_1, z_2, ..., z_s \,\rangle$ ein Erzeugendensystem mit der minimal möglichen Anzahl von Elementen, und es gilt die Relation

$$z_1^{m_1} \cdot z_2^{m_2} \cdot z_3^0 \cdot \cdots \cdot z_s^0 = e.$$

Wir schließen mit Behauptung 2. □

II.13.9 Bemerkungen. i) Das Buch [2] erlaubt sich im obigen Beweis eine kleine Ungenauigkeit, weil die Forderung $s = r + t$ nicht in der Formulierung der Aussage enthalten ist. Wenn wir aber nicht wissen, dass ein Erzeugendensystem mit den im Satz genannten Eigenschaften von minimaler Länge unter allen Erzeugendensystemen gewählt werden kann, dann lässt sich auch der Induktionsschluss nicht sauber durchführen. (In Beispiel II.13.8, i), haben wir ja erkannt, dass es Erzeugendensysteme unterschiedlicher Länge gibt, die **unverkürzbar** sind, d.h. aus denen man keinen Erzeuger entfernen kann.)

ii) Aus der Eindeutigkeitssaussage im Hauptsatz II.13.5 und Behauptung 1 im Existenzbeweis folgt, dass jedes Erzeugendensystem, das die im Hauptsatz genannten Eigenschaften aufweist, von minimaler Länge ist.

Für den Beweis der Eindeutigkeitsaussage im Hauptsatz benötigen wir weitere Vorbereitungen.

II.13.10 Hilfssatz. *Es sei G eine abelsche Gruppe.*

i) *Für jedes $k \geq 1$ ist*

$$\mathrm{Tors}_k(G) := \{\, x \in G \mid x^k = e \,\}$$

eine Untergruppe.

[39] Denn zu $\alpha_1 \in \{\, 1, ..., m_1 - 1 \,\}$ und $\alpha_2, ..., \alpha_s \in \mathbb{Z}$ mit $z_1^{\alpha_1} = x_2^{\alpha_2} \cdot \cdots \cdot x_s^{\alpha_s}$ gehört die Relation $z_1^{\alpha_1} \cdot x_2^{-\alpha_2} \cdot \cdots \cdot x_s^{-\alpha_s} = e$.

ii) *Die Menge*

$$\mathrm{Tors}(G) := \{\, x \in G \mid \exists k \geq 1 : x^k = e \,\} = \bigcup_{k\geq 1} \mathrm{Tors}_k(G)$$

ist eine Untergruppe von G.

iii) *Wenn G endlich erzeugt ist, dann ist* Tors(G) *eine endliche Gruppe.*

Beweis. i) Es gilt $e \in \mathrm{Tors}_k(G)$, und für $x \in \mathrm{Tors}_k(G)$ hat man

$$(x^{-1})^k = (x^k)^{-1} = e^{-1} = e, \tag{II.27}$$

so dass $x^{-1} \in \mathrm{Tors}_k(G)$. Schließlich seien $x, y \in \mathrm{Tors}_k(G)$. Dann berechnen wir

$$(x \cdot y)^k = x^k \cdot y^k = e \cdot e = e.$$

Deshalb gilt $x \cdot y \in \mathrm{Tors}_k(G)$.

ii) Auch hier folgt sofort $e \in \mathrm{Tors}(G)$. Für $x \in \mathrm{Tors}(G)$ und $k \geq 1$ mit $x^k = e$ gilt wegen (II.27) $(x^{-1})^k = e$ und damit $x^{-1} \in \mathrm{Tors}(G)$. Für $x, y \in \mathrm{Tors}(G)$ und $k, l \geq 1$ mit $x^k = e = y^l$ erhalten wir

$$(x \cdot y)^{k\cdot l} = (x^k)^l \cdot (y^l)^k = e^l \cdot e^k = e.$$

Es folgt $x \cdot y \in \mathrm{Tors}(G)$.

iii) Nach dem bereits bewiesenen Existenzteil des Hauptsatzes II.13.5 finden wir $r, t \geq 0$ und ganze Zahlen $m_1, ..., m_t$ mit

$$G \cong H := \mathbb{Z}^r \times \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_t}.$$

Wir schließen

$$\mathrm{Tors}(G) \cong \mathrm{Tors}(H) = \{0\} \times \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_t},$$

und das ist eine endliche Gruppe. □

II.13.11 Hilfssatz. i) *Es seien $m, k \geq 1$ natürliche Zahlen. Dann gilt*

$$\vartheta := \#\{\, 0 \leq r < m \mid m|(k \cdot r) \,\} = \mathrm{ggT}(k, m).$$

ii) *Für natürliche Zahlen $k, m_1, ..., m_t \geq 1$ gilt*

$$\#\mathrm{Tors}_k(\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_t}) = \mathrm{ggT}(k, m_1) \cdot \cdots \cdot \mathrm{ggT}(k, m_t).$$

Beweis. i) Es seien $\gamma := \mathrm{ggT}(k, m)$ und $k', m' \in \mathbb{N}$ natürliche Zahlen mit $k = k' \cdot \gamma$ und $m = m' \cdot \gamma$. Dabei gilt $\mathrm{ggT}(k', m') = 1$. Nun sei $r \in \{\, 0, ..., m-1 \,\}$ eine Zahl mit

$$(m' \cdot \gamma)|(k' \cdot \gamma \cdot r).$$

Es folgt $m'|r$, d.h.

$$r \in M := \{\, 0, m', ..., (\gamma - 1) \cdot m' \,\}.$$

Offenbar gilt

$$\#M = \gamma = \mathrm{ggT}(k, m).$$

Es ist noch zu zeigen, dass $m|(k \cdot r)$ für $r \in M$. Für $r \in M$ existiert ein $\lambda \in \{0, ..., \gamma - 1\}$ mit $r = \lambda \cdot m'$. Wir finden

$$k \cdot r = (k' \cdot \gamma) \cdot (\lambda \cdot m') = \lambda \cdot k' \cdot m' \cdot \gamma = \lambda \cdot k' \cdot m,$$

so dass $m|(k \cdot r)$.

ii) Für abelsche Gruppen $G_1, ..., G_t$ und $k \geq 1$ haben wir offensichtlich

$$\mathrm{Tors}_k(G_1 \times \cdots \times G_t) \cong \mathrm{Tors}_k(G_1) \times \cdots \times \mathrm{Tors}_k(G_t).$$

Deswegen darf $t = 1$ angenommen werden. Der Fall $t = 1$ ist aber Gegenstand von Teil i) des Hilfssatzes. □

Der folgende Hilfssatz enthält das Eindeutigkeitsresultat für die Torsionsuntergruppe einer endlich erzeugten abelschen Gruppe.

II.13.12 Hilfssatz. *Gegeben seien natürliche Zahlen $s, t \geq 1$ und $m_1, ..., m_s$ sowie $n_1, ..., n_t$ mit*

$$1 < m_1|m_2| \cdots |m_s \quad \textit{und} \quad 1 < n_1|n_2| \cdots |n_t.$$

Gilt

$$\forall k \geq 1 : \mathrm{ggT}(k, m_1) \cdot \cdots \cdot \mathrm{ggT}(k, m_s) = \mathrm{ggT}(k, n_1) \cdot \cdots \cdot \mathrm{ggT}(k, n_t),$$

dann folgt

$$s = t \quad \textit{und} \quad m_i = n_i, \quad i = 1, ..., s.$$

Beweis. Ohne Beschränkung der Allgemeinheit setzen wir $s \geq t$ voraus und weisen die Aussage durch vollständige Induktion über s nach.

$\boldsymbol{s = 1}$. Hier folgt $t = 1$. Aus $m_1 = \mathrm{ggT}(m_1, m_1) = \mathrm{ggT}(m_1, n_1)$ folgt $m_1|n_1$. Ebenso ergibt sich $n_1|m_1$ und somit $m_1 = n_1$.

$\boldsymbol{s - 1 \longrightarrow s}$. Wir haben

$$m_1^s = \mathrm{ggT}(m_1, m_1) \cdot \cdots \cdot \mathrm{ggT}(m_1, m_s) = \mathrm{ggT}(m_1, n_1) \cdot \cdots \cdot \mathrm{ggT}(m_1, n_t).$$

Jeder Faktor auf der rechten Seite liegt in $\{1, ..., m_1\}$. Wegen $t \leq s$ kann die obige Gleichung nur mit $s = t$ und $\mathrm{ggT}(m_1, n_i) = m_1$, $i = 1, ..., s$, erfüllt werden. Insbesondere haben wir $m_1|n_1$. Aus Symmetriegründen gilt auch $n_1|m_1$ und deswegen $m_1 = n_1$.

Für $k \geq 1$ haben wir somit

$$\mathrm{ggT}(k, m_1) \cdot \mathrm{ggT}(k, m_2) \cdot \cdots \cdot \mathrm{ggT}(k, m_s) = \mathrm{ggT}(k, m_1) \cdot \mathrm{ggT}(k, n_2) \cdot \cdots \cdot \mathrm{ggT}(k, n_t).$$

Da $\mathrm{ggT}(k, m_1) \neq 0$, folgt aus dieser Gleichung

$$\mathrm{ggT}(k, m_2) \cdot \cdots \cdot \mathrm{ggT}(k, m_s) = \mathrm{ggT}(k, n_2) \cdot \cdots \cdot \mathrm{ggT}(k, n_t),$$

so dass wir mit der Induktionsvoraussetzung schließen können. □

Der nächste Hilfssatz liefert die Eindeutigkeit des freien Anteils einer endlich erzeugten abelschen Gruppe.

II.13.13 Hilfssatz. *Es sei $\varphi\colon \mathbb{Z}^s \longrightarrow \mathbb{Z}^t$ eine Surjektion. Dann gilt $s \geq t$. Insbesondere sind für $s, t \in \mathbb{N}$ die abelschen Gruppen $\mathbb{Z}^s$ und $\mathbb{Z}^t$ genau dann isomorph, wenn $s = t$.*

Beweis. Wir betrachten $\mathbb{Z}^t$ als Unterring von $\mathbb{R}^t$. Es seien $e_i := (0, ..., 0, 1, 0, ..., 0) \in \mathbb{Z}^s$ der i-te Standarderzeuger mit der 1 als i-tem Eintrag und $v_i := \varphi(e_i) \in \mathbb{R}^t$, $i = 1, ..., s$. Es gilt[40]

$$\mathbb{R}^t = \langle \mathbb{Z}^t \rangle_{\mathbb{R}} \subset \langle\, v_1, ..., v_s \,\rangle_{\mathbb{R}} \subset \mathbb{R}^t.$$

Es muss in jedem Schritt Gleichheit gelten, so dass $\langle\, v_1, ..., v_s \,\rangle_{\mathbb{R}} = \mathbb{R}^t$. Aus der linearen Algebra ([20], §10; [5], Abschnitt 1.5) weiß man, dass $s \geq t$ gelten muss. □

Beweis von Satz II.13.5. *Teil 2: Eindeutigkeit von r, t und m_1, ..., m_t.* Es seien r, r', t, t', $m_1, ..., m_t$ und $m'_1, ..., m'_{t'}$ natürliche Zahlen mit

$$1 < m_1 | m_2 | \cdots | m_t \quad \text{und} \quad 1 < m'_1 | m'_2 | \cdots | m'_{t'},$$

so dass die Gruppen

$$G := \mathbb{Z}^r \times \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_t}$$

und

$$G' := \mathbb{Z}^{r'} \times \mathbb{Z}_{m'_1} \times \cdots \times \mathbb{Z}_{m'_{t'}}$$

zueinander isomorph sind. Wir fixieren einen Isomorphismus $\varphi\colon G \longrightarrow G'$. Dann gilt

$$\forall k \geq 1 : \quad \varphi(\mathrm{Tors}_k(G)) = \mathrm{Tors}_k(G'),$$

so dass insbesondere

$$\forall k \geq 1 : \quad \#\mathrm{Tors}_k(G) = \#\mathrm{Tors}_k(G').$$

Mit

$$\begin{aligned} \mathrm{Tors}_k(G) &\cong \mathrm{Tors}_k(\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_t}), \\ \mathrm{Tors}_k(G') &\cong \mathrm{Tors}_k(\mathbb{Z}_{m'_1} \times \cdots \times \mathbb{Z}_{m'_{t'}}) \end{aligned}$$

folgt aus Hilfssatz II.13.11 und II.13.12, dass $t = t'$ und $m_i = m'_i$, $i = 1, ..., t$.

Es gilt ebenso

$$\varphi(\mathrm{Tors}(G)) = \mathrm{Tors}(G'),$$

so dass für den Homomorphismus

$$\begin{array}{rccccc} \overline{\varphi}\colon G & \xrightarrow{\varphi} & G' & \longrightarrow & G'/\mathrm{Tors}(G') \cong \mathbb{Z}^{r'} \\ & & g & \longmapsto & [g] \end{array}$$

die Gleichung

$$\mathrm{Ker}(\overline{\varphi}) = \mathrm{Tors}(G)$$

folgt. Aus dem ersten Isomorphiesatz II.10.1 schließen wir, dass ein Isomorphismus

$$\widetilde{\varphi}\colon \mathbb{Z}^r \cong G/\mathrm{Tors}(G) \longrightarrow G'/\mathrm{Tors}(G') \cong \mathbb{Z}^{r'}$$

induziert wird. Hilfssatz II.13.13 zeigt $r = r'$. □

II.13.14 Aufgabe (Endliche abelsche Gruppen). Listen Sie alle Isomorphieklassen von endlichen abelschen Gruppen der Ordnung 36 auf.

[40] Mit $\langle\cdot\rangle_{\mathbb{R}}$ bezeichnen wir die lineare Hülle ([20], §9, Definition 2; [5], Abschnitt 1.4.4).

II.13.15 Aufgabe (Freie abelsche Gruppen). Beweisen Sie für $n \in \mathbb{N}$, dass es für jede Untergruppe $G \subset \mathbb{Z}^n$ eine Zahl $l \in \{0, ..., n\}$ mit $G \cong \mathbb{Z}^l$ gibt. Ist jeder Wert von l möglich?

II.13.16 Aufgabe (Die abelsche Gruppe $\mathbb{Q}/\mathbb{Z}$). a) Beweisen Sie

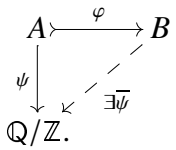
$$\mathrm{Tors}(\mathbb{R}/\mathbb{Z}) = \mathbb{Q}/\mathbb{Z}.$$

b) Bestimmen Sie für $k \geq 1$ die Untergruppe

$$\mathrm{Tors}_k(\mathbb{Q}/\mathbb{Z}).$$

c) Ist $\mathbb{Q}/\mathbb{Z}$ endlich erzeugt?

d) Beweisen Sie, dass die Gruppe $\mathbb{Q}/\mathbb{Z}$ folgende Eigenschaft aufweist: Für je zwei abelsche Gruppen A, B, jeden **injektiven** Homomorphismus $\varphi\colon A \longrightarrow B$ und jeden Homomorphismus $\psi\colon A \longrightarrow \mathbb{Q}/\mathbb{Z}$ existiert ein Homomorphismus $\overline{\psi}\colon B \longrightarrow \mathbb{Q}/\mathbb{Z}$ mit $\psi = \overline{\psi} \circ \varphi$. Wir merken uns diese Eigenschaft mit dem kommutativen Diagramm



Jeder Homomorphismus von A nach $\mathbb{Q}/\mathbb{Z}$ kann also auf B erweitert werden. (Diese Eigenschaft heißt *Injektivität*.)

Hinweis. Betrachten Sie Paare (C, ξ), die aus einer Untergruppe C von B, die $\varphi(A)$ enthält, und einem Homomorphismus $\xi\colon C \longrightarrow \mathbb{Q}/\mathbb{Z}$ mit $\psi = \xi \circ \varphi$ bestehen.

e) Folgern Sie, dass eine abelsche Gruppe A genau dann trivial ist, d.h. isomorph zu $\{0\}$, wenn der einzige Homomorphismus von A nach $\mathbb{Q}/\mathbb{Z}$ der Nullhomomorphismus $a \longmapsto 0$, $a \in A$, ist.

III

Das quadratische Reziprozitätsgesetz

Dieses Kapitel widmet sich der Untersuchung quadratischer Kongruenzen modulo einer Primzahl p. Dabei erkennt man schnell, dass es nur auf Kongruenzen der Form $x^2 \equiv a \bmod p$ ankommt, $a \in \mathbb{Z}$. Die Lösbarkeit lässt sich selbstverständlich „von Hand“ bestimmen, indem man die Zahlen $0, ..., p-1$ quadriert und die erhaltenen Quadrate modulo p reduziert. Viel interessanter ist jedoch, die Lösbarkeit der obigen Kongruenz in Abhängigkeit von a und p zu studieren. Ein erster wichtiger Satz dazu stammt von Euler und führt die Frage nach der Lösbarkeit der Kongruenz $x^2 \equiv a \bmod p$ auf die Berechnung der Potenz $a^{(p-1)/2}$ modulo p zurück. Mit Eulers Satz kann man sofort den Fall $a = -1$ behandeln. Interessanterweise lässt sich Eulers Satz im Rahmen der Gruppentheorie verstehen. Dazu schaut man die Einheitengruppe des Körpers $\mathbb{Z}_p$ an und wendet auf sie den Satz von Lagrange und den Hauptsatz über endlich erzeugte abelsche Gruppen an. Weiter zeigen elementare Betrachtungen, dass man nur Kongruenzen der Form $x^2 \equiv q \bmod p$, q eine Primzahl, verstehen muss. Eine überraschende Gesetzmäßigkeit, **quadratisches Reziprozitätsgesetz** genannt, besagt nun, dass für zwei gegebene Primzahlen $p \neq q$ die Frage nach der Lösbarkeit der Kongruenz $x^2 \equiv q \bmod p$ äquivalent zu der Frage nach der Lösbarkeit der Kongruenz $x^2 \equiv p \bmod q$ ist. Dabei ist in manchen Fällen die eine Kongruenz genau dann lösbar, wenn die andere es ist, und in anderen ist die eine genau dann lösbar, wenn die andere es nicht ist. Das quadratische Reziprozitätsgesetz geht auf Euler[1] und Legendre[2] zurück und wurde von Gauß bewiesen. Die Leserin bzw. der Leser wird an dieser Stelle ermutigt, einmal einen Blick in Gauß' berühmte „Disquisitiones Arithmeticae“ zu werfen, die auch in deutscher Übersetzung als „Arithmetische Untersuchungen“ [7] vorliegen. Das quadratische Reziprozitätsgesetz besticht durch die Eleganz seiner Aussage. Zudem ist es zusammen mit der Primfaktorzerlegung ein Werkzeug, die Lösbarkeit quadratischer Kongruenzen zu entscheiden.[3] Das vorliegende Kapitel basiert auf Kapitel 8 des Buchs [14] und Abschnitt 16 des Skripts [6].

[1] Leonhard Euler (1707 - 1783), schweizer Mathematiker und Physiker.

[2] Adrien-Marie Legendre (1752 - 1833), französischer Mathematiker.

[3] Allerdings ist die Primfaktorzerlegung auch der Schwachpunkt des Verfahrens, da sie sehr aufwändig ist.

III.1 Ringe und Körper

III.1.1 Definitionen. i) Ein Tupel $(R, 0, 1, +, \cdot)$, das aus einer Menge R, Elementen $0, 1 \in R$ und Abbildungen

$$+ \colon R \times R \longrightarrow R$$

und

$$\cdot \colon R \times R \longrightarrow R$$

besteht, ist ein *kommutativer Ring mit* 1, wenn gilt:

- ⋆ $(R, +)$ ist eine **abelsche** Gruppe mit Neutralelement 0.
- ⋆ 1 ist ein Neutralelement für die Multiplikation, d.h.

$$\forall r \in R : \quad r \cdot 1 = r = 1 \cdot r.$$

- ⋆ Die Multiplikation ist assoziativ, d.h.

$$\forall r, s, t \in R : \quad r \cdot (s \cdot t) = (r \cdot s) \cdot t.$$

- ⋆ Die Multiplikation ist kommutativ, d.h.

$$\forall r, s \in R : \quad r \cdot s = s \cdot r.$$

- ⋆ Addition und Multiplikation genügen dem *Distributivgesetz*, d.h.

$$\forall r, s, t \in R : \quad r \cdot (s + t) = r \cdot s + r \cdot t.$$

ii) Ein *Körper* ist ein Ring $(K, 0, 1, +, \cdot)$, in dem gilt:

- ⋆ $0 \neq 1$.
- ⋆ $\forall r \in K \setminus \{0\} \exists s \in K \setminus \{0\} : \quad r \cdot s = 1 = s \cdot r.$

iii) Es sei $(R, 0, 1, +, \cdot)$ ein Ring. Die Menge

$$R^\star := \{ r \in R \mid \exists s \in R : r \cdot s = 1 = s \cdot r \}$$

heißt *Einheitengruppe* von R.

iv) Es seien $(R, 0_R, 1_R, +_R, \cdot_R)$ und $(S, 0_S, 1_S, +_S, \cdot_S)$ Ringe. Eine Abbildung $\varphi \colon R \longrightarrow S$ ist ein *(Ring-)Homomorphismus*, wenn folgende Eigenschaften erfüllt sind:

- ⋆ $\varphi \colon (R, +_R) \longrightarrow (S, +_S)$ ist ein Gruppenhomomorphismus, i.e.

$$\forall r, s \in R : \quad \varphi(r + s) = \varphi(r) + \varphi(s).$$

- ⋆ $\varphi(1_R) = 1_S$.
- ⋆ $\forall r, s \in R : \varphi(r \cdot_R s) = \varphi(r) \cdot_S \varphi(s)$.

Wie üblich werden wir einen Ring $(R, 0, 1, +, \cdot)$ in der Form R notieren. Mit dem Begriff des Ringhomomorphismus definieren wir wie in Definition II.3.3, ii), den Begriff des Ringisomorphismus. Für zwei Ringe R und S schreiben wir $R \cong S$, wenn sie isomorph sind, d.h., wenn es einen Ringisomorphismus $\varphi\colon R \longrightarrow S$ gibt.

III.1.2 Bemerkungen. i) In einem Ring R gilt $0 \cdot r = 0 = r \cdot 0$ für jedes Element $r \in R$. Dazu beachte man $0 \cdot r = (0 + 0) \cdot r = 0 \cdot r + 0 \cdot r$. Wir addieren $-(0 \cdot r)$ auf beiden Seiten und finden damit $0 = 0 \cdot r$. Auf Grund des Kommutativgesetzes haben wir $r \cdot 0 = 0 \cdot r = 0$.

ii) Die Bedingung $\varphi(1_R) = 1_S$ folgt **nicht** aus den anderen Axiomen (s. Beispiel III.1.3, vi).

iii) Es seien $r, s \in R^\star$. Dann gilt auch $r \cdot s \in R^\star$. Dazu wähle man $r', s' \in R$ mit $r \cdot r' = 1 = s \cdot s'$. Wir haben dann $(r \cdot s) \cdot (r' \cdot s') = (r \cdot r') \cdot (s \cdot s') = 1 \cdot 1 = 1$. Damit ist die Multiplikation $\cdot\colon R^\star \times R^\star \longrightarrow R^\star$, $(r, s) \longmapsto r \cdot s$, definiert. Das Assoziativgesetz gilt, weil es in R gilt. Das Element 1 liegt in $R^\star$ und ist offenbar das neutrale Element. Nach Definition von $R^\star$ besitzt jedes Element von $R^\star$ ein inverses. Somit ist $R^\star$ in der Tat eine Gruppe. In einem Körper K ist dies die Gruppe $(K^\star = K \setminus \{0\}, \cdot)$.

III.1.3 Beispiele. i) Die Mengen $\mathbb{Q}$, $\mathbb{R}$ und $\mathbb{C}$ zusammen mit den bekannten Additionen und Multiplikationen bilden Körper und damit auch Ringe.

ii) Die Menge $\mathbb{Z}$ mit der üblichen Addition und Multiplikation ist ein Ring, jedoch kein Körper (vgl. Beispiel auf Seite 25).

iii) Die Menge $R = \{0\}$ mit der einzig möglichen Addition und Multiplikation ist ein Ring, in dem $0 = 1$ gilt. Bis auf Isomorphie ist er der einzige Ring mit dieser Eigenschaft. Denn in einem Ring S mit $0 = 1$ finden wir mit Definition III.1.1, i), und Bemerkung III.1.2, i), dass

$$\forall r \in R: \quad r = 1 \cdot r = 0 \cdot r = 0.$$

iv) Es seien R und S Ringe. Dann ist $T := R \times S$ mit

- $0_T = (0_R, 0_S)$,
- $1_T = (1_R, 1_S)$,
- $$\begin{array}{rcl} +_T\colon T \times T & \longrightarrow & T \\ ((r_1, s_1), (r_2, s_2)) & \longmapsto & (r_1 +_R r_2, s_1 +_S s_2), \end{array}$$
- $$\begin{array}{rcl} \cdot_T\colon T \times T & \longrightarrow & T \\ ((r_1, s_1), (r_2, s_2)) & \longmapsto & (r_1 \cdot_R r_2, s_1 \cdot_S s_2), \end{array}$$

ein Ring. Wir halten fest:

- Für jeden Ring R ist $\varphi\colon R \longrightarrow R \times \{0\}$, $r \longmapsto (r, 0)$, ein Isomorphismus.
- Es gilt $(0_R, 1_S) \cdot (1_R, 0_S) = (0_R, 0_S) = 0_T$. Deshalb ist T kein Körper, es sei denn $R = \{0\}$ und S ist ein Körper oder R ist ein Körper und $S = \{0\}$.

v) Die Inklusionen $\mathbb{Z} \subset \mathbb{Q}$, $\mathbb{Q} \subset \mathbb{R}$ und $\mathbb{R} \subset \mathbb{C}$ sind Ringhomomorphismen.

vi) Für die Abbildung

$$\begin{array}{rcl} \varphi\colon \mathbb{Z} & \longrightarrow & \mathbb{Z} \times \mathbb{Z} \\ k & \longmapsto & (k, 0) \end{array}$$

haben wir

$$\varphi(1) = (1,0) \neq (1,1) = 1_{\mathbb{Z}\times\mathbb{Z}}.$$

Alle anderen in Definition III.1.1, iv), genannten Eigenschaften sind allerdings erfüllt.

vii) Es sei $n \geq 1$. Wir betrachten die Menge $\mathbb{Z}_n = \{0, 1, ..., n-1\}$. Für $k \in \mathbb{Z}$ sei $[k]_n \in \mathbb{Z}_n$ die eindeutig bestimmte Zahl mit

$$k \equiv [k]_n \bmod n$$

(vgl. Aufgabe I.6.2, a). Wir haben gesehen, dass $\mathbb{Z}_n$ zusammen mit der Addition

$$\begin{array}{rcl} +\colon \mathbb{Z}_n \times \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \\ (i,j) & \longmapsto & [i+j]_n \end{array}$$

eine abelsche Gruppe mit neutralem Element 0 bildet. Jetzt definieren wir

$$\begin{array}{rcl} \cdot\colon \mathbb{Z}_n \times \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \\ (i,j) & \longmapsto & [i\cdot j]_n \end{array}$$

und behaupten, dass $(\mathbb{Z}_n, 0, 1, +, \cdot)$ ein Ring ist. Zu diesem Zweck betrachten wir die Abbildung

$$\begin{array}{rcl} \varphi\colon \mathbb{Z} & \longrightarrow & \mathbb{Z}_n \\ k & \longmapsto & [k]_n. \end{array}$$

Diese Abbildung hat folgende Eigenschaften:

- ⋆ φ ist surjektiv.
- ⋆ $\varphi\colon (\mathbb{Z}, +) \longrightarrow (\mathbb{Z}_n, +)$ ist ein Homomorphismus abelscher Gruppen.
- ⋆ $\varphi(1) = 1$.
- ⋆ $\varphi(i\cdot j) = \varphi(i)\cdot\varphi(j)$, $i, j \in \mathbb{Z}$. Diese Gleichung ist äquivalent zu

$$\forall i, j \in \mathbb{Z}: \quad [i\cdot j]_n = \big[[i]_n \cdot [j]_n\big]_n$$

und folgt aus Beobachtung I.6.5.

Die letztgenannte Eigenschaft und die Surjektivität von φ implizieren, dass $\cdot\colon \mathbb{Z}_n\times\mathbb{Z}_n \longrightarrow \mathbb{Z}_n$ assoziativ ist und in $\mathbb{Z}_n$ das Distributivgesetz gilt. Folglich sind $\mathbb{Z}_n$ ein Ring und φ ein surjektiver Ringhomomorphismus.

III.1.4 Chinesischer Restsatz. *Es seien $m, n \in \mathbb{N}_{>0}$ positive natürliche Zahlen mit* ggT$(m, n) = 1$. *Dann ist*

$$\begin{array}{rcl} \psi\colon \mathbb{Z}_{m\cdot n} & \longrightarrow & \mathbb{Z}_m \times \mathbb{Z}_n \\ i & \longmapsto & ([i]_m, [j]_n) \end{array}$$

ein Ringisomorphismus.

Beweis. Wie in Beispiel III.1.3, vii), sieht man ein, dass ψ ein Homomorphismus ist. Es bleibt nachzuweisen, dass ψ bijektiv ist. Zu $i \in \mathbb{Z}_m$ und $j \in \mathbb{Z}_n$ soll es genau ein Element $k \in \mathbb{Z}_{m\cdot n}$ mit

$$[k]_m = i \quad \text{und} \quad [k]_n = j,$$

d.h.

$$k \equiv i \bmod m \quad \text{und} \quad k \equiv j \bmod n$$

geben. Das folgt aber aus dem chinesischen Restsatz in der Formulierung I.6.14. □

III.2 Die eulersche φ-Funktion

III.2.1 Definitionen. i) Für $n \geq 1$ sei $U_n := \mathbb{Z}_n^\star$ die Einheitengruppe im Ring $\mathbb{Z}_n$.

ii) Sei $\mathbb{N}_+ := \mathbb{N} \setminus \{0\}$. Die Abbildung

$$\begin{array}{rcl} \varphi\colon \mathbb{N}_+ & \longrightarrow & \mathbb{N}_+ \\ n & \longmapsto & \#U_n \end{array}$$

heißt *eulersche φ-Funktion*.

III.2.2 Bemerkung. Für $n = 1$ gilt $\mathbb{Z}_1 = \{0\}$ und $\mathbb{Z}_1^\star = \{0\}$.

III.2.3 Eigenschaften. i) *Es gilt*

$$U_n = \{\, k \in \mathbb{Z}_n \mid \mathrm{ggT}(k, n) = 1 \,\}.$$

ii) *Es seien $m, n \in \mathbb{N}_+$ positive natürliche Zahlen mit* $\mathrm{ggT}(m, n) = 1$. *Dann gilt*

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n).$$

iii) *Für eine Primzahl p und eine positive natürliche Zahl $r \in \mathbb{N}_+$ gilt*

$$\varphi(p^r) = p^{r-1} \cdot (p - 1).$$

Insbesondere hat man

$$\varphi(p) = p - 1.$$

Beweis. i) Sei $k \in U_n$. Dann existiert ein $l \in U_n$ mit $k \cdot l = 1$ in $\mathbb{Z}_n$, d.h. $k \cdot l \equiv 1 \bmod n$. Deswegen existiert ein $m \in \mathbb{Z}$ mit

$$k \cdot l + m \cdot n = 1.$$

Dies zeigt $\mathrm{ggT}(k, n) = 1$. Diese Argumentation lässt sich umkehren.

ii) Nach dem chinesischen Restsatz gilt $\mathbb{Z}_{m\cdot n} \cong \mathbb{Z}_m \times \mathbb{Z}_n$. Mit Definition III.1.1, iii), und Beispiel III.1.3, iv), überprüft man

$$U_{m\cdot n} \cong U_m \times U_n.$$

iii) Aus Teil i) folgt

$$U_{p^r} = \{\, k \in \{\, 0, ..., p^r - 1 \,\} \mid p \nmid k \,\}.$$

Auf der anderen Seite finden wir

$$A_n := \mathbb{Z}_{p^r} \setminus U_{p^r} = \{\, k \in \{\, 0, ..., p^r - 1 \,\} \mid p|k \,\} = \{\, 0, p, 2 \cdot p, ..., (p^{r-1} - 1) \cdot p \,\}.$$

Damit berechnen wir

$$\#U_{p^r} = p^r - \#A_n = p^r - p^{r-1} = p^{r-1} \cdot (p - 1)$$

und zeigen die Behauptung. □

Aus diesen Eigenschaften folgern wir eine allgemeine Formel für die eulersche φ-Funktion:

III.2.4 Satz. *Es seien $n \geq 2$ eine natürliche Zahl und*

$$n = p_1^{r_1} \cdot \cdots \cdot p_s^{r_s}$$

ihre Primfaktorzerlegung. Dann gilt

$$\varphi(n) = \prod_{i=1}^{s} p_i^{r_i - 1} \cdot (p_i - 1).$$

Beweis. Man muss lediglich Eigenschaft III.2.3, ii) und iii), anwenden. □

III.2.5 Beispiel (Eine arithmetische Progression). Wir wollen zeigen, dass in der arithmetischen Progression[4] $(8k + 1)_{k \in \mathbb{N}}$ unendlich viele Primzahlen vorkommen.

Dazu geben wir uns eine Schranke $M \geq 1$ vor und zeigen, dass es eine Primzahl p mit $p > 2M+1$ und $p \equiv 1 \bmod 8$ gibt. Als Hilfsmittel verwenden wir die Primfaktorzerlegung, die eulersche φ-Funktion und den Satz von Lagrange II.7.4. Wir setzen

$$u := \prod_{k=1}^{M} (2 \cdot k + 1) \quad \text{und} \quad N_1 := (2 \cdot u)^4 + 1.$$

Man beachte

$$N_1 \equiv 1 \bmod 8.$$

Für eine Primzahl p mit $3 \leq p \leq 2M + 1$ haben wir $p|u$ und deshalb $p \nmid N_1$. Damit haben wir zu zeigen, dass eine Primzahl p mit $p|N_1$ und $p \equiv 1 \bmod 8$ existiert. Wir wählen eine Primzahl p, die N_1 teilt. Das bedeutet $N_1 \equiv 0 \bmod p$, so dass

$$(2 \cdot u)^4 \equiv -1 \bmod p.$$

Es sei $x := [2 \cdot u]_p \in \mathbb{Z}_p^\star$. In der Gruppe $\mathbb{Z}_p^\star$ hat das Element x die Ordnung 8. Mit Folgerung II.7.5 ergibt sich

$$8|\#\mathbb{Z}_p^\star, \quad \text{d.h.} \quad 8|(p - 1).$$

Diese Gleichung zeigt $p \equiv 1 \bmod 8$.

[4] Eine *arithmetische Folge* oder *arithmetische Progression* ist eine Folge $(a_k)_{k \in \mathbb{Z}}$ ganzer Zahlen, so dass die Differenz zweier aufeinanderfolgender Folgenglieder konstant ist, d.h. es gibt eine ganze Zahl $d \in \mathbb{Z}$ mit $a_k - a_{k-1} = d$ und daher $a_k = a_0 + k \cdot d$, $k \geq 1$.

III.2.6 Satz (Euler). *Es seien $n \in \mathbb{N}_+$ und $k \in \mathbb{N}$ natürliche Zahlen, so dass* $\mathrm{ggT}(k, n) = 1$. *Dann gilt*

$$k^{\varphi(n)} \equiv 1 \bmod n.$$

Beweis. Nach Eigenschaft III.2.3, i), gilt $[k]_n \in U_n$. Da U_n nach Eigenschaft III.2.3, ii), $\varphi(n)$ Elemente umfasst, ergibt sich aus Folgerung II.7.5

$$[k^{\varphi(n)}]_n = [k]_n^{\varphi(n)} = 1 \quad \text{in } U_n.$$

Das bedeutet

$$k^{\varphi(n)} \equiv 1 \bmod n$$

und liefert die Behauptung des Satzes. □

III.2.7 Folgerung (Der kleine Satz von Fermat). *Für eine Primzahl p und eine positive natürliche Zahl $k \in \mathbb{N}_+$ hat man die Kongruenz*

$$k^p \equiv k \bmod p.$$

Beweis. Falls $p|k$, ist die Aussage trivial. Andernfalls ist sie äquivalent zu der Kongruenz

$$k^{p-1} \equiv 1 \bmod p.$$

Nach Eigenschaft III.2.3, iii), gilt $\varphi(p) = p - 1$, so dass die Kongruenz im Satz von Euler III.2.6 enthalten ist. □

III.2.8 Satz. *Es sei $n \in \mathbb{N}_+$ eine positive natürliche Zahl. Dann ist $\mathbb{Z}_n$ genau dann ein Körper, wenn n eine Primzahl ist.*

Beweis. Zunächst setzen wir voraus, dass $n = p$ eine Primzahl ist. Aus Eigenschaft III.2.3, i), folgt

$$U_p = \{\, 1, ..., p-1 \,\} = \mathbb{Z}_p \setminus \{0\}.$$

Deshalb ist $\mathbb{Z}_p$ ein Körper (vgl. Definition III.1.1, ii), und Bemerkung III.1.2, iii).

Jetzt sei n keine Primzahl. Dann gibt es Zahlen[5] $l, m \in \{\, 2, ..., \lfloor n/2 \rfloor \,\}$ mit $n = l \cdot m$. Wir haben $l, m \in \mathbb{Z}_n \setminus \{0\}$ aber $l \cdot m = 0$ in $\mathbb{Z}_n$. Damit sind $l, m \in \mathbb{Z}_n \setminus \{0\}$ keine Einheiten, und $\mathbb{Z}_n$ ist kein Körper. □

III.2.9 Folgerung (Der Satz von Wilson[6]). *Für jede Primzahl p gilt*

$$(p-1)! \equiv -1 \bmod p.$$

Beweis. Nach Satz III.2.8 ist $\mathbb{Z}_p$ ein Körper. Die quadratische Gleichung $x^2 - 1 = 0$ hat die Lösungen $x_1 = 1$ und $x_2 = p - 1$ und keine weiteren. Das bedeutet, dass

$$k^{-1} \neq k \quad \text{für} \quad k \in \{\, 2, ..., p-2 \,\}.$$

[5] Für eine reelle Zahl $x \in \mathbb{R}$ ist

$$\lfloor x \rfloor := \max\{\, l \in \mathbb{Z} \mid l \leq x \,\}$$

die (*untere*) *Gauß-Klammer* von x (vgl. [16], Beispiel 3.1.3, v).

[6] John Wilson (1741 - 1793), britischer Mathematiker.

Wir folgern

$$2 \cdot 3 \cdot \cdots \cdot (p-2) = 1. \tag{III.1}$$

In der Tat kommt in dem Produkt mit jeder Zahl auch ihr Inverses vor. Da keine zwei Zahlen dasselbe Inverse haben und nach dem zuvor Gesagten keine der Zahlen mit ihrem Inversen übereinstimmt, folgt (III.1). Wegen $p - 1 \equiv -1 \bmod p$ ergibt sich aus (III.1) die Behauptung. □

Ein kurzer Ausflug in die Kryptographie

Wir wollen hier kurz das RSA-Verfahren der Kryptographie anreißen, das auf Rivest,[7] Shamir[8] und Adleman[9] zurückgeht. Das Skript [9] und das Buch [15] besprechen den mathematischen Hintergrund ausführlicher. Details zur Anwendung und Bedeutung des Verfahrens in der Kryptographie werden z.B. in Wikipedia ausgeführt.

Person B möchte an Person A eine verschlüsselte Nachricht senden. Person A

- ⋆ wählt zwei (große[10]) Primzahlen p und q,
- ⋆ setzt $n := p \cdot q$ und berechnet daraus $\varphi(n) = (p-1) \cdot (q-1)$,
- ⋆ bestimmt eine natürliche Zahl e mit $1 < e < \varphi(n)$ und $\mathrm{ggT}(e, \varphi(n)) = 1$,
- ⋆ ermittelt mit dem erweiterten euklidischen Algorithmus eine ganze Zahl d, so dass $d \cdot e \equiv 1 \bmod \varphi(n)$,
- ⋆ gibt den **öffentlichen Schlüssel** (**public key**) (n, e) bekannt.

Eine Person B, die eine verschlüsselte Nachricht A schicken möchte, benutzt dazu die **Kodierungsfunktion**

$$\begin{array}{rccc} E_e \colon & \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \\ & k & \longmapsto & [k^e]_n. \end{array}$$

Person A entschlüsselt die erhaltene Nachricht mit der **Dekodierungsfunktion**[11]

$$\begin{array}{rccc} D_d \colon & \mathbb{Z}_n & \longrightarrow & \mathbb{Z}_n \\ & k & \longmapsto & [k^d]_n. \end{array}$$

Es gibt eine ganze Zahl $l \in \mathbb{Z}$ mit $d \cdot e = 1 + l \cdot \varphi(n)$. Deshalb finden wir

$$\big(E_e(k)\big)^d \equiv (k^e)^d = k^{d \cdot e} = k \cdot (k^l)^{\varphi(n)} \equiv k \bmod n.$$

Warum gilt hier $k \cdot (k^l)^{\varphi(n)} \equiv k \bmod n$?

- ⋆ Falls $k = 0$, ist nichts zu zeigen.

[7] Ronald Linn Rivest (⋆1947), amerikanischer Mathematiker und Kryptologe.

[8] Adi Shamir (⋆1952), israelischer Kryptologieexperte.

[9] Leonard Adleman (⋆1945), amerikanischer Informatiker und Molekularbiologe.

[10] Die Leserin bzw. der Leser möge die oben erwähnten Quellen konsultieren, um herauszufinden, was „groß“ in diesem Zusammenhang bedeutet.

[11] Man beachte, dass d nur A bekannt ist.

- ⋆ Falls $\mathrm{ggT}(k,n) = 1$, dann gilt auch $\mathrm{ggT}(k^l,n) = 1$ und der Satz von Euler III.2.6 liefert $(k^l)^{\varphi(n)} \equiv 1 \bmod n$.

- ⋆ Um alle Fälle abzudecken, benutzen wir den Chinesischen Restsatz III.1.4:

$$\mathbb{Z}_n \cong \mathbb{Z}_p \times \mathbb{Z}_q.$$

Für eine Primzahl s und eine ganze Zahl m gilt entweder $s|m$, d.h. $m \equiv 0 \bmod s$, oder $s \nmid m$, d.h. $\mathrm{ggT}(m,s) = 1$. Mit den bereits vorgestellten Argumenten und Eigenschaft III.2.3, ii), folgern wir:

$$\begin{array}{rcl} k \cdot (k^l)^{\varphi(n)} & \equiv & k \cdot (k^l)^{\varphi(p)\cdot\varphi(q)} \equiv k \cdot (k^{l\cdot\varphi(q)})^{\varphi(p)} \equiv k \bmod p, \\ k \cdot (k^l)^{\varphi(n)} & \equiv & k \cdot (k^l)^{\varphi(p)\cdot\varphi(q)} \equiv k \cdot (k^{l\cdot\varphi(p)})^{\varphi(q)} \equiv k \bmod q. \end{array}$$

Diese beiden Kongruenzen implizieren $k \cdot (k^l)^{\varphi(n)} \equiv k \bmod n$.

III.2.10 Bemerkung. i) Die Nachricht muss also eine Zahl zwischen 0 und $n-1$ sein. Eine Textnachricht wandelt man z.B. mit dem ASCII-Kode in eine Zahl um. Man zerlegt die Nachricht weiter so in Blöcke, dass jeder Block einer Zahl in $\{0, ..., n-1\}$ entspricht.

ii) Die Sicherheit des Verfahrens beruht darauf, dass die Faktorisierung großer Zahlen schwierig ist. Allgemein sind zur Verschlüsselung solche Operationen nützlich, die sich leicht ausführen lassen, deren Umkehrung aber nur mühsam zu bewerkstelligen ist.

III.2.11 Beispiel. Wir wählen $p = 17$, $q = 19$ und $n = p \cdot q = 323$. Damit ergibt sich

$$\varphi(n) = (p-1)\cdot(q-1) = 16 \cdot 18 = 288 = 2^5 \cdot 3^2.$$

Eine zu $\varphi(n)$ teilerfremde Zahl ist z.B. $e = 95 = 5 \cdot 19$. Der öffentliche Schlüssel lautet

$$(323, 95).$$

Wir wollen die Nachricht $k = 24$ versenden. Mit einem geeigneten Computerprogramm, z.B. Maple, berechnet man

$$E_e(24) = 24^{95} \equiv 294 \bmod 323.$$

Für $d = 191$ gilt

$$d \cdot e = 18\,145 = 1 + 63 \cdot 288.$$

Man verifiziert schließlich

$$D_d(294) = 294^{191} \equiv 24 \bmod 323.$$

III.3 Die Einheitengruppe eines endlichen Körpers

III.3.1 Satz. *Es seien k ein Körper und $G \subset k^\star$ eine **endliche** Untergruppe. Dann ist G zyklisch.*

Beweis. Nach dem Hauptsatz über endlich erzeugte abelsche Gruppen II.13.5 gibt es natürliche Zahlen $t \geq 1$ und $m_1, ..., m_t$ mit $m_i | m_{i+1}$, $i = 1, ..., t-1$, so dass[12]

$$G \cong \mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_t}.$$

Wir wollen die Annahme $t > 1$ zum Widerspruch führen. Unter dieser Annahme besitzt $k^\star$ eine zu $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}$ isomorphe Untergruppe. Es sei p eine Primzahl, die m_1 teilt. Wegen $m_1 | m_2$ gibt es natürliche Zahlen $1 \leq r \leq s$ und m_1', m_2' mit

$$m_1 = p^r \cdot m_1', \quad m_2 = p^s \cdot m_2', \quad p \nmid m_1' \quad \text{und} \quad p \nmid m_2'.$$

Aus dem chinesischen Restsatz III.1.4 folgt weiter

$$\mathbb{Z}_{m_1} \cong \mathbb{Z}_{p^r} \times \mathbb{Z}_{m_1'} \quad \text{und} \quad \mathbb{Z}_{m_2} \cong \mathbb{Z}_{p^s} \times \mathbb{Z}_{m_2'}.$$

Wir erkennen, dass $k^\star$ eine zu

$$\mathbb{Z}_{p^r} \times \mathbb{Z}_{p^s}$$

isomorphe Untergruppe H enthält. Da $p^r | p^s$, gilt $p^s \cdot l = 0$ für jedes Element $l \in \mathbb{Z}_{p^r} \times \mathbb{Z}_{p^s}$. Jetzt wechseln wir von der additiven Schreibweise in $\mathbb{Z}_{p^r} \times \mathbb{Z}_{p^s}$ zur multiplikativen Schreibweise in $k^\star$ und halten fest:

$$\forall a \in H: \quad a^{p^s} = 1.$$

Die Ungleichung

$$\#H = p^{r+s} > p^s$$

zeigt, dass das Polynom

$$x^{p^s} - 1$$

mehr als p^s Nullstellen in k hat. Das widerspricht aber Folgerung A.1.9, so dass $t = 1$ gelten muss. □

III.3.2 Folgerung. *Es seien p eine Primzahl. Dann gilt*

$$U_p \cong \mathbb{Z}_{p-1}.$$

III.3.3 Definition. Es sei p eine Primzahl. Eine ganze Zahl $\zeta \in \mathbb{Z}$ ist eine *Primitivwurzel modulo p*, wenn $[\zeta]_p$ die Gruppe U_p erzeugt.

III.4 Das quadratische Reziprozitätsgesetz

Quadratische Kongruenzen

Es seien p eine Primzahl und $a, b, c \in \mathbb{Z}$ ganze Zahlen. Wir wollen die Kongruenz

$$a \cdot x^2 + b \cdot x + c \equiv 0 \bmod p \tag{III.2}$$

untersuchen. Um nicht die bereits behandelten linearen Kongruenzen zu wiederholen, setzen wir

$$a \not\equiv 0 \bmod p \tag{III.3}$$

voraus.

[12] Da G eine Untergruppe der multiplikativen Gruppe von k ist, wird die Vernüpfung in G mit „·“ bezeichnet. Die Verknüpfung auf der rechten Seite wird mit „+“ notiert, weil sie durch die Addition ganzer Zahlen induziert wird.

III.4.1 Bemerkung. Da p eine Primzahl ist, ist $\mathbb{F}_p := \mathbb{Z}_p$ ein Körper (Satz III.2.8). Das gestellte Problem ist somit äquivalent zu der Gleichung

$$[a]_p \cdot x^2 + [b]_p \cdot x + [c]_p = 0$$

über dem endlichen Körper $\mathbb{F}_p$.

Auf Grund der Voraussetzung (III.3) existiert eine ganze Zahl $a' \in \mathbb{Z}$ mit $a' \cdot a \equiv 1 \bmod p$. Die quadratische Kongruenz (III.2) ist deshalb äquivalent zu der Kongruenz

$$x^2 + a' \cdot b \cdot x + a' \cdot c \equiv 0 \bmod p. \tag{III.4}$$

Anders gesagt dürfen wir ohne Beschränkung der Allgemeinheit $a = 1$ annehmen.

III.4.2 Beispiel. Wir behandeln den Fall $p = 2$. Hier gibt es lediglich die folgenden Kongruenzen:

$$\begin{aligned}
&\text{(I)} && x^2 \equiv 0 \bmod 2\\
&\text{(II)} && x^2 + x = x \cdot (x+1) \equiv 0 \bmod 2\\
&\text{(III)} && x^2 + 1 \equiv (x+1)^2 \equiv 0 \bmod 2\\
&\text{(IV)} && x^2 + x + 1 \equiv 0 \bmod 2.
\end{aligned}$$

Wir können sofort die Lösungen dieser Gleichungen hinschreiben

$$\begin{aligned}
&\text{(I)} && x = 0\\
&\text{(II)} && x = 0 \wedge x = 1\\
&\text{(III)} && x = 1\\
&\text{(IV)} && \text{keine.}
\end{aligned}$$

Den Fall $p = 2$ können wir in den folgenden Betrachtungen ausklammern. Für $p \geq 3$ finden wir eine ganze Zahl $e \in \mathbb{Z}$ mit

$$2 \cdot e \equiv 1 \bmod p.$$

Damit können wir die Kongruenz (III.4) umschreiben zu

$$(x + b \cdot e)^2 \equiv b^2 \cdot e^2 - c \bmod p. \tag{III.5}$$

Daher beschäftigen wir uns im Folgenden mit einer Kongruenz der Form

$$x^2 \equiv a \bmod p$$

mit $a \in \mathbb{Z}$.

III.4.3 Definition. Es seien p eine Primzahl und $a \in \mathbb{Z}$ eine ganze Zahl mit $a \not\equiv 0 \bmod p$. Man sagt, a ist ein *quadratischer Rest* modulo p, wenn die Kongruenz

$$x^2 \equiv a \bmod p$$

eine Lösung besitzt. Ansonsten ist a ein *quadratischer Nichtrest* modulo p.

Das Legendre-Symbol

III.4.4 Definition. Es seien p eine Primzahl und $a \in \mathbb{Z}$. Die Zahl

$$\left(\frac{a}{p}\right) := \begin{cases} 0, & \text{falls } a \equiv 0 \bmod p \\ 1, & \text{falls } a \text{ quadratischer Rest modulo } p \\ -1, & \text{falls } a \text{ quadratischer Nichtrest modulo } p \end{cases}$$

heißt das *Legendre-Symbol* von a und p.

III.4.5 Bemerkung. Offenbar gilt

$$\forall p \text{ Primzahl } \forall a, b \in \mathbb{Z}: \quad a \equiv b \bmod p \quad \Longrightarrow \quad \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$

Da ferner

$$\left(\frac{0}{p}\right) = 0,$$

muss man (a/p) nur für $a \in \{1, ..., p-1\}$ bestimmen.

III.4.6 Beispiel. In $\mathbb{Z}_5$ haben wir $1^2 = 1$, $2^2 = 4$, $3^2 = 4$ und $4^2 = 1$. Somit gilt für $a = 0, ..., 4$

$$\left(\frac{a}{5}\right) = \begin{cases} 0, & \text{falls } a = 0 \\ 1, & \text{falls } a = 1, 4 \\ -1, & \text{falls } a = 2, 3 \end{cases}.$$

III.4.7 Satz (Euler). *Für jede Primzahl $p \geq 3$ und jede ganze Zahl $a \in \mathbb{Z}$ gilt*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \bmod p.$$

Beweis. Falls $a \equiv 0 \bmod p$, lautet die Behauptung $0 \equiv 0 \bmod p$ und stimmt. Für $a \not\equiv 0 \bmod p$ finden wir mit Satz III.2.6

$$\left(a^{\frac{p-1}{2}}\right)^2 = a^{p-1} \equiv 1 \bmod p.$$

Für die Zahl $x := a^{\frac{p-1}{2}}$ gilt demnach $x^2 - 1 = (x-1) \cdot (x+1) \equiv 0 \bmod p$, d.h. $p|(x^2-1)$. Nach Satz I.4.5 bedeutet dies $p|(x-1)$ oder $p|(x+1)$, so dass

$$x \equiv 1 \bmod p \quad \text{oder} \quad x \equiv -1 \bmod p.$$

Unsere Behauptung lautet demnach

$$x \equiv 1 \bmod p \quad \Longleftrightarrow \quad \left(\frac{a}{p}\right) = 1.$$

Es seien $\zeta \in \mathbb{Z}$ eine Primitivwurzel modulo p (Definition III.3.3) und $l \in \mathbb{Z}$ eine ganze Zahl mit $a \equiv \zeta^l \bmod p$. Dann ist die Kongruenz

$$x \equiv \zeta^{l \cdot \frac{p-1}{2}} \equiv 1 \bmod p$$

wegen Folgerung II.7.5 äquivalent zu

$$(p-1)\Big|\left(l\cdot\frac{p-1}{2}\right)$$

also dazu, dass l gerade ist. Wenn l gerade ist, ist a offenbar ein quadratischer Rest modulo p. Wenn l ungerade ist, $l = 2m+1$, dann gibt es keine ganze Zahl k, so dass

$$\zeta^l \equiv \zeta^{2k} \bmod p, \quad \text{d.h.} \quad \zeta^{2(m-k)+1} \equiv 1 \bmod p, \tag{III.6}$$

denn diese Gleichung ist wie zuvor äquivalent zu

$$(p-1)|(2\cdot(m-k)+1).$$

Da $p-1$ nach Voraussetzung gerade ist und $2\cdot(m-k)+1$ ungerade, ist dies unmöglich. Da Gleichung (III.6) nicht erfüllt werden kann, ist a ein quadratischer Nichtrest modulo p. □

Aus dem Satz von Euler III.4.7 ergeben sich wichtige Rechenregeln für das Legendre-Symbol:

III.4.8 Folgerung. *Es sei $p \geq 3$ eine Primzahl.*

i) *Es gilt*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{falls } p \equiv 1 \bmod 4 \\ -1, & \text{falls } p \equiv -1 \bmod 4 \end{cases}.$$

ii) *Für je zwei ganze Zahlen $a, b \in \mathbb{Z}$ hat man*

$$\left(\frac{a\cdot b}{p}\right) = \left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right).$$

iii) *Es seien $a, b \in \mathbb{Z}$ zwei ganze Zahlen, so dass $b \not\equiv 0 \bmod p$. Dann folgt*

$$\left(\frac{a\cdot b^2}{p}\right) = \left(\frac{a}{p}\right).$$

Beweis. i) Aus dem Satz von Euler folgt

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \bmod p.$$

Auf beiden Seiten können nur die Werte ± 1 angenommen werden. Wegen $p > 2$ bedeutet die Kongruenz daher Gleichheit (s. Beispiel I.6.4, i).

ii) Der Satz von Euler liefert

$$\left(\frac{a\cdot b}{p}\right) \equiv (a\cdot b)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}}\cdot b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right) \bmod p.$$

Ganz links und ganz rechts tauchen wiederum nur die Werte ± 1 auf, so dass wir wie in i) die Gleichheit dieser Zahlen folgern.

iii) Die Voraussetzung $b \not\equiv 0 \bmod p$ impliziert $(b/p) = \pm 1$. Mit ii) erhalten wir

$$\left(\frac{a\cdot b^2}{p}\right) = \left(\frac{a}{p}\right)\cdot\left(\frac{b}{p}\right)^2 = \left(\frac{a}{p}\right)$$

und zeigen somit die Behauptung. □

III.4.9 Bemerkung. i) Teil ii) der Folgerung besagt, dass

$$\begin{aligned}\left(\frac{\cdot}{p}\right): \mathbb{Z}_p^\star &\longrightarrow \{\pm 1\}\\ x &\longmapsto \left(\frac{x}{p}\right)\end{aligned}$$

ein Gruppenhomomorphismus ist. Der Kern besteht aus den quadratischen Resten modulo p. Die quadratischen Reste modulo p bilden somit eine Untergruppe von $\mathbb{Z}_p^\star$ mit $(p-1)/2$ Elementen. Ebenso gibt es $(p-1)/2$ quadratische Nichtreste modulo p.

Es sei $\zeta \in \mathbb{Z}$ eine Primitivwurzel modulo p. Bereits im Beweis des Satzes von Euler haben wir

$$\forall l \in \mathbb{Z}: \quad \zeta^l \text{ ist quadratischer Rest modulo } p \quad \Longleftrightarrow \quad l \text{ ist gerade}$$

erkannt.

ii) Auf Grund von Folgerung ii) reicht es, bei gegebener Primzahl $p \geq 3$ die Legendre-Symbole (q/p), q eine Primzahl, zu ermitteln.

Absolut kleinste Reste und ein Lemma von Gauß

III.4.10 Definition. Für eine Primzahl $p \geq 3$ sei

$$H(p) := \left\{1, ..., \frac{p-1}{2}\right\}.$$

III.4.11 Lemma. *Es seien $p \geq 3$ eine Primzahl und $a \in \mathbb{Z}$ eine ganze Zahl mit $a \not\equiv 0 \bmod p$. Dann existieren eindeutig bestimmte Zahlen $\varepsilon \in \{\pm 1\}$ und $\sigma \in H(p)$, so dass*

$$a \equiv \varepsilon \cdot \sigma \bmod p.$$

Beweis. Die Aussage ist offensichtlich. □

III.4.12 Definitionen. i) In der Situation des Lemmas heißt $\varepsilon \cdot \sigma$ der *absolut kleinste Rest* von a modulo p.

ii) Für $a \in \mathbb{Z}$ mit $a \not\equiv 0 \bmod p$ und $x \in H(p)$[13] seien $\varepsilon_a(x) \in \{\pm 1\}$ und $\sigma_a(x) \in H(p)$ die eindeutig bestimmten Zahlen, für die $\varepsilon_a(x) \cdot \sigma_a(x)$ der absolut kleinste Rest von $a \cdot x$ modulo p ist.

Das folgende Resultat gibt eine weitere Formel für das Legendre-Symbol an.

III.4.13 Lemma (Gauß; 1. Fassung). *Es seien $p \geq 3$ eine Primzahl und $a \in \mathbb{Z}$ eine ganze Zahl mit $a \not\equiv 0 \bmod p$. Dann gilt*

$$\left(\frac{a}{p}\right) = \prod_{x \in H(p)} \varepsilon_a(x).$$

[13] Man beachte, dass $x \not\equiv 0 \bmod p$ und deshalb $a \cdot x \not\equiv 0 \bmod p$.

Beweis. Zunächst bemerken wir, dass es zu jedem $y \in H(p)$ (genau) ein $x \in H(p)$ mit $\sigma_a(x) = y$ gibt. In der Tat ist die Kongruenz

$$a \cdot x \equiv \varepsilon \cdot y \bmod p$$

für $\varepsilon = \pm 1$ mit $x \in \{ 1, ..., p-1 \}$ eindeutig lösbar, weil $\mathrm{ggT}(a, p) = 1$. Bei geeigneter Wahl von ε gilt dann $x \in H(p)$.

Ferner berechnen wir

$$a^{\frac{p-1}{2}} \cdot \prod_{x \in H(p)} x = \prod_{x \in H(p)} (a \cdot x) \equiv \prod_{x \in H(p)} \varepsilon_a(x) \cdot \prod_{x \in H(p)} \sigma_a(x) = \prod_{x \in H(p)} \varepsilon_a(x) \cdot \prod_{x \in H(p)} x \bmod p. \quad \text{(III.7)}$$

Desweiteren hat man

$$p \nmid \prod_{x \in H(p)} x.$$

Daher folgt aus (III.7), dass

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \equiv \prod_{x \in H(p)} \varepsilon_a(x) \bmod p.$$

Links und rechts steht wieder nur ± 1, so dass zusammen mit $p \geq 3$ wieder Gleichheit folgt. □

III.4.14 Beispiel. Mit dem obigen Lemma berechnen wir $(2/7)$. Wir haben

$$H(7) = \{ 1, 2, 3 \}, \quad 2 \cdot 1 = 2, \quad 2 \cdot 2 = 4 \equiv -3 \bmod 7, \quad 2 \cdot 3 = 6 \equiv -1 \bmod 7.$$

Das obige Lemma zeigt

$$\left(\frac{2}{7}\right) = \varepsilon_2(1) \cdot \varepsilon_2(2) \cdot \varepsilon_2(3) = 1 \cdot (-1) \cdot (-1) = 1.$$

Daher ist 2 ein quadratischer Rest modulo 7.

Um für $a \in \mathbb{Z}$ mit $a \not\equiv 0 \bmod p$ das Vorzeichen $\varepsilon = \varepsilon_a(1) \in \{\pm 1\}$ in Lemma III.4.11 zu bestimmen, bilden wir in $\mathbb{R}$ die Intervalle

$$I_\nu := \left((\nu - 1) \cdot \frac{p}{2}, \nu \cdot \frac{p}{2}\right), \quad \nu \in \mathbb{Z}.$$

Da p ungerade ist, sind die Intervallgrenzen entweder nicht ganzzahlig oder durch p teilbar. Jede ganze Zahl $a \in \mathbb{Z}$, die nicht durch p teilbar ist, liegt deswegen in genau einem der Intervalle I_ν, $\nu \in \mathbb{Z}$.

III.4.15 Lemma. *Für eine ganze Zahl $a \in \mathbb{Z}$ mit $a \not\equiv 0 \bmod p$ gilt genau dann $\varepsilon_a(1) = -1$, wenn es eine **gerade** ganze Zahl $\nu \in \mathbb{Z}$ mit $a \in I_\nu$ gibt.*

Beweis. Falls $\varepsilon_a(1) = -1$, dann finden wir

$$a = l + 2 \cdot k \cdot \frac{p}{2} \quad \text{mit} \quad k \in \mathbb{Z} \quad \text{und} \quad -\left(\frac{p-1}{2}\right) \leq l \leq -1$$

und folgern

$$(2 \cdot k - 1) \cdot \frac{p}{2} = -\frac{p}{2} + 2 \cdot k \cdot \frac{p}{2} < l + 2 \cdot k \cdot \frac{p}{2} < 2 \cdot k \cdot \frac{p}{2},$$

d.h. $a \in I_{2k}$. Umgekehrt liefert $a \in I_{2k}$, also

$$(2 \cdot k - 1) \cdot \frac{p}{2} < a < 2 \cdot k \cdot \frac{p}{2},$$

dass

$$-\frac{p}{2} < a - k \cdot p < 0$$

und damit $a - k \cdot p \in \{ -(p-1)/2, ..., -1 \}$ und $\varepsilon_a(1) = -1$. □

Für eine **natürliche** Zahl $a \in \mathbb{N} \setminus \{0\}$, $x \in H(p)$ und $\nu \in \mathbb{Z}$ gilt:

$$\begin{aligned} & (\nu - 1) \cdot \frac{p}{2} < a \cdot x < \nu \cdot \frac{p}{2} \\ \iff \quad & (\nu - 1) \cdot \frac{p}{2 \cdot a} < x < \nu \cdot \frac{p}{2 \cdot a}. \end{aligned} \tag{III.8}$$

Aus der Voraussetzung $x \in H(p)$ folgt $1 \leq \nu \leq a$. Umgekehrt implizieren $x \in \mathbb{Z}$, $1 \leq \nu \leq a$ und (III.8) bereits $x \in H(p)$.

III.4.16 Lemma. *Für $a \in \mathbb{N}$ mit $a \not\equiv 0 \bmod p$ und $1 \leq \nu \leq a$ gilt*

$$\#\{ x \in \mathbb{Z} \mid a \cdot x \in I_\nu \} = \left\lfloor \nu \cdot \frac{p}{2 \cdot a} \right\rfloor - \left\lfloor (\nu - 1) \cdot \frac{p}{2 \cdot a} \right\rfloor.$$

Beweis. Die Zahl auf der rechten Seite gibt die Anzahl der ganzen Zahlen im halboffenen Intervall

$$\widetilde{I_\nu} := \left((\nu - 1) \cdot \frac{p}{2 \cdot a}, \nu \cdot \frac{p}{2 \cdot a} \right]$$

an. Es ist zu zeigen, dass die rechte Intervallgrenze nicht ganzzahlig sein kann. Sie ist genau dann ganzzahlig, wenn $(2 \cdot a) | (\nu \cdot p)$. Wir setzen $p \neq 2$ und $a \not\equiv 0 \bmod p$ voraus. Die genannte Bedingung ist somit äquivalent zu $(2 \cdot a) | \nu$. Das ist wegen $1 \leq \nu \leq a$ unmöglich, und die obere Intervallgrenze ist nicht ganzzahlig. □

Aus unseren Überlegungen ergibt sich die folgende Umformulierung von Lemma III.4.13:

III.4.17 Lemma (Gauß; 2. Fassung). *Es seien $p \geq 3$ eine Primzahl, $a > 0$ eine positive ganze Zahl mit $a \not\equiv 0 \bmod p$. Mit*

$$m := \sum_{k=1}^{\left\lfloor \frac{a}{2} \right\rfloor} \left(\left\lfloor k \cdot \frac{p}{a} \right\rfloor - \left\lfloor \left(k - \frac{1}{2} \right) \cdot \frac{p}{a} \right\rfloor \right)$$

gilt

$$\left(\frac{a}{p} \right) = (-1)^m.$$

Diese Formel ermöglicht uns die Berechnung der Legendre-Symbole $(2/p)$:

III.4.18 Satz. *Für eine Primzahl $p \geq 3$ hat man*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{falls } p \equiv \pm 1 \bmod 8 \\ -1, & \text{falls } p \equiv \pm 3 \bmod 8 \end{cases}.$$

Beweis. Mit dem Lemma von Gauß in der zweiten Fassung erkennen wir

$$\left(\frac{2}{p}\right) = (-1)^m, \quad m = \left\lfloor \frac{p}{2} \right\rfloor - \left\lfloor \frac{p}{4} \right\rfloor.$$

Für $k \in \mathbb{Z}$ und $p \in \{ 8 \cdot k \pm 1, 8 \cdot k \pm 3 \}$ bestimmen wir m anhand der folgenden Tabelle:

p	$\left\lfloor \frac{p}{2} \right\rfloor$	$\left\lfloor \frac{p}{4} \right\rfloor$	m	$\left(\frac{2}{p}\right)$
$8 \cdot k - 1$	$4 \cdot k - 1$	$2 \cdot k - 1$	$2 \cdot k$	1
$8 \cdot k + 1$	$4 \cdot k$	$2 \cdot k$	$2 \cdot k$	1
$8 \cdot k - 3$	$4 \cdot k - 2$	$2 \cdot k - 1$	$2 \cdot k - 1$	-1
$8 \cdot k + 3$	$4 \cdot k + 1$	$2 \cdot k$	$2 \cdot k + 1$	-1

Daraus lesen wir die Behauptung des Satzes ab. □

Das quadratische Reziprozitätsgesetz

III.4.19 Das quadratische Reziprozitätsgesetz. *Es seien $p, q \geq 3$ zwei verschiedene Primzahlen. Dann gilt*

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = \begin{cases} -1, & \text{falls } p \equiv q \equiv 3 \bmod 4 \\ 1, & \text{sonst} \end{cases}.$$

Im Beweis benötigen wir einen weiteren Hilfssatz. Man beachte zunächst, dass $p - q$ gerade ist, weil sowohl p als auch q ungerade sind. Somit gilt entweder $p - q \equiv 0 \bmod 4$ oder $p - q \equiv 2 \bmod 4$. Im zweiten Fall folgt $p + q \equiv 2 + 2 \cdot q \equiv 0 \bmod 4$, denn q ist ungerade.

III.4.20 Hilfssatz. *Es seien $p, q \geq 3$ zwei verschiedene Primzahlen und $r > 0$ eine positive ganze Zahl mit $p \equiv q \bmod 4r$ oder $p \equiv -q \bmod 4r$. Dann folgt*

$$\left(\frac{r}{p}\right) = \left(\frac{r}{q}\right).$$

Beweis. Wir definieren

$$s_\varkappa := \left\lfloor \varkappa \cdot \frac{p}{2 \cdot r} \right\rfloor \quad \text{und} \quad t_\varkappa := \left\lfloor \varkappa \cdot \frac{q}{2 \cdot r} \right\rfloor, \quad \varkappa = 1, ..., r.$$

Nach dem Lemma von Gauß III.4.17 gilt

$$\left(\frac{r}{p}\right) = (-1)^m \quad \text{mit} \quad m = \sum_{k=1}^{\left\lfloor \frac{r}{2} \right\rfloor} (s_{2k} - s_{2k-1})$$

und

$$\left(\frac{r}{q}\right) = (-1)^n \quad \text{mit} \quad n = \sum_{k=1}^{\left\lfloor \frac{r}{2} \right\rfloor} (t_{2k} - t_{2k-1}).$$

Fall 1: $q \equiv p \bmod 4r$. Es sei

$$q = p + 4 \cdot r \cdot l \quad \text{mit} \quad l \in \mathbb{Z}.$$

Dabei können wir ohne Beschränkung der Allgemeinheit $l > 0$ annehmen. Somit ergibt sich

$$t_\varkappa = \left\lfloor \varkappa \cdot \frac{p + 4 \cdot r \cdot l}{2 \cdot r} \right\rfloor = \left\lfloor \varkappa \cdot \frac{p}{2 \cdot r} + 2 \cdot \varkappa \cdot l \right\rfloor = \left\lfloor \varkappa \cdot \frac{p}{2 \cdot r} \right\rfloor + 2 \cdot \varkappa \cdot l, \quad \varkappa = 1, ..., r.$$

Daran erkennen wir

$$t_\varkappa \equiv s_\varkappa \bmod 2, \quad \varkappa = 1, ..., r.$$

Dies wiederum impliziert

$$m \equiv n \bmod 2$$

und

$$\left(\frac{r}{p}\right) = (-1)^m = (-1)^n = \left(\frac{r}{q}\right).$$

Fall 2: $q \equiv -p \bmod 4r$. In diesem Fall schreiben wir $q = -p + 4 \cdot r \cdot l$ mit $l > 0$ und finden

$$t_\varkappa = \left\lfloor \varkappa \cdot \frac{4 \cdot r \cdot l - p}{2 \cdot r} \right\rfloor = 2 \cdot \varkappa \cdot l + \left\lfloor -\varkappa \cdot \frac{p}{2 \cdot r} \right\rfloor = 2 \cdot \varkappa \cdot l - s_\varkappa - 1, \quad \varkappa = 1, ..., r. \quad \text{(III.9)}$$

Bei der letzten Umformung ist zu beachten, dass $(\varkappa \cdot p)/(2 \cdot r)$ keine ganze Zahl ist, $\varkappa = 1, ..., r$. Aus (III.9) folgt

$$t_{2k} - t_{2k-1} \equiv s_{2k} - s_{2k-1} \bmod 2, \quad k = 1, ..., \left\lfloor \frac{r}{2} \right\rfloor.$$

Daraus folgt wieder

$$m \equiv n \bmod 2, \quad \left(\frac{r}{p}\right) = \left(\frac{r}{q}\right)$$

und damit die Behauptung. □

Beweis des quadratischen Reziprozitätsgesetzes III.4.19. **Fall 1: $p \equiv q \bmod 4$.** Indem wir gegebenenfalls die Rollen von p und q vertauschen, dürfen wir annehmen, dass ein $r > 0$ mit $p = q + 4 \cdot r$ existiert. Hilfssatz III.4.20 zeigt

$$\left(\frac{r}{p}\right) = \left(\frac{r}{q}\right). \quad \text{(III.10)}$$

Weiter gilt offenkundig

$$\left(\frac{4}{p}\right) = \left(\frac{4}{q}\right) = 1.$$

Unter Benutzung von Folgerung III.4.8 errechnen wir

$$\left(\frac{r}{p}\right) = \left(\frac{4 \cdot r}{p}\right) = \left(\frac{p - q}{p}\right) = \left(\frac{-q}{p}\right) = \left(\frac{-1}{p}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot \left(\frac{q}{p}\right) \quad \text{(III.11)}$$

sowie

$$\left(\frac{r}{q}\right) = \left(\frac{4 \cdot r}{q}\right) = \left(\frac{q + 4 \cdot r}{q}\right) = \left(\frac{p}{q}\right). \tag{III.12}$$

Aus (III.10), (III.11) und (III.12) schließen wir

$$\left(\frac{q}{p}\right) = \begin{cases} -\left(\frac{p}{q}\right), & \text{falls } p \equiv q \equiv 3 \bmod 4 \\ \left(\frac{p}{q}\right), & \text{falls } p \equiv q \equiv 1 \bmod 4 \end{cases}.$$

Fall 2: $p \equiv -q \bmod 4$. In diesem Fall existiert eine natürliche Zahl $r > 0$ mit $p + q = 4 \cdot r$. Hilfssatz III.4.20 liefert wieder

$$\left(\frac{r}{p}\right) = \left(\frac{r}{q}\right),$$

und mit Folgerung III.4.8 und Bemerkung III.4.5 erhält man

$$\left(\frac{r}{p}\right) = \left(\frac{4 \cdot r}{p}\right) = \left(\frac{4 \cdot r - p}{p}\right) = \left(\frac{q}{p}\right)$$

und

$$\left(\frac{r}{q}\right) = \left(\frac{4 \cdot r}{q}\right) = \left(\frac{4 \cdot r - q}{q}\right) = \left(\frac{p}{q}\right).$$

Damit ist das quadratische Reziprozitätsgesetz bewiesen. □

Obwohl man es dem quadratischen Reziprozitätsgesetz auf den ersten Blick vielleicht nicht ansieht, ist es sehr nützlich für die Berechnung von Legendre-Symbolen. Die nächsten Beispiele zeigen warum.

III.4.21 Beispiele. i) Wir möchten herausfinden, ob die Kongruenz $x^2 \equiv 10 \bmod 13$ eine Lösung besitzt. Dazu ist

$$\left(\frac{10}{13}\right) = \left(\frac{2}{13}\right) \cdot \left(\frac{5}{13}\right)$$

zu berechnen. Da $13 \equiv -3 \bmod 8$ zeigt Satz III.4.18, dass $(2/13) = -1$. Die wiederholte Anwendung des quadratischen Reziprozitätsgesetzes III.4.19 und der Bemerkung III.4.5 ergibt

$$\left(\frac{5}{13}\right) = \left(\frac{13}{5}\right) = \left(\frac{3}{5}\right) = \left(\frac{5}{3}\right) = \left(\frac{2}{3}\right) = -1.$$

Die letzte Gleichung überprüft man direkt oder mit Satz III.4.18. Wir erkennen

$$\left(\frac{10}{13}\right) = \left(\frac{2}{13}\right) \cdot \left(\frac{5}{13}\right) = (-1) \cdot (-1) = 1,$$

so dass die untersuchte Kongruenz lösbar ist.

ii) Diesmal wollen wir die Kongruenz $x^2 \equiv 59 \bmod 89$ auf ihre Lösbarkeit untersuchen. Mit Hilfe des quadratischen Reziprozitätsgesetzes III.4.19 und Folgerung III.4.8, ii), berechnen wir

$$\left(\frac{59}{89}\right) \overset{89 \equiv 1 \bmod 4}{=} \left(\frac{89}{59}\right) = \left(\frac{30}{59}\right) = \left(\frac{2}{59}\right) \cdot \left(\frac{3}{59}\right) \cdot \left(\frac{5}{59}\right).$$

Mit $59 = 7 \cdot 8 + 3$ und Satz III.4.18 berechnen wir

$$\left(\frac{2}{59}\right) = -1,$$

mit $59 \equiv 3 \bmod 4$, dem quadratischen Reziprozitätsgesetz III.4.19 und Satz III.4.18

$$\left(\frac{3}{59}\right) = -\left(\frac{59}{3}\right) = -\left(\frac{2}{3}\right) = 1$$

und schließlich mit $5 \equiv 1 \bmod 4$ und dem quadratischen Reziprozitätsgesetz III.4.19

$$\left(\frac{5}{59}\right) = \left(\frac{59}{5}\right) = \left(\frac{4}{5}\right) = 1.$$

Insgesamt folgt

$$\left(\frac{59}{89}\right) = -1,$$

so dass die Kongruenz keine Lösung zulässt.

Primzahlen in arithmetischen Progressionen

Eine ungerade Primzahl p ist modulo 8 kongruent zu 1, 3, 5 oder 7. Wir wollen zeigen, dass jeder dieser Fälle unendlich oft auftritt:

III.4.22 Satz. *Jede der Folgen*

$$(8 \cdot k + 1)_{k\in\mathbb{N}}, \quad (8 \cdot k + 3)_{k\in\mathbb{N}}, \quad (8 \cdot k + 5)_{k\in\mathbb{N}} \quad \textit{und} \quad (8 \cdot k + 7)_{k\in\mathbb{N}}$$

enthält unendlich viele Folgenglieder, die Primzahlen sind.

Beweis. Die Folge $(8 \cdot k + 1)_{k\in\mathbb{N}}$ haben wir bereits in Beispiel III.2.5 behandelt. Daher können wir sie von unseren Betrachtungen ausschließen. Wir behalten die im genannten Beispiel verwendete Strategie bei und definieren zu einer gegebenen Schranke $M \in \mathbb{N}\setminus\{0\}$ die Zahl

$$u := \prod_{k=1}^{M}(2 \cdot k + 1).$$

Ferner setzen wir

$$N_3 := u^2 + 2, \quad N_5 := u^2 + 4 \quad \text{und} \quad N_7 := 8 \cdot u^2 - 1.$$

Offenbar haben wir

$$N_7 \equiv -1 \equiv 7 \bmod 8.$$

Weiter gilt

$$(2 \cdot k + 1)^2 = 4 \cdot k^2 + 4 \cdot k + 1 = 4 \cdot k \cdot (k + 1) + 1 \equiv 1 \bmod 8$$

für jede ganze Zahl $k \in \mathbb{Z}$. Wir schließen

$$N_3 \equiv 3 \bmod 8 \quad \text{und} \quad N_5 \equiv 5 \bmod 8.$$

Für jede Primzahl p mit $3 \le p \le 2 \cdot M + 1$ gilt $p|u$ und deswegen $p \nmid N_i$, $i = 3, 5, 7$. Unser Satz reduziert sich somit auf folgende Aussage:

Behauptung. *Sei $i \in \{3,5,7\}$. Dann gibt es eine Primzahl q, so dass*

$$q|N_i \quad \wedge \quad q \equiv i \bmod 8.$$

Fall 1. i=3. Für eine Primzahl q, die N_3 teilt, haben wir

$$u^2 \equiv -2 \bmod q.$$

Es folgt

$$\left(\frac{-1}{q}\right) \cdot \left(\frac{2}{q}\right) = \left(\frac{-2}{q}\right) = 1.$$

Mit Hilfe von Folgerung III.4.8, i), und Satz III.4.18 erkennen wir

$$q \equiv 1 \bmod 8 \quad \vee \quad q \equiv 3 \bmod 8.$$

Nun gilt aber auch:

$$(\forall p \text{ Primzahl}: \quad p|N_3 \Longrightarrow p \equiv 1 \bmod 8) \quad \Longrightarrow \quad (N_3 \equiv 1 \bmod 8).$$

Da wir aber N_3 so gewählt haben, dass $N_3 \equiv 3 \bmod 8$, muss es eine Primzahl q geben, die N_3 teilt und kongruent zu 3 modulo 8 ist.

Fall 2. i=5. Für eine Primzahl q mit $q|N_5$ folgt $u^2 \equiv -4 \bmod q$ und daher

$$\left(\frac{-1}{q}\right) = \left(\frac{-4}{q}\right) = 1.$$

Gemäß Folgerung III.4.8, i), muss $q \equiv 1 \bmod 4$ erfüllt sein, d.h.

$$q \equiv 1 \bmod 8 \quad \vee \quad q \equiv 5 \bmod 8.$$

Wie in Fall 1 schließen wir auf die Existenz einer Primzahl q, die N_5 teilt und kongruent 5 modulo 8 ist.

Fall 3. i=7. In diesem Fall gilt für eine Primzahl q, die N_7 teilt, dass

$$(4 \cdot u)^2 \equiv 2 \bmod q$$

und

$$\left(\frac{2}{q}\right) = 1.$$

Satz III.4.18 impliziert

$$q \equiv 1 \bmod 8 \quad \vee \quad q \equiv 7 \bmod 8.$$

Dieselben Argumente wie in den vorangegangenen Fällen führen zum Schluss, dass es eine Primzahl q mit $q|N_7$ und $q \equiv 7 \bmod 8$ geben muss. Die Behauptung und der Satz sind jetzt gezeigt. □

III.4.23 Aufgabe. a) Berechnen Sie die folgenden Legendre-Symbole:

$$\left(\frac{53}{311}\right), \quad \left(\frac{563}{1231}\right), \quad \left(\frac{2333}{3673}\right).$$

b) Ist die Kongruenz

$$x^2 \equiv 160 \bmod 51$$

lösbar? (Beachten Sie, dass $51 = 3 \cdot 17$ **keine Primzahl** ist.)

III.4.24 Aufgabe. a) Für welche Primzahlen p gilt

$$\left(\frac{3}{p}\right) = 1 \quad \text{bzw.} \quad \left(\frac{3}{p}\right) = -1?$$

b) Beweisen Sie mit den Ergebnissen aus a), dass für jede Primzahl $p \geq 7$

$$\left(\frac{6}{p}\right) = 1 \quad \Longleftrightarrow \quad \exists k \in \{1, 5, 19, 23\} : \; p \equiv k \bmod 24$$

gilt.

III.4.25 Aufgabe. a) Für $n \geq 1$ sei $P(n) := 20 \cdot n^2 - 1$. Zeigen Sie:

$$\forall n \geq 1 \forall p \text{ Primzahl} : \quad p | P(n) \quad \Longrightarrow \quad p \equiv \pm 1 \bmod 5.$$

b) Folgern Sie, dass es unendlich viele Primzahlen gibt, die kongruent 4 modulo 5 sind.

IV

Konstruktionen mit Zirkel und Lineal: Ein erster Einblick in die Galoistheorie

Untersucht man eine quadratische Gleichung

$$a \cdot x^2 + b \cdot x + c = 0, \quad a \in \mathbb{R}^\star,\ b \in \mathbb{R},$$

über den reellen Zahlen, dann entscheidet die Diskriminante

$$\Delta = b^2 - 4 \cdot a \cdot c$$

darüber, ob die Gleichung lösbar ist oder nicht. Ist Δ negativ, dann gibt es keine reelle Lösung. Die Lösungsformel

$$\alpha_{1/2} = \frac{-b \pm \sqrt{b^2 - 4 \cdot a \cdot c}}{2 \cdot a}$$

beschreibt **immer** die Lösungen im Körper $\mathbb{C}$ der komplexen Zahlen. Bekanntlich ist der Körper $\mathbb{C}$ **algebraisch abgeschlossen** ([5], Abschnitt 1.3.9). Zu jedem $n \geq 1$ und jedem Polynom

$$f(x) = a_0 + a_1 \cdot x + \cdots + a_n \cdot x^n, \quad a_0, ..., a_{n-1} \in \mathbb{C},\ a_n \in \mathbb{C}^\star,$$

vom Grad n existieren komplexe Zahlen $\alpha_1, ..., \alpha_n$ mit

$$f(x) = a_n \cdot (x - \alpha_1) \cdot \cdots \cdot (x - \alpha_n).$$

Das ist eine sehr wertvolle Eigenschaft. Möchte man allerdings ein Polynom f mit Koeffizienten in $\mathbb{Q}$ studieren, dann hat der Körper $\mathbb{C}$ gewisse Nachteile. Er ist viel zu groß: Neben den Nullstellen von f enthält er noch viele andere „unnötige“ Zahlen, er ist als $\mathbb{Q}$-Vektorraum unendlichdimensional. Zudem hängt er nicht von f ab und birgt damit keine Informationen zur konkreten Gleichung $f = 0$ in sich. Statt mit $\mathbb{C}$ kann man allerdings mit dem **Teilkörper**

$$\mathbb{Q}(\alpha_1, ..., \alpha_n) \subset \mathbb{C}$$

arbeiten. Dies ist der **kleinste** Teilkörper von $\mathbb{C}$, der alle Nullstellen von f enthält. Als $\mathbb{Q}$-Vektorraum ist er endlichdimensional. Für $f = x^2 + 1$ erhält man auf diese Weise den Teilkörper

$$\mathbb{Q}(i) = \mathbb{Q} \oplus \mathbb{Q} \cdot i \subset \mathbb{C}.$$

Das Studium der Gleichung f kann als Studium der Körpererweiterung $\mathbb{Q} \subset K$, $K := \mathbb{Q}(\alpha_1, ..., \alpha_n)$, durchgeführt werden. Gemäß eines in Kapitel II formulierten Prinzips hat jedes mathematische Objekt eine Symmetriegruppe. Die Symmetriegruppe der Körpererweiterung $\mathbb{Q} \subset K$ ist ihre **Galois-Gruppe**[1] $\mathrm{Gal}_{\mathbb{Q}}(K)$. Über die Galois-Gruppe stehen die Hilfsmittel der Gruppentheorie bei der Untersuchung algebraischer Gleichungen zur Verfügung, und damit lassen sich sehr interessante Resultate gewinnen.

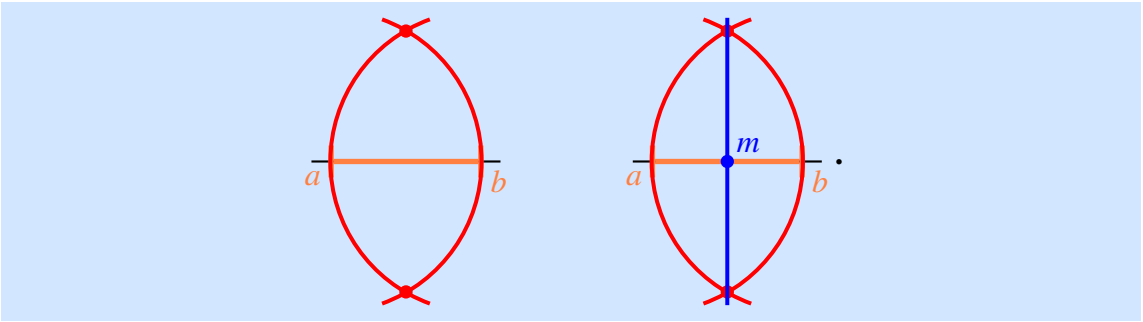
In diesem Kapitel werden wir diese Ideen am Beispiel der Gleichung

$$x^n - 1 = 0, \quad n \geq 3,$$

entwickeln. Die Ergebnisse zu dieser Gleichung geben auch Auskunft zu der Frage, ob sich das regelmäßige n-Eck mit Zirkel und Lineal konstruieren lässt. Konstruktionsprobleme mit Zirkel und Lineal wurden schon in der Antike betrachtet. Jedem Leser und jeder Leserin ist zudem die Konstruktion der Mittelsenkrechten mit Zirkel und Lineal im Gedächtnis. Daher beginnen wir dieses Kapitel mit einer Diskussion dieser Themen und ihrer Formulierung im Rahmen der Körpertheorie. Mit Hilfe dieser Formulierung lassen sich einige klassische Fragen zu Konstruktionsproblemen schnell negativ beantworten. Vorlagen für dieses Kapitel sind [12] und [22].

IV.1 Konstruktionen mit Zirkel und Lineal

Aus der Schule ist bekannt, wie man den Mittelpunkt einer gegebenen Strecke mit Zirkel und Lineal konstruieren kann:

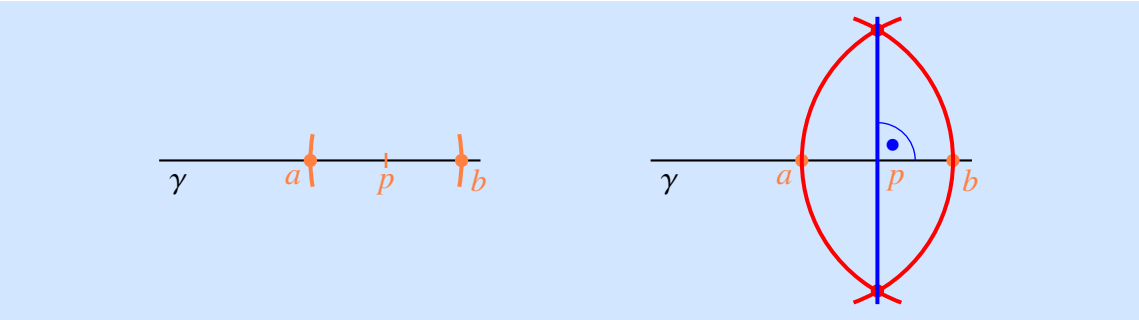


Die im zweiten Bild benutze Hilfsgerade ist die **Mittelsenkrechte** der Strecke.

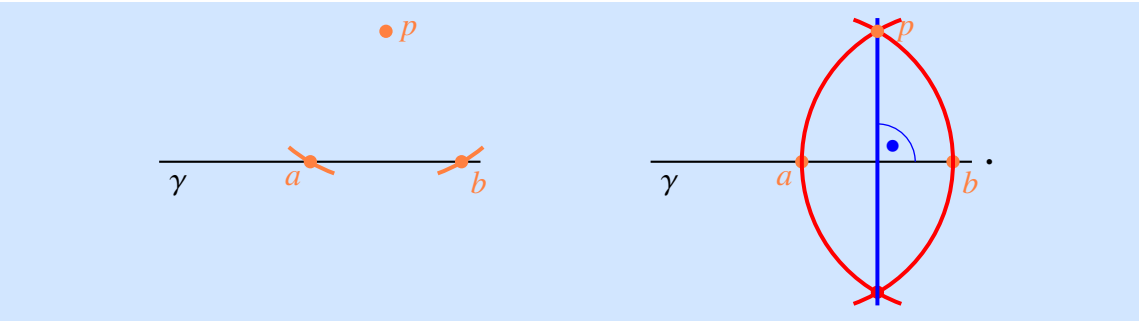
Um Konstruktionsprobleme zu formalisieren, legen wir fest, dass unsere Punkte in der „Zeichenebene“ $\mathbb{R}^2$ leben, die wir mit dem komplexen Zahlkörper $\mathbb{C}$ identifizieren.

Mit der Konstruktion der Mittelsenkrechten lässt sich das Lot auf eine Gerade $\gamma \subset \mathbb{C}$ in einem Punkt $p \in \gamma$ errichten

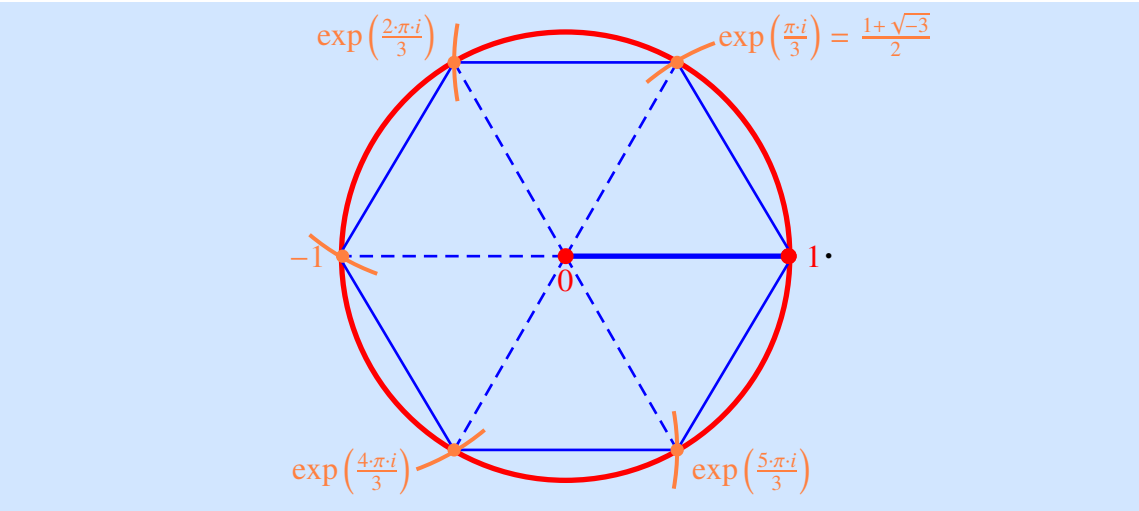
[1] Évariste Galois (1811 - 1832), französischer Mathematiker.



oder von einem Punkt $p \in \mathbb{C} \setminus \gamma$ aus fällen:



Ein regelmäßiges Sechseck lässt sich auf folgende Weise mit Zirkel und Lineal konstruieren:



In Abschnitt IV.4 werden wir die Frage aufgreifen, für welche Werte von $n \geq 3$ sich das regelmäßige n-Eck mit Zirkel und Lineal konstruieren lässt.

IV.1.1 Aufgabe. Erklären Sie, wie man ein regelmäßiges Fünfeck mit Zirkel und Lineal konstruiert.

Die Konstruktionsschritte nach Euklid

IV.1.2 Definitionen. Gegeben sei eine Teilmenge $M \subset \mathbb{C}$ mit $\{0, 1\} \subset M$.

i) Wir setzen

$$\begin{aligned} G(M) &:= \{\gamma \subset \mathbb{C} \mid \gamma \text{ ist Gerade durch zwei Punkte in } M\}, \\ R(M) &:= \{r \in \mathbb{R}_{>0} \mid \text{es gibt Punkte } z_1, z_2 \text{ in } M \text{ mit } r = |z_1 - z_2|\}, \\ K(M) &:= \{\varkappa \subset \mathbb{C} \mid \varkappa \text{ ist ein Kreis mit Mittelpunkt in } M \text{ und Radius in } R(M)\}. \end{aligned}$$

ii) Die Mengen M', M'' und M''' werden durch folgende Vorschriften festgelegt:

$$z \in M' \quad :\Longleftrightarrow \quad \exists \gamma_1, \gamma_2 \in G(M) : \ \gamma_1 \neq \gamma_2 \wedge \{z\} = \gamma_1 \cap \gamma_2$$

(Durchschnitt zweier Geraden);

$$z \in M'' \quad :\Longleftrightarrow \quad \exists \gamma \in G(M), \varkappa \in K(M) : \ z \in \gamma \cap \varkappa$$

(Durchschnitt einer Geraden und eines Kreises);

$$z \in M''' \quad :\Longleftrightarrow \quad \exists \varkappa_1, \varkappa_2 \in K(M) : \ \varkappa_1 \neq \varkappa_2 \wedge z \in \varkappa_1 \cap \varkappa_2$$

(Durchschnitt zweier Kreise).

iii) Die Teilmengen $M_k \subset \mathbb{C}$, $k \in \mathbb{N}$, werden rekursiv durch

- $M_0 := M$,
- $M_{k+1} := M_k \cup M_k' \cup M_k'' \cup M_k'''$, $k \in \mathbb{N}$,

eingeführt. Schließlich sei

$$M_\infty := \bigcup_{k=0}^{\infty} M_k$$

die *Menge der aus M (mit Zirkel und Lineal) konstruierbaren Punkte*.

Die Konstruierbarkeit eines Punkts lässt sich algebraisch untersuchen. Die Gerade $\gamma \subset \mathbb{C}$, die durch die Punkte $z_1, z_2 \in \mathbb{C}$ verläuft, ist von der Form

$$\gamma = \{z = z_1 + \lambda \cdot (z_2 - z_1) \mid \lambda \in \mathbb{R}\}.$$

Der Kreis mit Mittelpunkt $z_1 \in \mathbb{C}$ und Radius $|z_2 - z_3|$, $z_2, z_3 \in \mathbb{C}$, hat die Gleichung

$$(z - z_1) \cdot (\overline{z} - \overline{z}_1) = (z_2 - z_3) \cdot (\overline{z}_2 - \overline{z}_3).$$

Die Koordinaten eines Punkts in M', M'' bzw. M''' erfüllen polynomiale Gleichungen, deren Koeffizienten die Koordinaten von geeigneten Punkten aus M sind. Die Theorie der polynomialen Gleichungen in einer Variablen über einem Körper k ist die Theorie der Erweiterungskörper von k, mit deren Entwicklung wir im folgenden Abschnitt beginnen werden. Es wird sich ein Kriterium für die Konstruierbarkeit eines Punkts $z \in \mathbb{C}$ aus einer Menge M ergeben (Satz IV.3.4), mit dem wir beweisen können, dass sich die folgenden drei Konstruktionsprobleme der Antike im Allgemeinen nicht lösen lassen.

IV.1.3 Beispiel (Die Konstruktionsprobleme der Antike). i) **Das delische Problem.** Aus 0, 1 und der Kantenlänge ℓ eines Würfels W ist die Kantenlänge ℓ' eines Würfels W' mit doppeltem Volumen zu konstruieren:

$$\ell'^3 = \mathrm{Vol}(W') = 2 \cdot \mathrm{Vol}(W) = 2 \cdot \ell^3.$$

Das Problem lässt sich auf den Fall $\ell = 1$ reduzieren. Hier gilt $M = \{0, 1\}$, und es ist zu klären, ob sich $\sqrt[3]{2}$ aus M mit Zirkel und Lineal konstruieren lässt.

ii) **Winkeldreiteilung.** Ist es möglich, die Dreiteilung eines beliebigen Winkels $\alpha \in (0, 2\pi]$ mit Zirkel und Lineal durchzuführen? Dazu seien

$$\zeta := \exp(i \cdot \alpha) \quad \text{und} \quad \xi := \exp\left(i \cdot \frac{\alpha}{3}\right).$$

Die Frage lautet, ob ξ aus der Menge $M := \{0, 1, \zeta\}$ konstruierbar ist.

iii) **Die Quadratur des Kreises.** Aus 0, 1 und der positiven reellen Zahl r ist die Seitenlänge ℓ eines Quadrats Q zu konstruieren, das denselben Fächeninhalt wie ein Kreis[2] K vom Radius r hat:

$$\ell^2 = \mathrm{Fl}(Q) = \mathrm{Fl}(K) = \pi \cdot r^2.$$

Wieder genügt es, den Fall $r = 1$, d.h. $M = \{0, 1\}$, zu betrachten. Es ist folglich zu klären, ob π aus M konstruierbar ist.

IV.1.4 Bemerkung. Setzen wir in Definition IV.1.2 voraus, dass M ein Körper ist, dann gilt

$$K(M) = \{\varkappa \subset \mathbb{C} \mid \varkappa \text{ ist ein Kreis mit Mittelpunkt in } M \text{ und enthält einen Punkt aus } M\}.$$

IV.2 Erweiterungen des Körpers der rationalen Zahlen

IV.2.1 Definition. Es sei K ein Körper. Eine Teilmenge $k \subset K$ ist ein *Teilkörper*, wenn gilt

- ⋆ k ist eine Untergruppe von $(K, +)$,
- ⋆ $k \setminus \{0\}$ ist eine Untergruppe von $(K^\star, \cdot)$.

IV.2.2 Beispiel. i) Der Körper $\mathbb{R}$ der reellen Zahlen ist ein Teilkörper des Körpers $\mathbb{C}$ der komplexen Zahlen.

ii) Der Körper $\mathbb{Q}$ der rationalen Zahlen ist ein Teilkörper des Körpers $\mathbb{R}$ der reellen Zahlen und des Körpers $\mathbb{C}$ der komplexen Zahlen.

IV.2.3 Bemerkung. i) Es seien K ein Körper und $k \subset K$ ein Teilkörper. Dann gilt:

- ⋆ $0, 1 \in k$.
- ⋆ Da k eine Untergruppe von $(K, +)$ ist, haben wir die Addition

$$\begin{aligned} +\colon k \times k &\longrightarrow k \\ (a, b) &\longmapsto a + b. \end{aligned}$$

[2] Für die mathematisch exakte Berechnung des Flächeninhalts einer Kreisscheibe s. [18], Beispiel 3.3.5, i).

- ⋆ Für $a, b \in k$ gilt auch $a \cdot b \in k$. Falls $a \neq 0$ und $b \neq 0$, dann folgt das aus der Tatsache, dass $k \setminus \{0\}$ eine Untergruppe von $K^\star$ ist. Wenn $a = 0$ oder $b = 0$, dann gilt nach Bemerkung III.1.2, i), $a \cdot b = 0 \in k$. Somit haben wir auch eine Multiplikation

$$\begin{aligned} \cdot \colon k \times k &\longrightarrow k \\ (a, b) &\longmapsto a \cdot b. \end{aligned}$$

Man überprüft leicht, dass $(k, 0, 1, +, \cdot)$ ein Körper ist. Deshalb wird die Inklusion $k \subset K$ auch eine *Körpererweiterung* von k genannt.

ii) Jeder Teilkörper $k \subset \mathbb{C}$ enthält den Körper $\mathbb{Q}$ der rationalen Zahlen. Das sieht man folgendermaßen ein:

- ⋆ Da $1 \in k$ und $(k, +)$ eine Untergruppe von $(\mathbb{C}, +)$ ist, enthält k auch $\langle 1 \rangle = \mathbb{Z}$.
- ⋆ Für $l \in \mathbb{Z} \setminus \{0\}$ folgt $l^{-1} = 1/l \in k$, weil $(k^\star, \cdot)$ eine Untergruppe von $(\mathbb{C}^\star, \cdot)$ ist.
- ⋆ Für $a/b \in \mathbb{Q}$ gilt folglich

$$\frac{a}{b} = a \cdot \frac{1}{b} \in k.$$

IV.2.4 Satz. *Es seien L ein Körper und $A \subset L$ eine Teilmenge. Dann gibt es genau einen Teilkörper $K \subset L$, so dass gilt:*

- ⋆ $A \subset K$.
- ⋆ *Für jeden Teilkörper K' von L mit $A \subset K'$ gilt $K \subset K'$.*

Beweis. Wir setzen

$$\mathcal{K} := \{\, K' \subset L \mid K' \text{ ist Teilkörper von } L \text{ und } A \subset K' \,\}.$$

Wegen $L \in \mathcal{K}$ ist die Menge $\mathcal{K}$ nichtleer. Daher können wir

$$K := \bigcap_{K' \in \mathcal{K}} K'$$

definieren. Die Eigenschaften von K überprüft man wie in der Gruppentheorie (Satz II.4.10). □

IV.2.5 Beispiel. Wir können die obige Konstruktion auf $\varnothing$ anwenden. Das Ergebnis k wird der *Primkörper* von L genannt. Man erhält ebenfalls k, wenn man die Konstruktion für $A = \{\, 0, 1 \,\}$ durchführt. Nach Beispiel IV.2.3, ii), ist der Primkörper von $\mathbb{C}$ der Körper $\mathbb{Q}$ der rationalen Zahlen.

IV.2.6 Definition. Wir nennen K den *von A erzeugten Teilkörper* von L.
Schreibweise. $k(A) := K$, k der Primkörper von L. Gilt $A = \{\alpha_1, ..., \alpha_n\}$, dann setzen wir $k(\alpha_1, ..., \alpha_n) := k(\{\alpha_1, ..., \alpha_n\})$. Für einen Teilkörper $K \subset L$, $A \subset L$ und $B := K \cup A$ sei $K(A) := k(B)$.

Wenn $k \subset K$ eine Körpererweiterung ist, dann erhält K die Struktur eines k-Vektorraums.

IV.2.7 Definitionen. Es sei $k \subset K$ eine Körpererweiterung.

i) Die Zahl

$$[K : k] := \mathrm{Dim}_k(K) \in \{\, n \in \mathbb{N} \mid n \geq 1 \,\} \cup \{\infty\}$$

ist der *Grad* der Körpererweiterung.

ii) Die Körpererweiterung ist *endlich*, wenn $[K : k] < \infty$.

IV.2.8 Aufgabe. Es sei $k \subset K \subset L$ ein Turm von Körpererweiterungen, so dass $k \subset L$ endlich ist. Zeigen Sie

$$[L : k] = [L : K] \cdot [K : k].$$

Algebraische Elemente und ihre Minimalpolynome

IV.2.9 Satz. *Es seien $k \subset K$ eine Körpererweiterung und $\alpha \in K$. Dann sind die folgenden Behauptungen äquivalent:*

i) *Der Teilkörper $k(\alpha) \subset K$ ist ein endlichdimensionaler k-Vektorraum.*

ii) *Es gibt ein Polynom $f \in k[x] \setminus \{0\}$ mit $f(\alpha) = 0$.*

Beweis. „i)$\Longrightarrow$ii)“. Es sei $n := \mathrm{Dim}_k(k(\alpha))$. Die Vektoren $1, \alpha, ..., \alpha^n$ sind dann linear abhängig. Deshalb existieren Elemente $a_0, ..., a_n \in k$, nicht alle null, mit

$$a_0 \cdot 1 + a_1 \cdot \alpha + \cdots + a_n \cdot \alpha^n = 0.$$

Damit ist Behauptung ii) für das Polynom

$$f := a_0 + a_1 \cdot x + \cdots + a_n \cdot x^n \in k[x]$$

erfüllt.

„ii)$\Longrightarrow$i)“. Wir definieren

$$n := \min\{\, l \geq 1 \mid \exists f \in k[x] :\ \mathrm{Grad}(f) = l \wedge f(\alpha) = 0 \,\} - 1.$$

Dann sind die Vektoren $1, \alpha, ..., \alpha^n$ linear unabhängig über k, und

$$K' := \bigoplus_{i=0}^{n} k \cdot \alpha^i$$

sei der von diesen Vektoren aufgespannte k-Untervektorraum von K.

IV.2.10 Bemerkung. Es gilt $K' \subset k(\alpha)$.

Behauptung. *Bei K' handelt es sich um einen Teilkörper von K.*

Als k-Untervektorraum ist K' insbesondere eine Untergruppe von $(K, +)$. Es bleibt zu überprüfen, dass $(K' \setminus \{0\}, \cdot)$ eine Untergruppe von $(K^\star, \cdot)$ ist.

Zunächst gilt offensichtlich $1 \in K' \setminus \{0\}$. Durch Induktion über l zeigen wir weiter, dass

$$\forall l \in \mathbb{N} : \quad \alpha^l \in K'.$$

Für $l \leq n$ gilt das nach Konstruktion. Nun schließen wir von l auf $l+1$, $l \geq n$. Dazu fixieren wir ein Polynom $f = a_0 + a_1 \cdot x + \cdots + a_{n+1} \cdot x^{n+1} \in k[x]$ vom Grad $n+1$ mit $f(\alpha) = 0$. Wir schreiben

$$\begin{aligned} \alpha^{l+1} &= \alpha^{n+1} \cdot \alpha^{l-n} \\ &= -\frac{1}{a_{n+1}} \cdot (a_0 + a_1 \cdot \alpha + \cdots + a_n \cdot \alpha^n) \cdot \alpha^{l-n} \\ &= -\frac{1}{a_{n+1}} \cdot (a_0 \cdot \alpha^{l-n} + a_1 \cdot \alpha^{l-n+1} + \cdots + a_n \cdot \alpha^l). \end{aligned}$$

Nach Induktionsvoraussetzung liegen α^{l-n}, ..., α^l in K'. Da K' ein k-Untervektorraum von K ist, folgt aus der letzten Beschreibung des Elements α^{l+1}, dass es ebenfalls in K' liegt.

Man sieht nun leicht:

$$\forall a, b \in K' : \quad a \cdot b \in K'.$$

Schließlich zeigen wir, dass zu jedem Element $\beta = a_0 + a_1 \cdot \alpha + \cdots + a_n \cdot \alpha^n \in K' \setminus \{0\}$ auch das inverse Element β^{-1} in K' liegt. Zu diesem Zweck halten wir fest, dass es Elemente b_0, ..., $b_{n+1} \in k$ mit

$$b_0 + b_1 \cdot \beta + \cdots + b_{n+1} \cdot \beta^{n+1} = 0$$

gibt, denn K' hat als k-Vektorraum die Dimension $n+1$. Dabei können wir ohne Beschränkung der Allgemeinheit $b_0 = -1$ annehmen. Es folgt,

$$\beta^{-1} = b_1 + b_2 \cdot \beta + \cdots + b_{n+1} \cdot \beta^n \in K',$$

so dass K' wirklich ein Teilkörper von K ist. √

Aus $\alpha \in K'$ und $k \subset K'$ folgt nach Satz IV.2.4, dass $k(\alpha) \subset K'$. Mit Bemerkung IV.2.10 ist nun $k(\alpha) = K'$ und $\mathrm{Dim}_k(k(\alpha)) = \mathrm{Dim}_k(K') = n+1 < \infty$ gezeigt. □

IV.2.11 Definitionen. i) Es sei $k \subset K$ eine Körpererweiterung. Ein Element $\alpha \in K$ mit

$$\mathrm{Dim}_k(k(\alpha)) < \infty$$

ist *algebraisch* über k.

ii) Es seien R ein Ring und $f = a_0 + a_1 \cdot x + \cdots + a_n \cdot x^n \in R[x]$ ein Polynom vom Grad n. Das Polynom f ist *normiert*, wenn $a_n = 1$ gilt.

IV.2.12 Satz. *Es seien $k \subset K$ eine Körpererweiterung und $\alpha \in K$ ein über k algebraisches Element. Dann existiert genau ein **normiertes** Polynom $\mu_\alpha \in k[x]$ für das*

- ⋆ $\mu_\alpha(\alpha) = 0$,
- ⋆ $\forall f \in k[x] : f(\alpha) = 0 \Longrightarrow \mu_\alpha | f$

gilt.

Beweis. **Eindeutigkeit.** Es seien μ_α und μ'_α zwei Polynome in $k[x]$ mit den angegebenen Eigenschaften. Dann gilt $\mu_\alpha | \mu'_\alpha$ und $\mu'_\alpha | \mu_\alpha$. Nach Lemma A.1.3, ii), haben wir $\mathrm{Grad}(\mu_\alpha) = \mathrm{Grad}(\mu'_\alpha)$, und es gibt ein Element $\lambda \in k^\star$ mit $\mu_\alpha = \lambda \cdot \mu'_\alpha$. Da sowohl μ_α als auch μ'_α normiert ist, gilt $\lambda = 1$ und $\mu_\alpha = \mu'_\alpha$.

Existenz. Sei

$$n := \min\{\, l \geq 1 \mid \exists f \in k[x] :\ \mathrm{Grad}(f) = l \wedge f(\alpha) = 0 \,\}.$$

Es gibt dann Elemente $a_0, ..., a_{n-1} \in k$, so dass

$$\mu_\alpha(\alpha) = 0, \quad \mu_\alpha = a_0 + a_1 \cdot x + \cdots + a_{n-1} \cdot x^{n-1} + x^n.$$

Für ein Polynom $f \in k[x]$ mit $f(\alpha) = 0$ gilt $f = 0$ oder $\mathrm{Grad}(f) \geq \mathrm{Grad}(\mu_\alpha)$. Es gibt nach Satz A.1.5 Polynome $q, r \in k[x]$ mit

$$f = q \cdot \mu_\alpha + r, \quad \mathrm{Grad}(r) < \mathrm{Grad}(\mu_\alpha).$$

Dabei gilt

$$r(\alpha) = f(\alpha) - q(\alpha) \cdot \mu_\alpha(\alpha) = 0.$$

Aus der Definition von n folgt, dass r das Nullpolynom ist. Deshalb gilt $\mu_\alpha | f$. □

IV.2.13 Bemerkung. In der Situation des Satzes gilt

$$\mathrm{Grad}(\mu_\alpha) = [k(\alpha) : k].$$

IV.2.14 Definition. Es seien $k \subset K$ eine Körpererweiterung und $\alpha \in K$ ein Element, das über k algebraisch ist. Dann heißt das Polynom μ_α aus Satz IV.2.12 das *Minimalpolynom* von α über k.

IV.2.15 Bemerkung. Das Element $\alpha \in K$ definiert die k-lineare Abbildung

$$\begin{array}{rcl} L_\alpha : K & \longrightarrow & K \\ v & \longmapsto & \alpha \cdot v. \end{array}$$

Das Minimalpolynom μ_α stimmt mit dem Minimalpolynom der k-linearen Abbildung L_α überein, das in der Linearen Algebra untersucht wird ([20], §36; [5], Abschnit 4.5.5).

IV.2.16 Aufgabe. a) Bestimmen Sie das Minimalpolynom von $\sqrt{7} + 1$ über $\mathbb{Q}$ und geben Sie den Grad der Körpererweiterung $\mathbb{Q} \subset \mathbb{Q}(\sqrt{7} + 1)$ an.

b) Es sei $L := \mathbb{Q}(\sqrt[4]{2}, i)$. Berechnen Sie $[L : \mathbb{Q}]$. Betrachten Sie dazu die Körpererweiterungen $\mathbb{Q} \subset \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(\sqrt[4]{2})(i) = L$.

Die Galois-Gruppe einer Körpererweiterung

IV.2.17 Definition. Es sei $k \subset K$ eine Körpererweiterung: Die Gruppe

$$\mathrm{Gal}_k(K) := \{\, \varphi : K \longrightarrow K \mid \varphi \text{ ist Körperautomorphismus, so dass } \forall a \in k : \varphi(a) = a \,\}$$

ist die *Galois-Gruppe* der Körpererweiterung.

IV.2.18 Bemerkung. Es sei $\mathbb{Q} \subset K$ eine Erweiterung des Körpers der rationalen Zahlen. Dann gilt

$$\forall v \in \mathbb{Q} : \quad \varphi(v) = v$$

für jeden Körperautomorphismus $\varphi : K \longrightarrow K$.

Man hat $\varphi(0) = 0$ und $\varphi(1) = 1$. Es folgt $\varphi(n) = n$ für alle natürlichen Zahlen. Dies beweist man induktiv. Der Induktionsanfang ist bereits gemacht. Im Induktionsschritt berechnet man $\varphi(n+1) = \varphi(n) + \varphi(1) = n + 1$, $n \in \mathbb{N}$. Außerdem gilt $\varphi(-n) = -\varphi(n) = -n$, $n \in \mathbb{N}$. Somit ist $\varphi(k) = k$ für jede ganze Zahl $k \in \mathbb{Z}$ nachgewiesen. Für $k \in \mathbb{Z} \setminus \{0\}$ beobachten wir weiter

$$\varphi\left(\frac{1}{k}\right) = \frac{1}{\varphi(k)} = \frac{1}{k}.$$

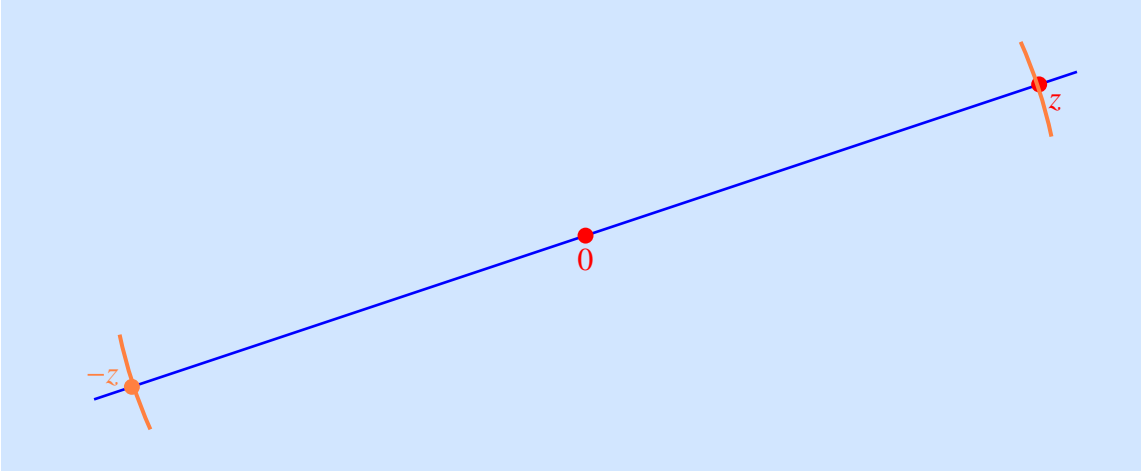
Damit schließen wir

$$\forall \frac{a}{b} \in \mathbb{Q}: \quad \varphi\left(\frac{a}{b}\right) = \varphi(a) \cdot \varphi\left(\frac{1}{b}\right) = a \cdot \frac{1}{b} = \frac{a}{b}.$$

IV.3 Mit Zirkel und Lineal konstruierbare Punkte

IV.3.1 Satz. *Es seien $M \subset \mathbb{C}$ eine Teilmenge, so dass $0 \in M$ und $1 \in M$. Dann ist die Teilmenge $M_\infty \subset \mathbb{C}$ aller aus M konstruierbaren Punkte ein Teilkörper.*

Beweis. **i) M_∞ ist eine Untergruppe von $(\mathbb{C}, +)$.** Auf Grund der Voraussetzungen an M gilt $0 \in M_\infty$. Weiter liegt zu jedem Punkt $z \in M_\infty$ auch $-z \in M_\infty$. Für $z = 0$ ist dazu nichts zu zeigen. Andernfalls zeichnen wir die Gerade γ durch z und 0. Sie schneidet den Kreis vom Radius $|z|$ in den Punkten z und $-z$.



Für zwei Punkte $z_1, z_2 \in M_\infty$ konstruiert man die Summe $z_1 + z_2$ auf folgende Weise mit Zirkel und Lineal: Es seien K_1 der Kreis vom Radius $|z_2|$ um z_1 und K_2 der Kreis vom Radius $|z_1|$ um z_2. Der Durchschnitt $K_1 \cap K_2$ enthält den Punkt $z_1 + z_2$ (s. Abbildung IV.1).

ii) $M_\infty \setminus \{0\}$ ist eine Untergruppe von $(\mathbb{C}^\star, \cdot)$. Wir haben $1 \in M_\infty$ nach Voraussetzung. Für die verbleibenden Argumente schreiben wir einen Punkt z in **Polarkoordinaten** (vgl. [16], Kapitel 4, Ausblick; [17], Beispiel 3.2.4, iv)

$$z = |z| \cdot \exp(i \cdot \arg(z)).$$

Dabei ist $\arg(z) \in [0, 2\pi)$ der Winkel, den z mit der x-Achse einschließt.

Nun sei $z \in M_\infty \setminus \{0\}$. Um zu zeigen, dass z^{-1} ebenfalls in $M_\infty \setminus \{0\}$ liegt, bemerken wir, dass $\arg(z)$ als einer der Schnittpunkte des Kreises vom Radius 1 um den Nullpunkt

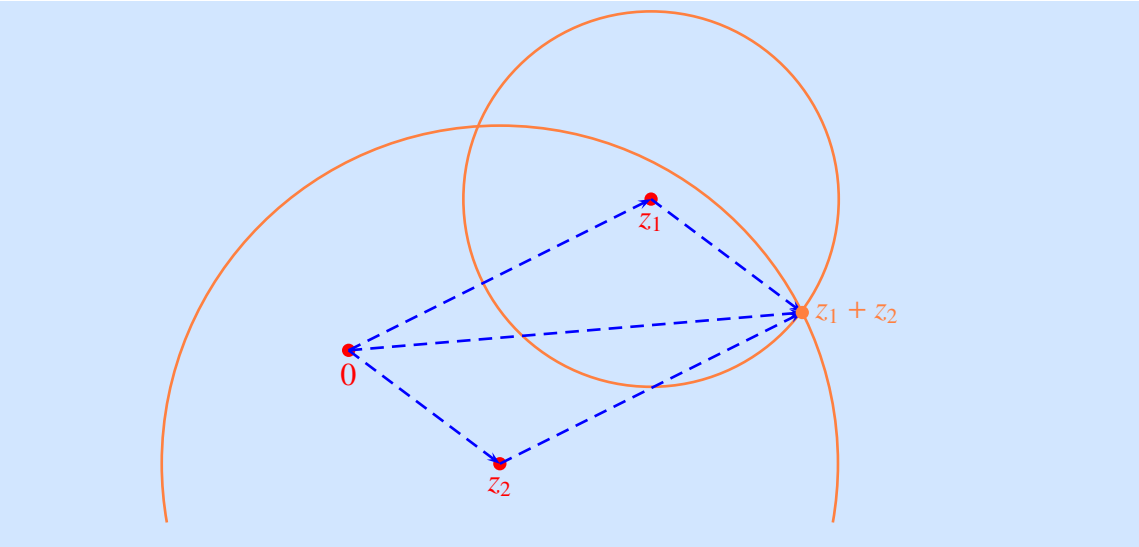


Abbildung IV.1: Die Addition zweier komplexer Zahlen mit Zirkel und Lineal

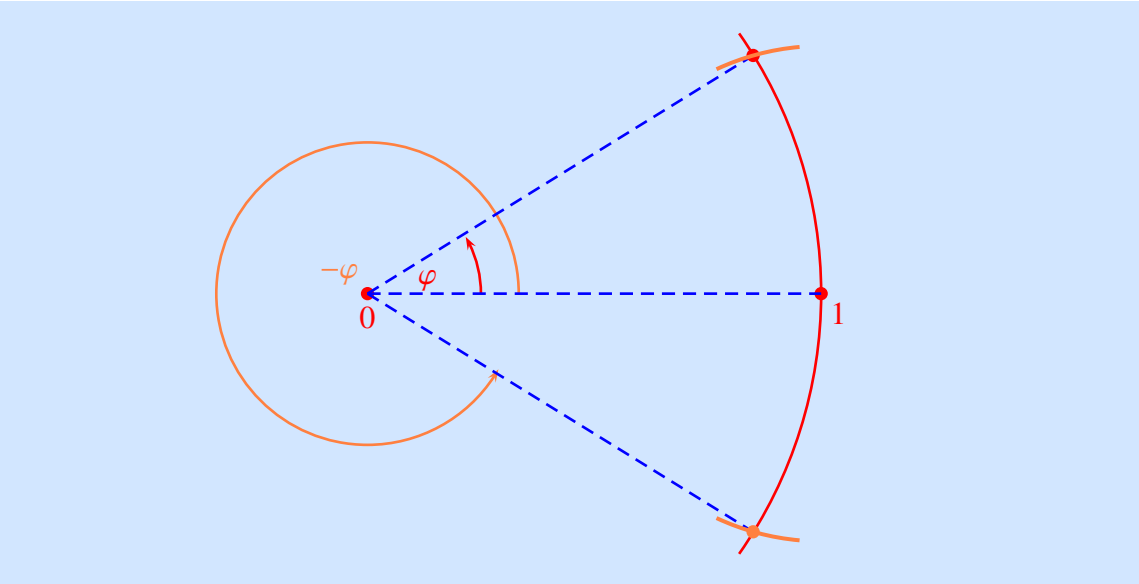
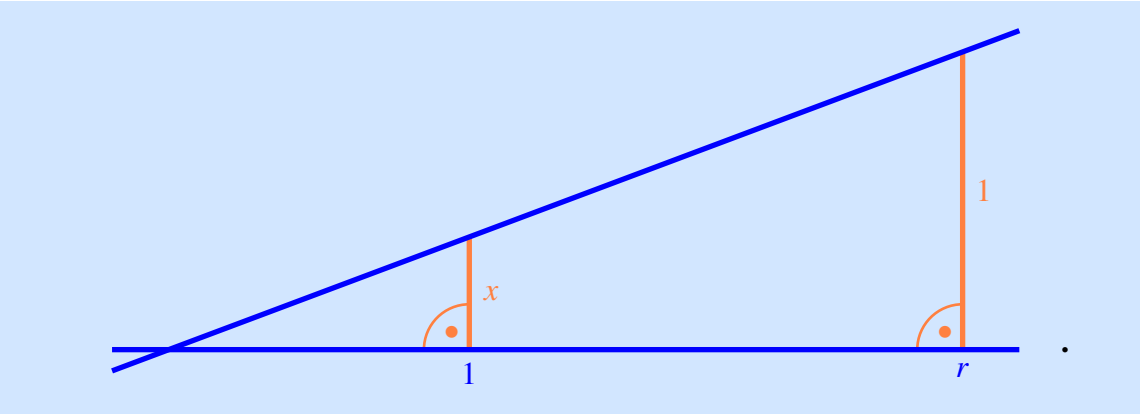


Abbildung IV.2: Konstruktion des Negativen eines Winkels

mit der Geraden durch 0 und z ebenfalls in M_∞ liegt. Der Kreis durch z um 0 schneidet die x-Achse in $|z|$ und $-|z|$. Auf Grund der Formel

$$z^{-1} = \frac{1}{|z|} \cdot \exp(-i \cdot \arg(z))$$

ist zu zeigen, dass wir $-\arg(z)$ und $1/|z|$ konstruieren können. Die Konstruktion des Winkels $-\varphi$ aus dem Winkel φ ist einfach (s. Abbildung IV.2). Mit der Konstruktion von Loten erkennt man, dass zu $r \in \mathbb{R}_{>0}$ folgendes Gebilde konstruierbar ist



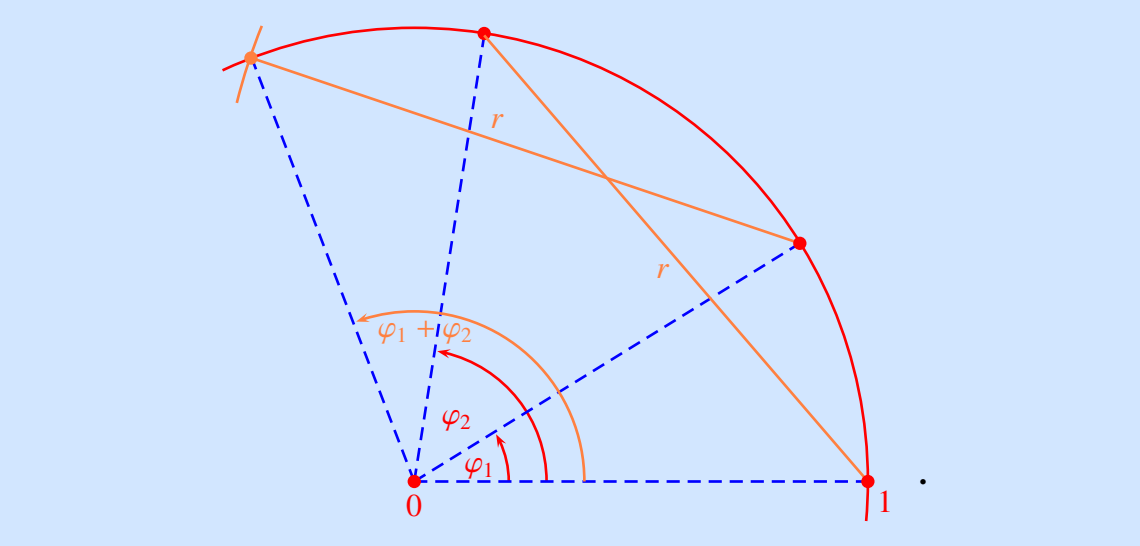
Der Strahlensatz ([19], Kapitel III, §11, Aufgabe 62; [1], Abschnitt 2.1.1) zeigt

$$x = \frac{1}{r}.$$

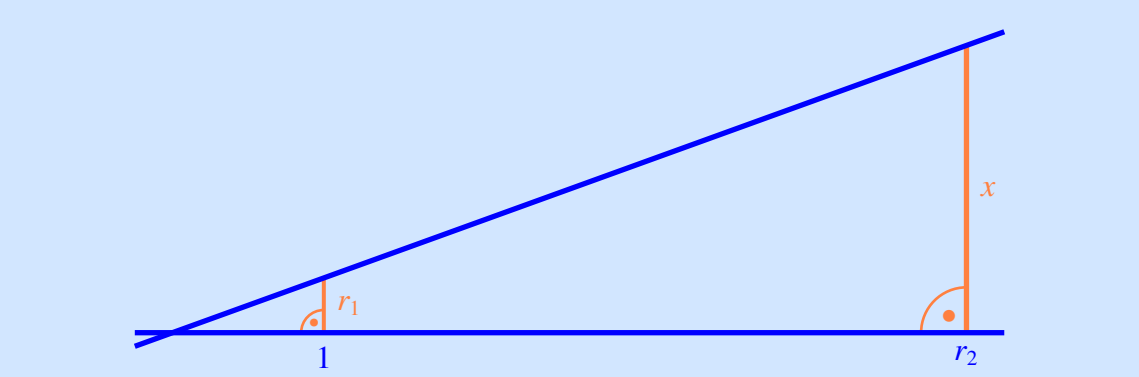
Nun seien $z_1, z_2 \in M_\infty \setminus \{0\}$. Das Produkt dieser komplexen Zahlen wird mit der Formel

$$z_1 \cdot z_2 = |z_1| \cdot |z_2| \cdot \exp\Big(i \cdot (\arg(z_1) + \arg(z_2))\Big)$$

berechnet. Für Winkel φ_1, φ_2 kann der Winkel $\varphi_1 + \varphi_2$ leicht konstruiert werden:



Um das Produkt zweier positiver reeller Zahlen r_1, r_2 zu konstruieren, bemühen wir die Konfiguration



und den Strahlensatz (loc. cit.), um

$$x = r_1 \cdot r_2$$

nachzuweisen. □

Aus den Argumenten im obigen Beweis leitet man auch folgende Aussage ab:

IV.3.2 Folgerung. *In der Situation des Satzes gilt:*

$$\forall z \in M_\infty : \quad \overline{z} \in M_\infty.$$

Kurz: $\overline{M}_\infty = M_\infty$.

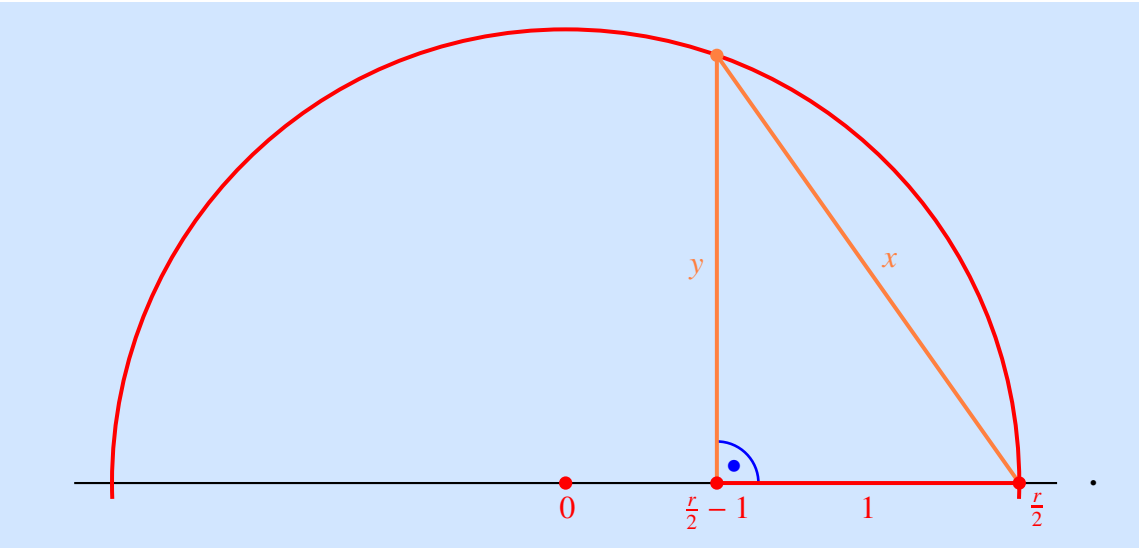
IV.3.3 Satz. *Es seien $M \subset \mathbb{C}$ eine Teilmenge, so dass $0 \in M$ und $1 \in M$. Für die Teilmenge $M_\infty \subset \mathbb{C}$ aller aus M konstruierbaren Punkte gilt:*

$$\forall z \in \mathbb{C} : \quad z \in M_\infty \quad \Longleftrightarrow \quad z^2 \in M_\infty.$$

Beweis. Die Implikation „$\Longrightarrow$“ ist gültig, weil M_∞ ein Teilkörper von $\mathbb{C}$ ist. Für „$\Longleftarrow$“ beachte man, dass

$$\forall z \in \mathbb{C} : \quad z = \pm \sqrt{|z|^2} \cdot \exp\left(\frac{i}{2} \cdot \arg(z^2)\right).$$

Mit Hilfe von Mittelsenkrechten kann man aus einem Winkel φ den halben Winkel $\varphi/2$ erzeugen (s. Abbildung IV.3). Es bleibt, die Wurzel aus einer positiven reellen Zahl zu konstruieren. Wir bilden



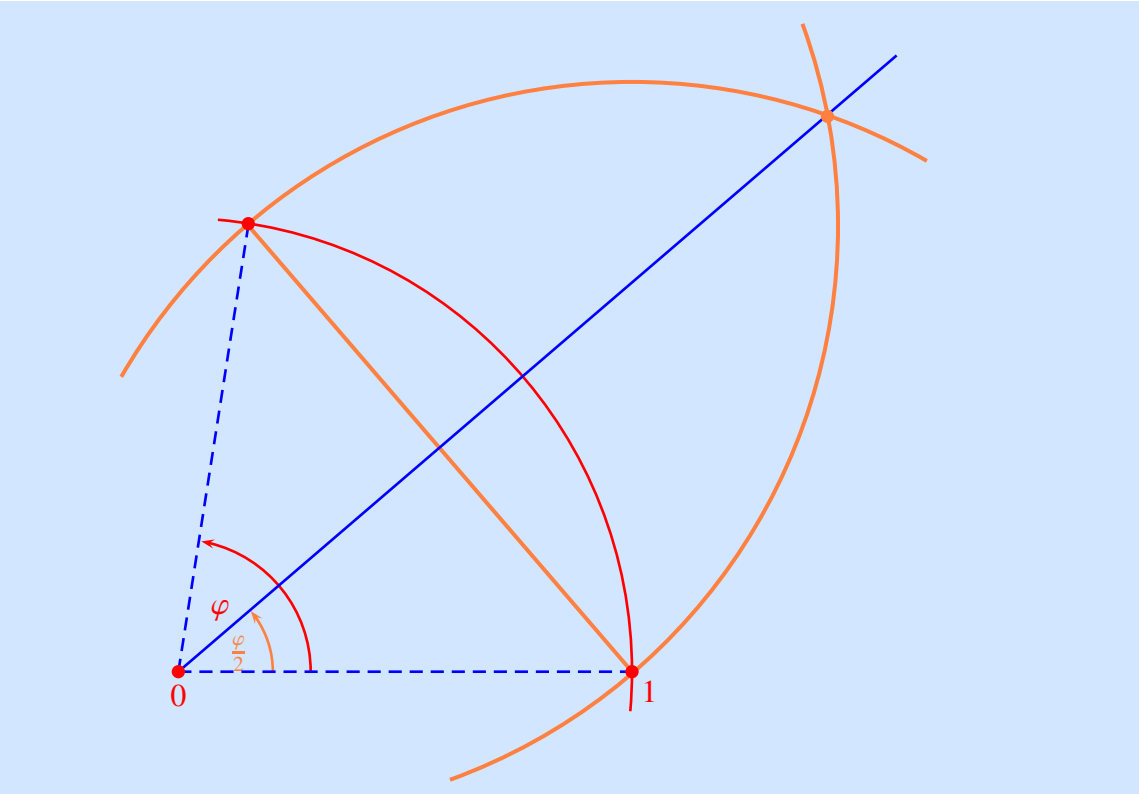


Abbildung IV.3: Konstruktion der Winkelhalbierenden

Wir haben

- ⋆ $x = \sqrt{1+y^2}$,
- ⋆ $\left(\frac{r}{2}-1\right)^2 + y^2 = \frac{r^2}{4}$.

Aus diesen Gleichungen ergibt sich

$$\frac{r^2}{4} - r + x^2 = \frac{r^2}{4}$$

und damit wie gewünscht $x^2 = r$. □

IV.3.4 Satz. *Es sei $M \subset \mathbb{C}$ eine Teilmenge, die die Zahlen 0 und 1 enthält. Für einen Punkt $z \in \mathbb{C}$ sind folgende Aussagen äquivalent:*

i) *Der Punkt z ist aus M konstruierbar, d.h. $z \in M_\infty$.*

ii) *Es gibt ein $k \geq 0$ und eine Kette*

$$\mathbb{Q}(M \cup \overline{M}) =: L_0 \subset L_1 \subset \cdots \subset L_k \subset \mathbb{C}$$

von Teilkörpern, so dass

- ⋆ $[L_i : L_{i-1}] = 2,\ i = 1, ..., k,$
- ⋆ $z \in L_k.$

Beweis. „ii)⟹i)". Nach Satz IV.3.1 und Folgerung IV.3.2 ist $M_\infty \subset \mathbb{C}$ ein Teilkörper mit $\overline{M}_\infty = M_\infty$. Deshalb gilt $\mathbb{Q} \subset \overline{M}_\infty$ (Bemerkung IV.2.3), $M \cup \overline{M} \subset M_\infty$ und $\mathbb{Q}(M \cup \overline{M}) \subset M_\infty$ (Satz IV.2.4).

Seien $i \in \{1, ..., k\}$ und $z_i \in L_i \setminus L_{i-1}$. Es gibt somit Zahlen $a, b \in L_{i-1}$ mit

$$z_i^2 + 2 \cdot a \cdot z_i + b = 0, \quad \text{d.h.} \quad (z_i + a)^2 = c_i := a^2 - b.$$

Es folgt

$$L_i = L_{i-1}(z_i) = L_{i-1}(z_i + a) = L_{i-1}(\sqrt{c_i}).$$

Nach Satz IV.3.3 ist $z_i + a = \sqrt{c_i}$ aus L_{i-1} konstruierbar. Wenn $z_i + a$ aus L_{i-1} konstruierbar ist, dann auch z_i.

„i)⟹ii)". Wir betrachten einen Teilkörper $L \subset \mathbb{C}$ mit $\overline{L} = L$ und definieren (vgl. Definition IV.1.2 und Bemerkung IV.1.4)

$$\begin{aligned} G(L) &:= \{\gamma \subset \mathbb{C} \mid \gamma \text{ ist Gerade durch zwei Punkte in } L\}, \\ K(L) &:= \{\varkappa \subset \mathbb{C} \mid \varkappa \text{ ist ein Kreis mit Mittelpunkt in } L \text{ und enthält einen Punkt aus } L\}. \end{aligned}$$

Wir untersuchen die Gleichungen, die in den verschiedenen Konstruktionsschritten auftauchen und zeigen, dass sie zu Erweiterungen von L vom Grad eins oder zwei führen.

Behauptung 1. *Es seien γ_1, γ_2 zwei verschiedene Geraden aus $G(L)$ und z ihr Schnittpunkt. Dann gilt $z \in L$.*

Wir finden Zahlen $u_0, u_1, v_0, v_1 \in L$, so dass

$$\begin{aligned} \gamma_1 &= \{u_0 + \lambda \cdot u_1 \mid \lambda \in \mathbb{R}\}, \\ \gamma_2 &= \{v_0 + \mu \cdot v_1 \mid \mu \in \mathbb{R}\}. \end{aligned}$$

Wir müssen die Gleichung

$$u_0 + \lambda \cdot u_1 = v_0 + \mu \cdot v_1 \tag{IV.1}$$

lösen. Da λ und μ reell sind, ist Gleichung (IV.1) äquivalent zu dem Gleichungssystem

$$\begin{aligned} \mathrm{Re}(u_0) + \lambda \cdot \mathrm{Re}(u_1) &= \mathrm{Re}(v_0) + \mu \cdot \mathrm{Re}(v_1) \\ \mathrm{Im}(u_0) + \lambda \cdot \mathrm{Im}(u_1) &= \mathrm{Im}(v_0) + \mu \cdot \mathrm{Im}(v_1), \end{aligned}$$

mit reellen Koeffizienten, d.h.

$$\underbrace{\begin{pmatrix} \mathrm{Re}(u_1) & -\mathrm{Re}(v_1) \\ \mathrm{Im}(u_1) & -\mathrm{Im}(v_1) \end{pmatrix}}_{=:A} \cdot \begin{pmatrix} \lambda \\ \mu \end{pmatrix} = \begin{pmatrix} \mathrm{Re}(v_0) - \mathrm{Re}(u_0) \\ \mathrm{Im}(v_0) - \mathrm{Im}(u_0) \end{pmatrix}.$$

Die Voraussetzung $\gamma_1 \neq \gamma_2$ bedeutet, dass A den Rang zwei hat.

Bemerkung. Es sei $z \in L$. Da $L = \overline{L}$ vorausgesetzt wurde, gilt

- $\mathrm{Re}(z) = \frac{1}{2} \cdot (z + \overline{z}) \in L,$

- $i \cdot \mathrm{Im}(z) = \frac{1}{2} \cdot (z - \overline{z}) \in L$.

Aus der Bemerkung folgt, dass die Einträge des Vektors

$$A^{-1} \cdot \begin{pmatrix} \mathrm{Re}(v_0) - \mathrm{Re}(u_0) \\ \mathrm{Im}(v_0) - \mathrm{Im}(u_0) \end{pmatrix}$$

in L liegen. Damit zeigt Gleichung (IV.1), dass $z \in L$. √

Behauptung 2. *Es seien $\gamma \in G(L)$, $\varkappa \in K(L)$ und $z \in \gamma \cap \varkappa$. Dann existiert eine Zahl $w \in L$, so dass $z \in L(\sqrt{w})$.*

Es seien $u_0, u_1 \in L$, so dass

$$\gamma = \{\, u_0 + \lambda \cdot u_1 \mid \lambda \in \mathbb{R} \,\}.$$

Weiter seien v_0 der Mittelpunkt von $\varkappa$ und v_1 ein Punkt in $\varkappa \cap L$. Wegen $\overline{L} = L$ gilt

$$|z|^2 = z \cdot \overline{z} \in L$$

für jedes Element $z \in L$ und damit insbesondere

$$r^2 = |v_1 - v_0|^2 \in L.$$

Wir haben

$$\varkappa = \{\, z \in \mathbb{C} \mid (z - v_0) \cdot (\overline{z} - \overline{v}_0) = r^2 \,\}.$$

Die Werte für λ, die einem Schnittpunkt von γ und $\varkappa$ beschreiben, genügen somit der Gleichung

$$(\lambda \cdot u_1 + u_0 - v_0) \cdot (\lambda \cdot \overline{u}_1 + \overline{u}_0 - \overline{v}_0) = r^2,$$

also

$$\lambda^2 \cdot |u_1|^2 + \lambda \cdot (u_1 \cdot (\overline{u}_0 - \overline{v}_0) + \overline{u}_1 \cdot (u_0 - v_0)) + |u_0 - v_0|^2 - r^2 = 0.$$

Es seien

$$a := |u_1|^2, \quad b := u_1 \cdot (\overline{u}_0 - \overline{v}_0) + \overline{u}_1 \cdot (u_0 - v_0) \quad \text{und} \quad c := |u_0 - v_0|^2 - r^2.$$

Nach der Lösungsformel für quadratische Gleichungen in den komplexen Zahlen haben wir

$$\lambda = \frac{-b \pm \sqrt{b^2 - 4 \cdot a \cdot c}}{2 \cdot a} \in L(\sqrt{b^2 - 4 \cdot a \cdot c}).$$

Dabei gilt $w := b^2 - 4 \cdot a \cdot c \in L$. √

Behauptung 3. *Zu zwei verschiedenen Kreisen $\varkappa_1, \varkappa_2 \in K(L)$ und einem Punkt $z \in \varkappa_1 \cap \varkappa_2$ existiert eine Zahl $w \in L$ mit $z \in L(\sqrt{w})$.*

Es sei u_0 bzw. v_0 der Mittelpunkt von $\varkappa_1$ bzw. $\varkappa_2$ und u_1 bzw. v_1 ein Punkt in $\varkappa_1 \cap L$ bzw. $\varkappa_2 \cap L$. Der Punkt z erfüllt die Gleichungen

$$\begin{aligned} |z|^2 - z \cdot \overline{u}_0 - \overline{z} \cdot u_0 + |u_0|^2 &= (z - u_0) \cdot (\overline{z} - \overline{u}_0) = r_1^2, \quad r_1 := \sqrt{(u_1 - u_0) \cdot (\overline{u}_1 - \overline{u}_0)}, \\ |z|^2 - z \cdot \overline{v}_0 - \overline{z} \cdot v_0 + |v_0|^2 &= (z - v_0) \cdot (\overline{z} - \overline{v}_0) = r_2^2, \quad r_2 := \sqrt{(v_1 - v_0) \cdot (\overline{v}_1 - \overline{v}_0)}. \end{aligned}$$

Daraus folgt

$$\begin{aligned} 2 \cdot \mathrm{Re}(z) \cdot \mathrm{Re}(\overline{v}_0 - \overline{u}_0) - 2 \cdot \mathrm{Im}(z) \cdot \mathrm{Im}(\overline{v}_0 - \overline{u}_0) &= 2 \cdot \mathrm{Re}(z \cdot (\overline{v}_0 - \overline{u}_0)) \\ &= z \cdot (\overline{v}_0 - \overline{u}_0) + \overline{z} \cdot (v_0 - u_0) \\ &= r_1^2 - r_2^2 - |u_0|^2 + |v_0|^2. \end{aligned}$$

Da die Kreise $\varkappa_1$ und $\varkappa_2$ verschieden sind und sich schneiden, gilt $u_0 \neq v_0$. Deshalb ist dies ist die Gleichung einer Geraden $\gamma \subset \mathbb{C}$.

Wir betrachten zunächst den Fall, dass $L \subset \mathbb{R}$. Es folgt

$$\mathrm{Re}(z) = u := \frac{r_1^2 - r_2^2 - |u_0|^2 + |v_0|^2}{2 \cdot \mathrm{Re}(\overline{v}_0 - \overline{u}_0)} \in L.$$

Damit ergibt sich

$$\mathrm{Im}(z) = \sqrt{\widetilde{w}},\ \widetilde{w} := r_1^2 - (u - u_0)^2, \quad \text{und} \quad i \cdot \mathrm{Im}(z) = i \cdot \sqrt{\widetilde{w}} = \sqrt{-\widetilde{w}} \in L(\sqrt{w}),\ w := -\widetilde{w} \in L.$$

In den verbleibenden Fällen enthält die Gerade γ zwei verschiedene Punkte aus L (Übung) und gehört folglich der Menge $G(L)$ an. Es gilt $z \in \gamma \cap \varkappa_1$. Wir können jetzt Behauptung 2 anwenden. √

Wir zeigen die Aussage durch vollständige Induktion über l für Punkte $z \in M_l$. Für $l = 0$ gilt $z \in \mathbb{Q}(M \cup \overline{M})$, und es nichts zu zeigen. Nun sei $z \in M_{l+1}$. Dann ist z nach Definition Schnittpunkt zweier verschiedener Geraden aus $G(M_l)$, einer Geraden aus $G(M_l)$ und eines Kreises aus $K(M_l)$ oder zweier Kreise aus $K(M_l)$. Um die beiden Geraden, die Gerade und den Kreis bzw. die beiden Kreise zu spezifizieren benötigen wir Punkte $u_1, ..., u_t \in M_l$ mit $3 \leq t \leq 6$. Es sei

$$L' := \mathbb{Q}(M \cup \overline{M})(u_1, ..., u_t, \overline{u}_1, ..., \overline{u}_t).$$

Behauptung 1, 2 und 3 zeigen, dass

$$[L'(z) : L'] \in \{1, 2\}. \tag{IV.2}$$

Für das Folgende sei k ein Körper. Eine Körpererweiterung $k \subset L$ hat *Eigenschaft (Q)*, wenn es ein $m \geq 0$ und einen Turm

$$k =: L_0 \subset L_1 \subset \cdots \subset L_m \tag{IV.3}$$

von Körpererweiterungen mit

$$[L_i : L_{i-1}] = 2, \quad i = 1, ..., m, \quad \text{und} \quad L \subset L_m$$

gibt. In unserem Fall werden wir eine Körpererweiterung $k \subset L \subset \mathbb{C}$ mit $\overline{k} = k$ betrachten. Komplexe Konjugation $\overline{\cdot}: \mathbb{C} \longrightarrow \mathbb{C}$, $z \longmapsto \overline{z}$, ist ein Automorphismus des komplexen Zahlkörpers. Somit ist $\overline{K}$ für jeden Teilkörper K von $\mathbb{C}$ ebenfalls ein Teilkörper. Wenn $k \subset L$ eine Erweiterung mit Eigenschaft (Q) ist und $\overline{k} = k$ gilt, dann hat auch die Erweiterung $k = \overline{k} \subset \overline{L}$ Eigenschaft (Q), denn Anwendung von $\overline{\cdot}$ auf (IV.3) ergibt

$$k = \overline{k} = \overline{L}_0 \subset \overline{L}_1 \subset \cdots \subset \overline{L}_m \quad \text{und} \quad \overline{L} \subset \overline{L}_m.$$

Der Grad der Körpererweiterung $\overline{L}_{i-1} \subset \overline{L}_i$ ist wieder zwei, $i = 1, ..., m$.

Behauptung 4. *Es seien $k \subset K$ eine Körpererweiterung und $v_1, ..., v_s \in K$ Elemente, so dass $k \subset k(v_i)$ Eigenschaft (Q) hat, $i = 1, ..., s$. Dann hat auch die Körpererweiterung $k \subset k(v_1, ..., v_s)$ Eigenschaft (Q).*

Diese Aussage beweisen wir durch Induktion über s. Für $s = 1$ ist die Behauptung gleichbedeutend mit der Voraussetzung. Im Induktionsschritt $s \longrightarrow s + 1$ ist wegen der Induktionsvoraussetzung nur zu zeigen, dass die Erweiterung $k(v_1, ..., v_s) \subset k(v_1, ..., v_{s+1})$ Eigenschaft (Q) hat. Nach Voraussetzung existieren eine Zahl m und komplexe Zahlen $w_1, ..., w_m$, so dass die Teilkörper

$$L_0 := k, \quad L_i := L_{i-1}(\sqrt{w_i}), \quad i = 1, ..., m,$$

die Bedingung

$$k(v_{s+1}) \subset L_m$$

erfüllen. Weiter gibt es einen Turm

$$k =: K_0 \subset K_1 \subset \cdots \subset K_n$$

von Körpererweiterungen mit

$$[K_i : K_{i-1}] = 2, \quad i = 1, ..., n, \quad \text{und} \quad k(v_1, ..., v_s) \subset K_n.$$

Nun setzen wir

$$L_0' := K_n, \quad L_i' := L_{i-1}'(\sqrt{w_i}), \quad i = 1, ..., m.$$

Dann finden wir den Turm

$$L_0' \subset L_1' \subset \cdots \subset L_m'$$

von Körpererweiterungen mit

$$[L_i' : L_{i-1}'] \in \{1, 2\}, \quad i = 1, ..., m.$$

Dies vollendet den Induktionsschritt. √

Wir wenden Behauptung 4 auf $k := \mathbb{Q}(M \cup \overline{M})$ und $u_1, ..., u_t, \overline{u}_1, ..., \overline{u}_t$ an. Zusammen mit (IV.2) folgt endlich der Satz. □

IV.3.5 Folgerung. *Es sei $\alpha \in \mathbb{C}$ eine aus der Menge $\{0, 1\}$ konstruierbare Zahl. Dann existiert eine Zahl $k \in \mathbb{N}$ mit*

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^k.$$

Beweis. Hier benötigt man Aufgabe IV.2.8. □

Wir wenden diese Erkenntnisse auf die Konstruktionsfragen der Antike (s. Beispiel IV.1.3) an.

IV.3.6 Beispiele. i) Das delische Problem ist unlösbar. Dazu reicht es, $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ zu beweisen. Dafür genügt es wiederum zu überprüfen, dass das Polynom $x^3 - 2$ irreduzibel ist. Wäre es reduzibel, so folgte aus dem Satz von Gauß A.2.5 und der Tatsache, dass der Koeffizient von x^3 eins ist, dass es einen Linearfaktor der Form $x - a$, $a \in \mathbb{Z}$, und damit eine ganzzahlige Nullstelle hätte. Das ist aber nicht der Fall.

ii) Die Winkeldreiteilung ist im allgemeinen unmöglich. Wir zeigen an dieser Stelle, dass die Winkeldreiteilung für den Winkel $\alpha = \pi/3$ unmöglich ist. Wir bemerken, dass für

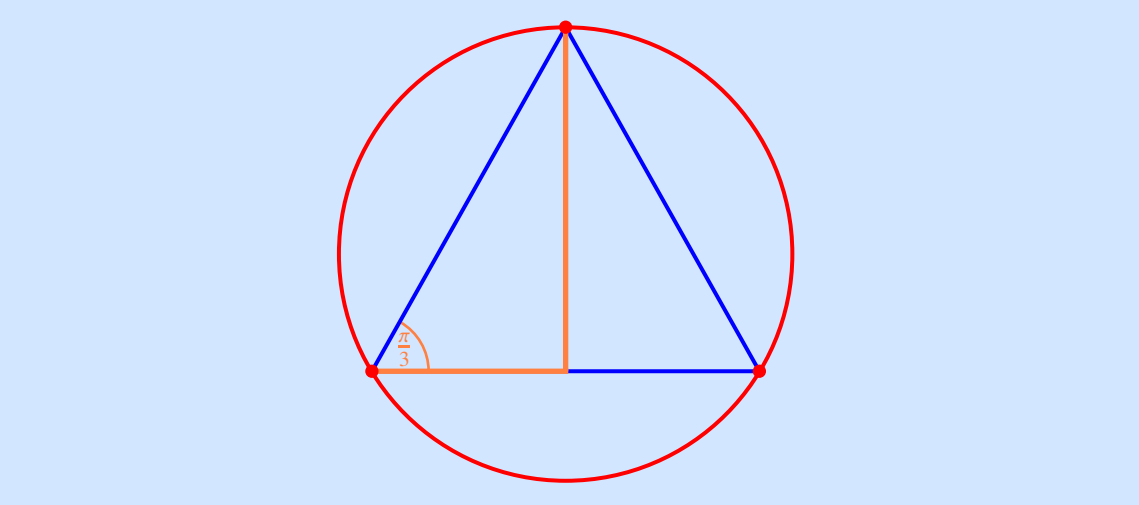
$\xi \in (0, 2\pi]$ der Teilkörper der aus $\{0, 1, \exp(i \cdot \xi)\}$ konstruierbaren komplexen Zahlen mit dem Teilkörper der aus $\{0, 1, \cos(\xi)\}$ konstruierbaren komplexen Zahlen übereinstimmt. Das stimmt, weil nach der Euler-Formel ([16], Satz 4.10.12)

$$\cos(\xi) = \mathrm{Re}(\exp(i \cdot \xi))$$

gilt und man $\exp(i \cdot \xi)$ aus $\{0, 1, \cos(\xi)\}$ konstruieren kann, indem man die Parallele zur imaginären Achse durch $\cos(\xi)$ mit dem Einheitskreis schneidet.

Ein gleichseitiges Dreieck mit Seitenlänge 1 hat dreimal den Innenwinkel $\pi/3$. Zeichnet man die Höhe auf eine der Grundseiten, so erkennt man

$$\cos\left(\frac{\pi}{3}\right) = \frac{1}{2}.$$



Weiter zeigen die Additionstheoreme für Sinus und Kosinus ([16], Satz 4.8.8 oder Folgerung 4.10.13), dass

$$4 \cdot \cos^3(\beta) - 3 \cdot \cos(\beta) = \cos(3 \cdot \beta) = \cos(\alpha) = \frac{1}{2}.$$

Für den speziellen Winkel α lautet die Frage, ob $\cos(\beta)$ aus der Menge $\{0, 1\}$ konstruierbar ist. Das Polynom

$$4 \cdot x^3 - 3 \cdot x - \frac{1}{2} \in \mathbb{Q}[x]$$

ist irreduzibel. Andernfalls hätte es eine Nullstelle $\xi_0 \in \mathbb{Q}$. Die Zahl ξ_0 wäre dann auch Nullstelle von

$$8 \cdot x^3 - 6 \cdot x - 1.$$

Folglich wäre $2 \cdot \xi_0$ eine Nullstelle des Polynoms

$$h := x^3 - 3 \cdot x - 1 \in \mathbb{Z}[x].$$

Das Polynom h ist primitiv und wäre damit nach dem Satz von Gauß A.2.5 als Element von $\mathbb{Z}[x]$ reduzibel. Da der Leitkoeffizient und der konstante Term von h eins sind, würde

h durch ein Polynom der Form $x \pm 1$ geteilt, d.h. 1 oder -1 wäre eine Nullstelle von h. Das ist aber nicht der Fall. Mit Bemerkung IV.2.13 schließen wir

$$[\mathbb{Q}(\cos(\beta)) : \mathbb{Q}] = 3.$$

Wegen Folgerung IV.3.5 und der Gradformel aus Aufgabe IV.2.8 kann $\cos(\beta)$ nicht konstruierbar sein.

iii) Die Quadratur des Kreises ist unmöglich. Dazu beachte man, dass eine aus $\{0, 1\}$ konstruierbare Zahl nach Folgerung IV.3.5 algebraisch ist. Die Zahl π ist aber **transzendent**, d.h. nicht algebraisch. Diese tiefliegende Aussage wollen wir hier nicht beweisen. Eine lebhafte Darstellung dieses Resultats ist in dem Buch [22] enthalten.

IV.4 Kreisteilungspolynome

Sei $n \geq 3$ eine natürliche Zahl. Jetzt werden wir uns mit der Frage beschäftigen, unter welchen Voraussetzungen ein regelmäßiges n-Eck mit Zirkel und Lineal konstruierbar ist. Dabei können wir uns auf den Fall beschränken, dass das zu konstruierende n-Eck auf dem Einheitskreis liegt und 1 eine der Ecken ist. Die „Startmenge“ ist in diesem Fall $M = \{0, 1\}$ und wir möchten wissen, ob die komplexe Zahl

$$\zeta_n := \exp\left(\frac{2\pi i}{n}\right)$$

konstruierbar ist. Nach Bemerkung IV.2.13 und Folgerung IV.3.5 müssen wir dafür den Grad des Minimalpolynoms von ζ_n bestimmen.

IV.4.1 Bemerkungen. i) Für das Polynom $f := x^n - 1$ gilt $f(\zeta_n) = 0$. Damit ist ζ_n eine algebraische Zahl.

ii) Es sei

$$C_n := \langle \zeta_n \rangle = \{1, \zeta_n, ..., \zeta_n^{n-1}\}$$

die von ζ_n erzeugte Untergruppe von $\mathbb{C}^\star$. Die Abbildung

$$\begin{array}{rccc} \psi\colon & \mathbb{Z}_n & \longrightarrow & C_n \\ & k & \longmapsto & \zeta_n^k \end{array}$$

ist ein Isomorphismus. Schließlich gilt

$$C_n = \{\alpha \in \mathbb{C} \mid \alpha^n = 1\}.$$

IV.4.2 Definitionen. i) Ein Element $\alpha \in C_n$ ist eine *n-te Einheitswurzel*.

ii) Eine n-te Einheitswurzel $\alpha \in C_n$, die C_n erzeugt, d.h. für die $\langle \alpha \rangle = C_n$ gilt, darf sich *primitive n-te Einheitswurzel* nennen.

IV.4.3 Beobachtung. *Sei $n \geq 1$. Für eine n-te Einheitswurzel $\zeta \in C_n$ sind folgende Aussagen äquivalent:*

i) *ζ ist eine primitive n-te Einheitswurzel.*

ii) *Es gibt eine Zahl $k \in \{0, ..., n-1\}$ mit* $\mathrm{ggT}(k, n) = 1$ *und $\zeta = \zeta_n^k$.*

Beweis. Es gibt ein $k \in \{0, ..., n-1\}$ mit $\zeta = \zeta_n^k$. Man beachte, dass

$$\forall l \in \mathbb{Z}: \quad \zeta_n^{k\cdot l} = \zeta^l = 1 \quad \Longleftrightarrow \quad n|(k \cdot l).$$

Es seien $d := \mathrm{ggT}(k, n)$, $k' := k/d$ und $n' := n/d$. Man sieht nun leicht

$$\mathrm{Ord}(\zeta) = \min\{\nu \geq 1 \,|\, n|(k \cdot \nu)\} = n'.$$

Dies zeigt, dass $\langle\zeta\rangle = C_n$ äquivalent zu $\mathrm{ggT}(k, n) = 1$ ist. □

IV.4.4 Definition. Für $n \in \mathbb{N}$ sei

$$C_n^\star := \{\zeta \in C_n \,|\, \zeta \text{ ist primitive } n\text{-te Einheitswurzel}\}.$$

IV.4.5 Beobachtung. *Für jede natürliche Zahl $n \geq 1$ gilt*

$$\#C_n^\star = \varphi(n).$$

Beweis. Dies ergibt sich aus Beobachtung IV.4.3 und Eigenschaft III.2.3, i). □

IV.4.6 Definition. Es sei $n \geq 1$ eine natürliche Zahl. Das Polynom

$$\Phi_n(x) := \prod_{\zeta \in C_n^\star} (x - \zeta) \in \mathbb{C}[x]$$

heißt das *n-te Kreisteilungspolynom*.

IV.4.7 Satz. *Für $n \geq 1$ gilt $\Phi_n(x) \in \mathbb{Z}[x]$.*

Beweis. i) Für jede Primzahl p gilt nach Beobachtung IV.4.3

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

Dies ist ein Polynom mit ganzzahligen Koeffizienten.

ii) Für eine natürliche Zahl $n \geq 1$ und einen Teiler d von n gilt

$$C_d \subset C_n.$$

Dazu sei $m := n/d \in \mathbb{N}$. Für $\zeta \in C_d$ haben wir

$$\zeta^n = (\zeta^d)^m = 1,$$

so dass $\zeta \in C_n$. Weiter erkennen wir

$$C_d^\star = \{\zeta \in C_n \,|\, \mathrm{Ord}(\zeta) = d\}.$$

Es folgt

$$x^n - 1 = \prod_{d|n} \Phi_d(x) = \Phi_n(x) \cdot \underbrace{\prod_{\substack{d|n \\ d<n}} \Phi_d(x)}_{=:\Psi_n(x)}.$$

Eine leichte Induktion ergibt

$$\forall n \geq 1: \quad \Psi_n(x) \in \mathbb{Z}[x] \wedge \text{der Leitkoeffizient von } \Psi_n(x) \text{ ist eins.}$$

Polynomdivision mit Rest A.1.5 zeigt abermals, dass $\Phi_n(x)$ ein ganzzahliges Polynom ist. □

IV.4.8 Beispiele. i) $\Phi_1(x) = x - 1$.
ii) $\Phi_2(x) = (x^2 - 1)/(x - 1) = x + 1$.
iii) $\Phi_3(x) = (x^3 - 1)/(x - 1) = x^2 + x + 1$.
iv) $\Phi_4(x) = (x^4 - 1)/(\Phi_1(x) \cdot \Phi_2(x)) = (x^4 - 1)/(x^2 - 1) = x^2 + 1$.
v) $\Phi_5(x) = (x^5 - 1)/(x - 1) = x^4 + x^3 + x^2 + x + 1$.
vi) $\Phi_6(x) = (x^6 - 1)/(\Phi_1(x) \cdot \Phi_2(x) \cdot \Phi_3(x)) = (x^6 - 1)/((x^2 - 1) \cdot (x^2 + x + 1)) = (x^6 - 1)/(x^4 + x^3 - x - 1) = x^2 - x + 1$.

Vereinbarung. Ab jetzt setzen wir voraus, dass $p := n$ eine Primzahl ist.

Viele der folgenden Aussagen gelten auch für natürliche Zahlen, die keine Primzahlen sind. Sie sind dann aber aufwändiger zu beweisen (s. [12], §13).

IV.4.9 Satz. *Es sei p eine Primzahl. Dann ist das Polynom $\Phi_p(x) \in \mathbb{Q}[x]$ irreduzibel. Insbesondere gilt*

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1.$$

Beweis. Da der Leitkoeffizient des Polynoms

$$\Phi_p(x) = x^{p-1} + x^{p-2} + \cdots + x + 1 \in \mathbb{Z}[x]$$

eins ist, handelt es sich um ein primitives Polynom. Wäre es als Element von $\mathbb{Q}[x]$ reduzibel, so gäbe es nach dem Satz von Gauß A.2.5 zwei nicht konstante ganzzahlige Polyome $g, h \in \mathbb{Z}[x] \setminus \mathbb{Z}$, so dass

$$\Phi_p = g \cdot h.$$

Insbesondere haben wir

$$p = \Phi_p(1) = g(1) \cdot h(1).$$

Man beachte, dass g und h primitiv sind, weil Φ_p es ist. Wir können die Situation so einrichten, dass

- $\star$ g irreduzibel ist,
- $\star$ $g(1) = p$.

Es sei $\zeta \in \mathbb{C}$ eine Nullstelle von g. Dann gilt $\zeta \neq 1$, und ζ ist nach Beobachtung IV.4.3 eine primitive p-te Einheitswurzel. Weiter sei $\widetilde{\zeta} \in \mathbb{C}$ eine Nullstelle von h. Dann ist $\widetilde{\zeta}$ ebenfalls eine (primitive) p-te Einheitswurzel. Es existiert somit ein $k \in \{1, ..., p-1\}$ mit $\widetilde{\zeta} = \zeta^k$. Wir definieren

$$\widetilde{h}(x) := h(x^k).$$

Es gilt

$$\widetilde{h}(\zeta) = h(\zeta^k) = h(\widetilde{\zeta}) = 0.$$

Da das Polynom g irreduzibel ist, stimmt es bis auf einen Faktor in $\mathbb{Q}^\star$ mit dem Minimalpolynom von ζ überein. Also folgern wir

$$g | \widetilde{h} \quad \text{in} \quad \mathbb{Q}[x].$$

Nun ist g primitiv. Nach dem Satz von Gauß A.2.5 gilt sogar

$$g | \widetilde{h} \quad \text{in} \quad \mathbb{Z}[x].$$

Daher finden wir ein Polynom $\overline{h} \in \mathbb{Z}[x]$ mit

$$\widetilde{h} = g \cdot \overline{h}.$$

Die Berechnung

$$1 = h(1) = \widetilde{h}(1) = g(1) \cdot \overline{h}(1) = p \cdot \overline{h}(1)$$

zeigt, dass die konstruierte Situation absurd ist und deshalb unsere Annahme, dass Φ_p reduzibel ist, falsch war.

Da Φ_p irreduzibel ist und den Leitkoeffizienten 1 hat, ist es das Minimalpolynom der p-ten Einheitswurzel ζ_p und jeder anderen p-ten Einheitswurzel ungleich eins. Die Formel für den Grad der Körpererweiterung $\mathbb{Q} \subset \mathbb{Q}(\zeta_p)$ ergibt sich aus Bemerkung IV.2.13. □

Jetzt widmen wir uns der Galois-Gruppe

$$\Gamma := \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_p)).$$

Für $\gamma \in \Gamma$ ist $\gamma(\zeta_p)$ ebenfalls eine primitive p-te Einheitswurzel. Deswegen gibt es genau eine Zahl $k_\gamma \in \{ 1, ..., p-1, \}$, so dass

$$\gamma(\zeta_p) = \zeta_p^{k_\gamma}.$$

IV.4.10 Satz. *Die Abbildung*

$$\begin{array}{rcl} \psi\colon \Gamma & \longrightarrow & (\mathbb{Z}_p^\star, \cdot)(\cong (\mathbb{Z}_{p-1}, +)) \\ \gamma & \longmapsto & k_\gamma \end{array}$$

ist ein Isomorphismus.

Beweis. Es ist leicht einzusehen, dass ψ ein injektiver Gruppenhomomorphismus ist. Um zu beweisen, dass ψ auch surjektiv ist, seien $k \in \{ 1, ..., p-1 \}$ und $\zeta = \zeta_p^k$. Folglich ist ζ eine primitive p-te Einheitswurzel. Die Abbildung

$$\begin{array}{rcl} \gamma\colon \mathbb{Q}(\zeta_p) & \longrightarrow & \mathbb{Q}(\zeta_p) \\ \displaystyle\sum_{i=0}^{p-2} a_i \cdot \zeta_p^i & \longmapsto & \displaystyle\sum_{i=0}^{p-2} a_i \cdot \zeta^i \end{array}$$

ist ein Automorphismus des $\mathbb{Q}$-Vektorraums $\mathbb{Q}(\zeta_p)$. Dass auch

$$\forall a, b \in \mathbb{Q}(\zeta_p) : \quad \gamma(a \cdot b) = \gamma(a) \cdot \gamma(b)$$

gilt, leitet man schnell aus der Tatsache ab, dass Φ_p sowohl das Minimalpolynom von ζ_p als auch dasjenige von ζ ist. □

Zur Konstruierbarkeit des regelmäßigen p-Ecks

IV.4.11 Satz. *Es sei $p \geq 3$ eine Primzahl. Die folgenden Aussagen sind äquivalent:*

i) *p ist eine Fermat-Primzahl.*

ii) *Das regelmäßige p-Eck ist mit Zirkel und Lineal konstruierbar.*

Beweis. ii)$\Longrightarrow$i). Nach Folgerung IV.3.5 muss ein $k \in \mathbb{N}$ existieren, so dass

$$2^k = [\mathbb{Q}(\zeta_p) : \mathbb{Q}] \overset{\text{IV.4.9}}{=} \varphi(p) \overset{\text{III.2.3, iii)}}{=} p - 1.$$

Aus Satz I.3.7 folgt, dass p eine Fermat-Primzahl ist.

i)$\Longrightarrow$ii). Wir schreiben $p = 2^k + 1$. Die Galois-Gruppe $\Gamma = \mathrm{Gal}_{\mathbb{Q}}(\mathbb{Q}(\zeta_p))$ ist nach Satz IV.4.10 zyklisch von der Ordnung 2^k. Wir wählen einen Erzeuger γ_0 und setzen

$$\Gamma_i := \langle \gamma_0^{2^i} \rangle, \quad i = 0, ..., k.$$

Es gilt:

- $\star$ $\{e\} = \Gamma_k \subset \Gamma_{k-1} \subset \cdots \subset \Gamma_1 \subset \Gamma_0 = \Gamma$.
- $\star$ $\#(\Gamma_{i-1}/\Gamma_i) = 2$, $i = 1, ..., k$.

Weiter sei

$$L_i := \mathrm{Fix}(\Gamma_i) := \{\, a \in \mathbb{Q}(\zeta_p) \,|\, \forall \gamma \in \Gamma_i : \gamma(a) = a \,\}, \quad i = 0, ..., k.$$

Diese Teilkörper formen den Turm

$$\mathbb{Q}(\zeta_p) = L_k \supset L_{k-1} \supset \cdots \supset L_1 \supset L_0 \supset \mathbb{Q}.$$

Wir zeigen

$$L_{i-1} \subsetneq L_i, \quad i = 1, ..., k.$$

Aus der Gradformel in Aufgabe IV.2.8 und $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = 2^k$ folgt dann $\mathbb{Q} = L_0$ und $[L_i : L_{i-1}] = 2$, $i = 1, ..., k$.

Für $\gamma \in \Gamma$ führen wir den Ringautomorphismus (vgl. Aufgabe A.1.7)

$$\begin{array}{rcl} \gamma_\star \colon \mathbb{Q}(\zeta_p)[x] & \longrightarrow & \mathbb{Q}(\zeta_p)[x] \\ f = a_0 + a_1 \cdot x + \cdots + a_n \cdot x^n & \longmapsto & \gamma_\star(f) := \gamma(a_0) + \gamma(a_1) \cdot x + \cdots + \gamma(a_n) \cdot x^n \end{array}$$

ein. Hier gilt für $i = 1, ..., k$ und ein Polynom $f \in \mathbb{Q}(\zeta_p)[x]$:

$$(\forall \gamma \in \Gamma_i : \ \gamma_\star(f) = f) \quad \Longleftrightarrow \quad \text{(Die Koeffizienten von } f \text{ liegen in } L_i\text{)}.$$

Sei weiter

$$\begin{array}{rcl} \sigma_i \colon \Gamma_i \times C_p & \longrightarrow & C_p \\ (\gamma, \zeta) & \longmapsto & \gamma(\zeta). \end{array}$$

Die Standgruppe von ζ_p ist trivial, so dass nach Satz II.7.2 die Bahn $\Gamma_i \cdot \zeta_p$ genau 2^{k-i} Elemente umfasst.

Schließlich sei

$$\Psi_i(x) := \prod_{\gamma \in \Gamma_i} (x - \gamma(\zeta_p)), \quad i = 0, ..., k.$$

Das Polynom Ψ_i hat Grad 2^{k-i} und erfüllt

$$\forall \gamma \in \Gamma_i : \quad \gamma_\star(\Psi_i) = \Psi_i,$$

so dass seine Koeffizienten in L_i liegen, $i = 0, ..., k$.

Für $i \in \{1, ..., k\}$ ist das Polynom $\Psi_i = c_0 + c_1 \cdot x + \cdots + c_{2^{k-i}} \cdot x^{2^{k-i}}$ nicht invariant unter Γ_{i-1}, d.h. es existiert ein Index $j \in \{0, ..., 2^{k-i}\}$, so dass $c_j \notin L_{i-1}$. Damit gilt $c_j \in L_i \setminus L_{i-1}$. □

IV.4.12 Bemerkung. i) Im Anschluss an Beispiel I.3.9 haben wir bereits festgehalten, dass $65\,537 = 2^{2^4} + 1$ die größte bekannte Fermat-Primzahl ist. Nach Satz IV.4.11 ist das regelmäßige 65 537-Eck konstruierbar. Ein etwas anders gelagertes Problem ist, die Konstruktion explizit durchzuführen. Diesem Problem hat sich Johann Gustav Hermes (1846 - 1912) in seiner Dissertation, an der er angeblich über zehn Jahre lang gearbeitet hat, gewidmet. Seine umfangreichen Berechnungen und Konstruktionen sind in einem Koffer enthalten, der heutzutage an der Georg-August-Universität zu Göttingen zu besichtigen ist.

ii) Im Beweis der Implikation „i)⟹ii)“ tritt die Hauptidee der Galois-Theorie auf: Für eine endliche Körpererweiterung $k \subset L$ mit Galois-Gruppe können wir jedem **Zwischenkörper** $k \subset K \subset L$ die Galois-Gruppe

$$\mathrm{Gal}_K(L) \subset \mathrm{Gal}_k(L)$$

zuordnen. Umgekehrt können wir einer Untergruppe $\Gamma' \subset \mathrm{Gal}_k(L)$ den **Fixkörper**

$$\mathrm{Fix}(\Gamma') := \{ a \in L \mid \forall \gamma \in \Gamma' : \gamma(a) = a \}$$

zuweisen. Es gibt eine Klasse von endlichen Körpererweiterungen, die sinnigerweise als Klasse der **Galois-Erweiterungen** bezeichnet wird, so dass für jede Körpererweiterung in dieser Klasse die obigen Zuordnungen zueinander inverse Bijektionen darstellen. Dies ist Bestandteil des **Hauptsatzes der Galoistheorie** ([12], §10).

Über die Struktur endlicher Gruppen weiß man sehr viel. Dieses Wissen kann man einsetzen, um Körpererweiterungen oder algebraische Gleichungen zu analysieren. Im obigen Beweis ist das sehr gut zu erkennen: Die Galois-Gruppe des „Kreisteilungskörpers“ $\mathbb{Q}(\zeta_p)$ ist sehr einfach. Wir haben sie durch Untergruppen $\Gamma_k \subset \cdots \subset \Gamma_0$ filtriert, so dass $\#(\Gamma_{i-1}/\Gamma_i) = 2$, $i = 1, ..., k$. Dieser Filtrierung steht die Filtrierung $\mathbb{Q}(\zeta_p) = L_k \supset \cdots \supset L_0 = \mathbb{Q}$ durch Teilkörper mit $[L_{i-1} : L_i] = 2$, $i = 1, ..., k$, gegenüber.

IV.4.13 Aufgabe (Regelmäßige Polygone). Es seien $m, n \geq 1$ zwei **teilerfremde** positive natürliche Zahlen. Zeigen Sie, dass das regelmäßige $(m \cdot n)$-Eck genau dann mit Zirkel und Lineal konstruierbar ist, wenn sowohl das regelmäßige m-Eck als auch das regelmäßige n-Eck es sind.

A

Über Polynome

Ein großer Teil der Algebra beschäftigt sich mit der Untersuchung von Nullstellen von Polynomen. An dieser Stelle fassen wir einige grundlegende Eigenschaften der Polynomringe in einer Veränderlichen zusammen, die an verschiedenen Stellen in diesem Skript benötigt werden. Man beachte die Gemeinsamkeiten der Teilbarkeitslehre im Ring $\mathbb{Z}$ der ganzen Zahlen mit derjenigen im Polynomring $k[x]$, k ein Körper.

A.1 Polynomdivision mit Rest

A.1.1 Definition. Es sei R ein Ring.

i) Ein *Polynom* über R ist eine Abbildung

$$f\colon \mathbb{N} \longrightarrow R,$$

so dass

$$\#\{\, n \in \mathbb{N} \mid f(n) \neq 0 \,\} < \infty.$$

ii) Das *Nullpolynom* ist die Abbildung $0\colon \mathbb{N} \longrightarrow R$, $n \longmapsto 0$.

iii) Für ein Polynom $f \neq 0$ ist der *Grad* definiert als

$$\mathrm{Grad}(f) := \max\{\, n \in \mathbb{N} \mid f(n) \neq 0 \,\}.$$

Die Zahl $f(\mathrm{Grad}(f))$ ist der *Leitkoeffizient* von f. Dem Nullpolynom weisen wir den Grad $-\infty$ zu.

Schreibweise. Es sei x eine Unbestimmte. Wir schreiben ein Polynom f vom Grad $n \geq 0$ in der Form[1]

$$f = f(x) = f(0) + f(1) \cdot x + \cdots + f(n) \cdot x^n.$$

Weiter sei

$$R[x] := \{\, f\colon \mathbb{N} \longrightarrow R \mid f \text{ ist Polynom} \,\}.$$

[1] Die missbräuchliche Notation $f(x)$ bitten wir zu entschuldigen. Sie ist dadurch gerechtfertigt, dass die Interpretation eines Polynoms als Abbildung von der Menge der natürlichen Zahlen $\mathbb{N}$ in den Körper k bei den folgenden Überlegungen in den Hintergrund tritt.

iv) Für zwei Polynome f und g ist die *Summe* das Polynom

$$\begin{array}{rcl} f+g\colon \mathbb{N} & \longrightarrow & R \\ n & \longmapsto & f(n)+g(n). \end{array}$$

v) Das *Produkt* der Polynome f und g ist das Polynom

$$\begin{array}{rcl} f\cdot g\colon \mathbb{N} & \longrightarrow & R \\ n & \longmapsto & f(0)\cdot g(n)+f(1)\cdot g(n-1)+\cdots+f(n-1)\cdot g(1)+f(n)\cdot g(0). \end{array}$$

A.1.2 Beispiel. Für ein Element $a \in k$ sei

$$\begin{array}{rcl} f_a\colon \mathbb{N} & \longrightarrow & k \\ n & \longmapsto & \begin{cases} a, & \text{falls } n=0 \\ 0, & \text{falls } n\neq 0 \end{cases}. \end{array}$$

Gemäß der obigen Konventionen wird dieses Polynom mit a bezeichnet. Auf diese Weise fassen wir k als Teilmenge von $k[x]$ auf.

A.1.3 Lemma. i) *Das Tupel* $(R[x], 0, 1, +, \cdot)$ *ist ein Ring.*
ii) *Es seien R ein Körper oder der Ring der ganzen Zahlen. Dann gilt*

$$\operatorname{Grad}(f\cdot g) = \operatorname{Grad}(f)+\operatorname{Grad}(g)$$

für zwei vom Nullpolynom verschiedene Polynome $f, g \in R[x]\setminus\{0\}$. *Insbesondere gilt*

$$R[x]^\star = R^\star$$

für die Einheiten in $R[x]$.

Beweis. Übung. □

A.1.4 Definition. Es sei R ein Ring. Der Ring $R[x]$ ist der *Polynomring* in einer Veränderlichen über R.

A.1.5 Satz (Polynomdivision mit Rest). *Es seien k ein Körper und*

$$f = a_0+a_1\cdot x+\cdots+a_n\cdot x^n, \quad g = b_0+b_1\cdot x+\cdots+b_m\cdot x^m \neq 0$$

Polynome. Dann existieren eindeutig bestimmte Polynome $q, r \in k[x]$, *so dass*

$$f = q\cdot g+r \quad \textit{und} \quad \operatorname{Grad}(r) < \operatorname{Grad}(g).$$

Beweis. **Eindeutigkeit.** Es seien $q_1, q_2, r_1, r_2 \in k[x]$ Polynome, so dass

$$q_1\cdot g+r_1 = q_2\cdot g+r_2 \quad \text{und} \quad \operatorname{Grad}(r_1),\ \operatorname{Grad}(r_2) < \operatorname{Grad}(g).$$

Es folgt

$$(q_1-q_2)\cdot g = r_2-r_1.$$

Aus

$$\operatorname{Grad}(r_2-r_1) \leq \max\{\operatorname{Grad}(r_1), \operatorname{Grad}(r_2)\} < \operatorname{Grad}(g)$$

und Lemma A.1.3, ii), folgt

$$q_1 - q_2 = 0, \quad \text{d.h.} \quad q_1 = q_2.$$

Das beinhaltet weiter

$$r_1 - r_2 = 0, \quad \text{d.h.} \quad r_1 = r_2.$$

Existenz. Falls $\mathrm{Grad}(g) = 0$, dann setzen wir

$$q := \frac{1}{b_0} \cdot f, \quad r := 0.$$

Für $\mathrm{Grad}(g) > 0$ beweisen wir die Aussage durch Induktion über $n := \mathrm{Grad}(f)$.

***n* < Grad(*g*).** Hier setzen wir

$$q := 0, \quad r := f.$$

***n* ⟶ *n* + 1.** Wir haben $n + 1 \geq \mathrm{Grad}(g)$. Es seien

$$q_1 := \frac{a_{n+1}}{b_m} \cdot x^{n+1-\mathrm{Grad}(g)} \quad \text{und} \quad f_1 := f - q_1 \cdot g.$$

Dabei gilt

$$\mathrm{Grad}(f_1) < \mathrm{Grad}(f).$$

Falls $\mathrm{Grad}(f_1) < \mathrm{Grad}(g)$, dann setzen wir $q := q_1$ und $r := f_1$. Ansonsten finden wir auf Grund der Induktionsvoraussetzung Polynome $q_2, r \in k[x]$ mit

$$f_1 = q_2 \cdot g + r \quad \text{und} \quad \mathrm{Grad}(r) < \mathrm{Grad}(g).$$

Mit

$$f = q_1 \cdot g + f_1 = q \cdot g + r, \quad q := q_1 + q_2,$$

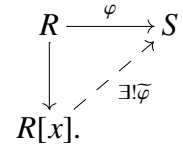
haben wir die gewünschte Zerlegung von f gefunden. □

A.1.6 Bemerkungen. i) Der obige Beweis beschreibt den üblichen Algorithmus zur Polynomdivision (vgl. [16], Satz 3.6.3).

ii) Der Beweis funktioniert auch im Ring $\mathbb{Z}[x]$, falls wir voraussetzen, dass der Leitkoeffizient b_m von g eine Einheit in $\mathbb{Z}$ ist, d.h. $b_m = \pm 1$.

A.1.7 Aufgabe (Die universelle Eigenschaft des Polynomrings). Beweisen Sie: Es seien R, S Ringe, $\varphi\colon R \longrightarrow S$ ein Homomorphismus und $\alpha \in S$. Dann existiert genau ein Homomorphismus $\widetilde{\varphi}\colon R[x] \longrightarrow S$, so dass

- ⋆ $\forall r \in R : \widetilde{\varphi}(r) = \varphi(r)$,
- ⋆ $\widetilde{\varphi}(x) = \alpha$:



Schreibweise. Wenn $\varphi\colon R \subset S$ eine Inklusion ist, z.B. eine Körpererweiterung, dann sei

$$f(\alpha) := \widetilde{\varphi}(f).$$

A.1.8 Folgerung. *Es seien R ein Körper oder der Ring der ganzen Zahlen und $f \in R[x]$ ein Polynom vom Grad $n \geq 1$. Falls $\alpha \in R$ eine Nullstelle von f ist, d.h. $f(\alpha) = 0$, dann existiert ein Polynom $q \in R[x]$ vom Grad $n - 1$ mit*

$$f = (x - \alpha) \cdot q.$$

Beweis. Wir führen gemäß Satz A.1.5 und Bemerkung A.1.6, ii), die Division von f durch $g := x - \alpha$ durch. Es gibt dann eine Zahl $r = c_0 \in R$, so dass

$$f = (x - \alpha) \cdot q + c_0.$$

Es folgt, dass

$$c_0 = f(\alpha) - (\alpha - \alpha) \cdot q(\alpha) = 0.$$

Das zeigt die Behauptung. □

A.1.9 Folgerung. *Es seien k ein Körper, $n \in \mathbb{N}_+$ eine positive ganze Zahl und $f \in k[x]$ ein Polynom vom Grad n, d.h.*

$$f = a_0 + a_1 \cdot x + \cdots + a_{n-1} \cdot x^{n-1} + a_n \cdot x^n$$

mit $a_i \in k$, $i = 0, ..., n$, und $a_n \neq 0$. Dann hat f höchstens n verschiedene Nullstellen in k.

Beweis. Übung. □

A.2 Irreduzible Polynome und der Satz von Gauß

A.2.1 Definition. Es seien R ein Ring und $R[x]$ der Polynomring in der Unbestimmten x über R.

i) Ein vom Nullpolynom verschiedenes Polynom $f \in R[x] \setminus \{0\}$ ist *reduzibel*, wenn es Polynome $g, h \in R[x] \setminus R^\star$ mit

$$f = g \cdot h \tag{A.1}$$

gibt. Wenn f nicht reduzibel ist, dann nennt man f *irreduzibel*.

ii) Es seien $f, g \in R[x]$ Polynome. Wir sagen, f *teilt* g, wenn ein Polynom $h \in R[x]$ mit

$$g = f \cdot h$$

existiert.

Schreibweise. $f|g$.

A.2.2 Bemerkung. Es sei R ein Körper. Dann gilt

$$0 < \mathrm{Grad}(g), \mathrm{Grad}(h) < \mathrm{Grad}(f)$$

in (A.1). Für $\mathbb{Z}$ ist z.B. das Polynom

$$2 \cdot x + 2 = 2 \cdot (x + 1)$$

reduzibel, denn $2 \notin \mathbb{Z}^\star$ und $x + 1 \notin \mathbb{Z}^\star$.

A.2.3 Definition. Ein Polynom

$$f(x) = a_0 + a_1 \cdot x + \cdots + a_n \cdot x^n \in \mathbb{Z}[x]$$

ist *primitiv*, wenn $f \neq 0$ und seine Koeffizienten keinen gemeinsamen Teiler haben:

$$(f \neq 0) \wedge (\forall p \text{ Primzahl} \exists k \in \{0, ..., n\} : \quad p \nmid a_k).$$

A.2.4 Lemma (Gauß). *Es seien $f, g \in \mathbb{Z}[x]$ primitive Polynome. Dann ist auch das Polynom $f \cdot g \in \mathbb{Z}[x]$ primitiv.*

Beweis. Für ein Polynom $h = c_0 + c_1 \cdot x + \cdots + c_n \cdot x^n \in \mathbb{Z}[x]$ und eine Primzahl p definieren wir

$$[h]_p := [c_0]_p + [c_1]_p \cdot x + \cdots + [c_n]_p \cdot x^n \in \mathbb{Z}_p[x].$$

Man beachte:

- ⋆ Die Abbildung

$$\begin{array}{rccc} [\cdot]_p \colon & \mathbb{Z}[x] & \longrightarrow & \mathbb{Z}_p[x] \\ & h & \longmapsto & [h]_p \end{array}$$

  ist ein Ringhomomorphismus. (Übung.)

- ⋆ Das Polynom h ist genau dann primitiv, wenn $[h]_p \neq 0$ für jede Primzahl p gilt.

Für jede Primzahl p gilt also $[f]_p \neq 0$ und $[g]_p \neq 0$. Da $\mathbb{Z}_p$ ein Körper ist (Satz III.2.8), gilt nach Lemma A.1.3, ii), auch

$$[f \cdot g]_p = [f]_p \cdot [g]_p \neq 0,$$

und wir erkennen, dass $f \cdot g$ primitiv ist. □

Wir betrachten die Ringinklusion $\mathbb{Z}[x] \subset \mathbb{Q}[x]$. Für Polynome $f, g \in \mathbb{Z}[x]$ können wir die Fragen, ob das Polynom f das Polyom g teilt oder ob das Polynom f irreduzibel ist, sowohl in $\mathbb{Z}[x]$ als auch in $\mathbb{Q}[x]$ stellen. Eine bemerkenswerte Beobachtung von Gauß besagt, dass das für ein primitives Polynom f keinen Unterschied macht:

A.2.5 Satz (Gauß). *Es seien $f, g \in \mathbb{Z}[x]$ Polynome, und f sei primitiv.*
i) *Das Polynom f teilt das Polynom g genau dann in $\mathbb{Z}[x]$, wenn es dies in $\mathbb{Q}[x]$ tut.*
ii) *Das Polynom f ist genau dann als Polynom in $\mathbb{Z}[x]$ irreduzibel, wenn es als Polynom in $\mathbb{Q}[x]$ irreduzibel ist.*

Beweis. i) Wenn $f|g$ in $\mathbb{Z}[x]$ gilt, dann haben wir offenbar auch $f|g$ in $\mathbb{Q}[x]$.

Nun gebe es ein Polynom $h \in \mathbb{Q}[x]$, so dass $g = f \cdot h$. Es gibt dann ganze Zahlen $r, s > 0$, so dass

- ⋆ $h' = \frac{r}{s} \cdot h \in \mathbb{Z}[x]$,
- ⋆ h' primitiv ist,
- ⋆ $\text{ggT}(r, s) = 1$.

Nach dem Lemma von Gauß A.2.4 ist das Polynom $f \cdot h'$ primitiv. Die Gleichung

$$r \cdot g = s \cdot f \cdot h'$$

zeigt wegen $\mathrm{ggT}(r, s) = 1$, dass r alle Koeffizienten von $f \cdot h'$ teilt und deshalb $r = 1$ gilt. Dies wiederum impliziert $h = s \cdot h' \in \mathbb{Z}[x]$.

ii) Da f primitiv ist, impliziert die Irreduzibilität von f in $\mathbb{Q}[x]$ die Irreduzibilität von f in $\mathbb{Z}[x]$ (vgl. Bemerkung A.2.2). Jetzt setzen wir voraus, dass f als Element von $\mathbb{Z}[x]$ irreduzibel ist. Weiter seien $g, h \in \mathbb{Q}[x]$ Polynome mit $0 < \mathrm{Grad}(g), \mathrm{Grad}(h) < \mathrm{Grad}(f)$, so dass

$$f = g \cdot h.$$

Wie im Beweis von Teil i) sei $q > 0$ eine rationale Zahl, für die $h' = q \cdot h$ ein primitives Polynom in $\mathbb{Z}[x]$ ist. Da $\mathbb{Q}$ ein Körper ist, teilt auch h' das Polynom f in $\mathbb{Q}[x]$. Teil i) zeigt nun, dass $h' | f$ auch in $\mathbb{Z}[x]$ gilt. Das widerspricht aber der Voraussetzung, dass $f \in \mathbb{Z}[x]$ irreduzibel ist. □

Literaturhinweise

[1] I. Agricola, Th. Friedrich, *Elementargeometrie*, Fachwissen für Studium und Mathematikunterricht, 3. überarb. Aufl., Studium: Mathematik für das Lehramt, Wiesbaden: Vieweg+Teubner, 2011, xii+226 S. ISBN 978-3-8348-1385-5/pbk.

[2] M.A. Armstrong, *Groups and symmetry*, Undergraduate Texts in Mathematics, New York etc.: Springer-Verlag, 1983, xi+186 S.

[3] G. Cornell, J.H. Silverman, G. Stevens (Herausgg.), *Modular forms and Fermat's last theorem*, Papers from the Instructional Conference on Number Theory and Arithmetic Geometry held at Boston University, Boston, MA, August 9-18, 1995, Springer-Verlag, New York, 1997, xx+582 S. ISBN: 0-387-94609-8; 0-387-98998-6.

[4] R. Elwes, *An Enormous Theorem: the classification of finite simple groups*, http://plus.maths.org/content/os/issue41/features/elwes/index.

[5] G. Fischer, *Lineare Algebra. Eine Einführung für Studienanänger*, 16. überarb. und erw. Aufl., Vieweg Studium: Grundkurs Mathematik, Wiesbaden: Vieweg, 2008, xxii+384 S. ISBN 978-3-8348-0428-0.

[6] O. Forster, *Einführung in die Zahlentheorie*, Vorlesungsskript, www.mathematik.uni-muenchen.de/~forster/v/zth/noteszth.html.

[7] C.F. Gauß, *Arithmetische Untersuchungen*, AMS Chelsea Publishing.

[8] V.E. Hill, *Groups, representations, and characters*, New York: Hafner Press, London: Collier Macmillan Publishers, 1975, x+182 S.

[9] N. Hoffmann, *Kryptographie*, Vorlesungsskript, http://userpage.fu-berlin.de/~nhoffman/.

[10] I. Izmestiev, *Einführung in die Konvexgeometrie*, Vorlesungsskript, http://page.math.tu-berlin.de/~izmestie/Teaching/ConvGeom.pdf

[11] C. Jordan, D. Jordan, *Groups*, Modular Mathematics Series, Butterworth–Heinemann, 1994, 224 S.

[12] E. Kunz, *Algebra*, 2. überarb. Aufl., Wiesbaden: Vieweg, 1994, ix+254 p.

[13] S. Lang, *Algebra*, 3. überarb. Aufl., Graduate Texts in Mathematics, Band 211, New York, NY: Springer, 2002, xv+914 S.

[14] St. Müller-Stach, J. Piontkowski, *Elementare und algebraische Zahlentheorie. Ein moderner Zugang zu klassischen Themen*, 2. Aufl., Wiesbaden: Vieweg+Teubner, 2011, 261 S.

[15] P. Ribenboim, *Die Welt der Primzahlen. Geheimnisse und Rekorde*, 2. überarb. und erg. Aufl., Springer-Lehrbuch, Berlin: Springer, 2011, xxv+366 S.

[16] A. Schmitt, *Analysis* I, Vorlesungsskript, `http://userpage.fu-berlin.de/~aschmitt`.

[17] A. Schmitt, *Analysis* II, Vorlesungsskript, `http://userpage.fu-berlin.de/~aschmitt`.

[18] A. Schmitt, *Analysis* III, Vorlesungsskript, `http://userpage.fu-berlin.de/~aschmitt`.

[19] R.-H. Schulz, *Elementargeometrie*, Vorlesungsskript, `http://page.mi.fu-berlin.de/rhschulz/Elgeo-Skript/elgeo.html`

[20] V. Schulze, *Lineare Algebra*, Vorlesungsskript, `http://page.mi.fu-berlin.de/klarner/lina_skript.pdf`

[21] R. Taylor, A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. **141** (1995), 553-72.

[22] F. Toenniessen, *Das Geheimnis der transzendenten Zahlen. Eine etwas andere Einführung in die Mathematik*, Spektrum Sachbuch, Heidelberg: Spektrum Akademischer Verlag, 2010, xiii+434 S.

[23] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. **141** (1995), 443-551.

[24] G.M. Ziegler, *Lectures on polytopes*, Graduate Texts in Mathematics, 152, Springer-Verlag, New York, 1995, x+370 S.

Stichwortverzeichnis