Einführung in die Algebra und Zahlentheorie

Vorlesungsmanuskript WS 2010/11

Janko Böhm

30. November 2012

Inhaltsverzeichnis

Abbildungsverzeichnis

List of Symbols

0

Einleitung

Algebra und Zahlentheorie sind eng verknüpfte Teilgebiete der reinen Mathematik, neben Analysis, Geometrie und Topologie.

Was ist Zahlentheorie? Wie der Name schon verrät beschäftigen sich die Zahlentheoretiker mit den Eigenschaften von Zahlen $(..., -1, 0, 1, 2, 3, ...)$, insbesondere mit der Beziehung zwischen der Addition und der Multiplikation. Viele zahlentheoretische Probleme können sehr einfach formuliert, aber nur sehr schwer gelöst werden, das bekannteste Beispiel ist sicherlich Fermats letzter Satz von 1637: Es gibt keine (nichttriviale) ganzzahlige Lösung der Gleichung

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

für $n \geq 3$. Ein anderes Beispiel ist die Vermutung, dass es unendlich viele Primzahlzwillinge gibt, d.h. Primzahlen p, sodass auch $p+2$ eine Primzahl ist. Fermats letzter Satz wurde erst 1995 (von A. Wiles) bewiesen nach 350-jährigen Vorarbeiten, bei denen viele neue Konzepte in der Mathematik entwickelt wurden. Heute bestehen enge Beziehungen der Zahlentheorie zur algebraischen Geometrie, Darstellungstheorie, Kombinatorik, Kryptographie und Kodierungstheorie.

Was ist Algebra? Die Algebra ist ein weites Gebiet der Mathematik, das sich mit für alle Bereiche der Mathematik grundlegenden algebraischen Strukturen, wie Gruppen, Ringen und Körpern beschäftigt, d.h. mit der Frage wie man auf Mengen Verknüpfungen einführen kann, wie z.B. die Addition und Multiplikation von ganzen Zahlen. Wichtige Berührungsbereiche bestehen neben der Zahlentheorie mit der algebraischen Geometrie.

Diese beschäftigt sich mit den Lösungsmengen von polynomialen Gleichungssystemen in mehreren Variablen über Körpern. Das einfachste Beispiel sind lineare Gleichungssysteme

$$Ax = b$$

mit $A \in K^{n \times m}$, $b \in K^n$ (K ein Körper) nach dem Vektor $x \in K^m$, das Kernthema der linearen Algebra. Ein anderer Spezialfall sind Polynomgleichungen höheren Grades in einer einzigen Variablen x. Zum Beispiel kann man nach der Lösungsmenge der quadratischen Gleichung

$$f(x) = ax^2 + bx + c = 0$$

fragen. Diese kann man mit Wurzeln darstellen durch

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Sind a, b, c Elemente eines Körpers K beschäftigt sich die Algebra mit der Frage wie man K erweitern muss, um x darstellen zu können. Insbesondere kann man sich fragen, ob es vergleichbare Wurzelausdrücke auch für f von Grad $d > 2$ gibt. Die Anwort ist ja für $d = 3$ (Tartaglia 1535, Cardano 1545) und $d = 4$ (Ferrari 1522) und nein für $d \geq 5$. Wenn wir diese Frage auch hier nicht komplett beantworten können, werden wir doch alle wichtigen Grundlagen hierfür behandeln.

1

Zahlen

In diesem Abschnitt beschäftigen wir uns mit wesentlichen Eigenschaften der ganzen Zahlen. Alle diese Eigenschaften werden wir in allgemeinerem Kontext später auch für andere Ringe kennenlernen.

1.1 Die ganzen Zahlen

Die **natürlichen Zahlen** sind

$$\mathbb{N} = \{1, 2, 3, ...\}$$

die **ganzen Zahlen**

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

und wir schreiben $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$.

Auf $\mathbb{N}$ gibt es Verknüpfungen $+$ und $\cdot$, die den Assoziativ-, Kommutativ- und Distributivgesetzen gehorchen

$$\begin{aligned} a + (b + c) &= (a + b) + c & a + b &= b + a \\ a \cdot (b \cdot c) &= (a \cdot b) \cdot c & a \cdot b &= b \cdot a \\ a \cdot (b + c) &= a \cdot b + a \cdot c \end{aligned}$$

für alle $a, b, c \in \mathbb{N}$. Auf die axiomatische Definition der natürlichen Zahlen wollen wir hier nicht weiter eingehen. Als Übungsaufgabe informiere man sich in Buch oder Suchmaschine der Wahl über die Peano-Axiome.

Bemerkung 1.1.1 *Es ist*

$$\mathbb{Z} = (\mathbb{N}_0 \times \mathbb{N}_0) / \sim$$

mit der Äquivalenzrelation

$$(a,b) \sim (c,d) \Leftrightarrow a + d = b + c$$

und die Äquivalenzklasse

$$[(a,b)] = \{(c,d) \mid (c,d) \sim (a,b)\}$$

repräsentiert die ganze Zahl $a - b$. Es gibt Verknüpfungen $+$ und $\cdot$ auf $\mathbb{Z}$

$$\begin{aligned}[(a,b)] + [(c,d)] &= [(a + c, b + d)] \\ [(a,b)] \cdot [(c,d)] &= [(a \cdot c + b \cdot d, a \cdot d + b \cdot c)]\end{aligned}$$

die den Assoziativ-, Kommutativ- und Distributivgesetzen gehorchen. Weiter ist

$$\begin{aligned}[(0,0)] + [(a,b)] &= [(a,b)] \\ [(1,0)] \cdot [(a,b)] &= [(a,b)]\end{aligned}$$

Eine Menge mit solchen Verknüpfungen nennt man kommutativen Ring mit 1. Mit Ringen werden wir uns ausführlich in Kapitel 3 beschäftigen.

Siehe auch Übung 1.1.
Die ganzen Zahlen sind angeordnet durch $\leq$.

Lemma 1.1.2 (Division mit Rest) *Sind $a, b \in \mathbb{Z}$, $b \neq 0$, dann gibt es $q, r \in \mathbb{Z}$ mit*

$$a = b \cdot q + r$$

mit $0 \leq r < |b|$.

Beweis. Ohne Einschränkung ist $b > 0$. Die Menge

$$\{w \in \mathbb{Z} \mid b \cdot w > a\} \neq \varnothing$$

hat ein kleinstes Element w. Setze dann

$$q := w - 1 \qquad r := a - qb$$

■

Definition 1.1.3 *Seien $a, b \in \mathbb{Z}$. Man sagt b* ***teilt*** *a*

$$b \mid a$$

wenn es ein $q \in \mathbb{Z}$ gibt mit $a = b \cdot q$.

Zwei Zahlen $a, b \in \mathbb{Z}$ heißen ***teilerfremd****, wenn für $t \in \mathbb{N}$ mit $t \mid a$ und $t \mid b$ folgt $t = 1$.*

Sei $m \in \mathbb{N}$ und $a, b \in \mathbb{Z}$. Dann heißt a ***kongruent*** *zu b modulo m*

$$a \equiv b \bmod m$$

wenn $m \mid (a - b)$.

Kongruent modulo m zu sein ist eine Äquivalenzrelation, siehe auch Übungsaufgabe 1.2. Wir schreiben auch $a \equiv_m b$.

1.2 Fundamentalsatz der Arithmetik

Definition 1.2.1 *Ein Element $p \in \mathbb{Z}_{>1}$ heißt* ***Primzahl****, wenn aus $p = a \cdot b$, $a, b \in \mathbb{Z}_{\geq 1}$ folgt $a = 1$ oder $b = 1$.*

Satz 1.2.2 (Fundamentalsatz der Arithmetik) *Jede Zahl $n \in \mathbb{Z} \setminus \{0, 1, -1\}$ hat eine eindeutige Darstellung*

$$n = \pm 1 \cdot p_1^{r_1} \cdot \ldots \cdot p_r^{r_r}$$

mit Primzahlen $p_1 < \ldots < p_r$ und $r_i \in \mathbb{N}$. Die p_i heißen ***Primfaktoren*** *von n.*

Beweis. Existenz mit Induktion nach n:

$n = 2$ ist eine Primzahl. Ist $n > 2$ und keine Primzahl, dann ist $n = a \cdot b$ mit $a, b \neq 1$. Da $a, b < n$, haben a und b eindeutige Zerlegungen, und durch Sortieren der Primfaktoren erhalten wir die Darstellung von n.

Eindeutigkeit:

$n = 2$ ist klar. Ist $n > 2$ und

$$n = p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s$$

mit $p_1 \leq \ldots \leq p_r$ und $q_1 \leq \ldots \leq q_s$. Ist $r = 1$ oder $s = 1$, dann ist n prim, und die Behauptung ist klar.

Ist $p_1 = q_1$ dann ist $p_2 \cdot \ldots \cdot p_r = q_2 \cdot \ldots \cdot q_s$ und

$$p_2 \cdot \ldots \cdot p_r = q_2 \cdot \ldots \cdot q_s < n$$

hat nach Induktionsvoraussetzung eine eindeutige Primfaktorzerlegung und die Behauptung folgt.

Angenommen es wäre $p_1 < q_1$. Dann hat

$$n > p_1 \cdot (p_2 \cdot \ldots \cdot p_r - q_2 \cdot \ldots \cdot q_s) = (q_1 - p_1) \cdot q_2 \cdot \ldots \cdot q_s \geq 2$$

nach Induktionsvoraussetzung eine eindeutige Primfaktorzerlegung. Wegen $p_1 < q_1 \leq \ldots \leq q_s$ ist $p_1 \neq q_i$, und p_1 ist kein Teiler von $q_1 - p_1$, denn sonst würde p_1 auch q_1 teilen. Somit ist p_1 ein Primfaktor der linken Seite, jedoch keiner der rechten Seite, ein Widerspruch. ■

Aus der Eindeutigkeit der Primfaktorzerlegung folgt:

Corollar 1.2.3 (Euklids erster Satz) *Ist $p \in \mathbb{Z}$ prim und $a, b \in \mathbb{Z}$ mit $p \mid ab$, dann $p \mid a$ oder $p \mid b$.*

Satz 1.2.4 (Euklids zweiter Satz) *Es gibt unendlich viele Primzahlen.*

Beweis. Sei $M = \{p_1, \ldots, p_r\}$ eine endliche Menge von Primzahlen. Wir zeigen, dass es eine Primzahl gibt, die nicht in M enthalten ist. Die Zahl $N = p_1 \cdot \ldots \cdot p_r + 1$ ist durch keine der Primzahlen p_i teilbar, denn sonst wäre auch 1 durch p_i teilbar. Ein Primfaktor p von N ist also eine Primzahl, die nicht in M liegt. ■

Für einen anderen Beweis von Euler siehe auch Übungsaufgabe 1.3 und Bemerkung 1.2.6.

Satz 1.2.5 (Primzahlsatz) *Sei für $x \in \mathbb{R}_{>0}$*

$$\pi(x) = |\{p \leq x \mid p \in \mathbb{N} \text{ prim}\}|$$

dann gilt

$$\lim_{x \to \infty} \frac{\pi(x)}{\frac{x}{\ln(x)}} = 1$$

Ohne Beweis. Wie wir auch in Übung 1.5 sehen werden, gibt es bessere Approximationen für $\pi(x)$.

Bemerkung 1.2.6 *Wir skizzieren einen anderen Beweis von Euklids zweitem Satz, der auf Euler zurückgeht. Die* ***Riemannsche Zetafunktion*** *ist gegeben durch die für* $s \in \mathbb{C}$, $\mathrm{Re}(s) > 1$ *absolut konvergente und für* $s = 1$ *divergente Reihe*

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

Das unendliche Produkt

$$\prod_{p \ prim} \frac{1}{1 - \frac{1}{p^s}}$$

konvergiert ebenfalls für $\mathrm{Re}(s) > 1$, *also ist es nach dem großen Umordnungssatz für absolut konvergente Reihen gleich* $\zeta(s)$. *Wäre die Menge der Primzahlen endlich, dann würde* $\sum_{n=1}^{\infty} \frac{1}{n}$ *konvergieren.*

Riemann zeigte, dass $\zeta(s)$ *eine meromorphe Fortsetzung auf* $\mathbb{C} \setminus \{1\}$ *besitzt und die Gleichung*

$$\zeta(s) = 2^s \pi^{s-1} \sin\left(\frac{\pi s}{2}\right) \Gamma(1-s)\, \zeta(1-s)$$

(mit der Gamma-Funktion Γ*) erfüllt. Außerhalb des kritischen Streifens* $0 \leq \mathrm{Re}(s) \leq 1$ *ist also* $\zeta(s)$ *direkt durch die konvergente Reihe* $\sum_{n=1}^{\infty} \frac{1}{n^{s'}}$ *mit* $s' = s$ *oder* $s' = 1 - s$ *bestimmt. Die* ***Riemannsche Vermutung*** *besagt, dass sämtliche Nullstellen von* $\zeta(s)$ *im kritischen Streifen* $\mathrm{Re}(s) = \frac{1}{2}$ *haben. Die Richtigkeit der Riemannschen Vermutung ist äquivalent zu*

$$\pi(x) = \mathrm{Li}(x) + O(x^{\frac{1}{2}+\varepsilon}) \ \forall \varepsilon > 0$$

mit dem ***Integrallogarithmus***

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\ln(t)}$$

Zu Primzahlen siehe auch die Übung 1.4 über Mersenne-Primzahlen und Fermat-Zahlen.

1.3 Division mit Rest und Euklidischer Algorithmus

Definition 1.3.1 *Sind $a_1, ..., a_r \in \mathbb{Z}$, dann heißt $d \in \mathbb{N}$* ***größter gemeinsamer Teiler*** *von $a_1, ..., a_r$, geschrieben $d = \mathrm{ggT}(a_1, ..., a_r)$, wenn gilt*

1) *$d \mid a_j \ \forall j = 1, ..., r$, d.h. d ist ein Teiler von allen a_j, und*
2) *ist $\tilde{d} \in R$ ein Teiler aller a_j, d.h. $\tilde{d} \mid a_j \ \forall j = 1, ..., r$, dann gilt $\tilde{d} \mid d$.*

Weiter heißt $m \in \mathbb{N}$ ***kleinstes gemeinsames Vielfaches*** *von $a_1, ..., a_r$, geschrieben $m = \mathrm{kgV}(a_1, ..., a_r)$, wenn gilt*

1) *$a_j \mid m \ \forall j = 1, ..., r$, d.h. m ist ein Vielfaches aller a_j, und*
2) *ist $\tilde{m} \in R$ ein Vielfaches aller a_j, d.h. $a_j \mid \tilde{m} \ \forall j = 1, ..., r$, dann gilt $m \mid \tilde{m}$.*

Schreiben wir

$$a_j = \pm 1 \cdot \prod_{i=1}^{s} p_i^{r_{ji}}$$

mit p_i prim und $r_{ji} \geq 0$, dann ist

$$\mathrm{ggT}(a_1, ..., a_r) = \prod_{i=1}^{s} p_i^{\min_j \{r_{ji}\}} \tag{1.1}$$

(und für kgV analog mit dem Maximum).

Zwei Zahlen $a, b \in \mathbb{Z}$ sind teilerfremd genau dann, wenn

$$\mathrm{ggT}(a, b) = 1$$

Satz 1.3.2 (Euklidischer Algorithmus) *Seien $a_1, a_2 \in \mathbb{Z} \setminus \{0\}$. Dann terminiert die sukzessive Division mit Rest*

$$\begin{aligned} a_1 &= q_1 a_2 + a_3 \\ &\vdots \\ a_j &= q_j a_{j+1} + a_{j+2} \\ &\vdots \\ a_{n-1} &= q_{n-1} a_n + 0 \end{aligned}$$

und

$$\mathrm{ggT}\,(a_1, a_2) = a_n$$

Rückwärtseinsetzen dieser Gleichungen

$$\begin{aligned} a_n &= a_{n-2} - q_{n-2}a_{n-1} \\ &\vdots \\ a_3 &= a_1 - q_1 a_2 \end{aligned}$$

liefert eine Darstellung

$$\mathrm{ggT}\,(a_1, a_2) = x \cdot a_1 + y \cdot a_2$$

mit $x, y \in \mathbb{Z}$.

Beweis. Es ist $|a_{i+1}| < |a_i|$ für $i \geq 2$ und somit muss nach endlich vielen Schritten $a_i = 0$ sein. Es ist a_n ein Teiler von a_{n-1}, also auch von $a_{n-2} = q_{n-2}a_{n-1} + a_n$ und induktiv von $a_{n-2}, ..., a_1$. Ist t ein Teiler von a_1 und a_2, dann auch von $a_3, ..., a_n$. ■

Beispiel 1.3.3 *Wir bestimmen den ggT von* 36 *und* 15 *mit Hilfe des Euklidischen Algorithmus, d.h. durch sukzessive Division mit Rest:*

$$\begin{aligned} 36 &= 2 \cdot 15 + 6 \\ 15 &= 2 \cdot 6 + 3 \\ 6 &= 2 \cdot 3 + 0 \end{aligned}$$

Somit ist $\mathrm{ggT}\,(36, 15) = 3$*, denn von unten gelesen gilt*

$$3 \mid 6 \text{ also } 3 \mid 15 \text{ also } 3 \mid 36$$

und von oben gelesen, ist t *ein Teiler von* 36 *und* 15 *dann*

$$t \mid 36 \text{ und } t \mid 15 \text{ also } t \mid 6 \text{ also } t \mid 3$$

Weiter erhalten wir eine Darstellung von $\mathrm{ggT}\,(36, 15)$ *als* $\mathbb{Z}$*-Linearkombination von* 36 *und* 15.

$$3 = 15 - 2 \cdot 6 = 15 - 2 \cdot (36 - 2 \cdot 15) = 5 \cdot 15 + (-2) \cdot 36$$

1.4 Der chinesische Restsatz

Satz 1.4.1 (Chinesischer Restsatz in $\mathbb{Z}$) *Sind $n_1, ..., n_r \in \mathbb{Z}_{>0}$ paarweise teilerfremd und $a_1, ..., a_r \in \mathbb{Z}$, dann ist die* ***simultane Kongruenz***

$$\begin{aligned} x &\equiv a_1 \bmod n_1 \\ &\vdots \\ x &\equiv a_r \bmod n_r \end{aligned}$$

lösbar. Die Lösung ist eindeutig modulo $n = n_1 \cdot ... \cdot n_r$.

Beweis. Sei

$$\hat{n}_i = \frac{n}{n_i}$$

und finde mit dem erweiterten Euklidischen Algorithmus $x_i, y_i \in \mathbb{Z}$ mit

$$1 = \mathrm{ggT}\,(n_i, \hat{n}_i) = x_i n_i + y_i \hat{n}_i$$

Dann ist

$$\begin{aligned} y_i \hat{n}_i &\equiv 0 \bmod n_j \ \ \forall j \neq i \\ y_i \hat{n}_i &\equiv 1 \bmod n_i \end{aligned}$$

Somit erfüllt

$$x = \sum_{i=1}^{r} a_i y_i \hat{n}_i$$

die Kongruenzen und ebenso $x + k \cdot n$ für alle k. Sind x und x' Lösungen, dann $n_i \mid (x - x') \ \forall i$, also

$$n \mid (x - x')$$

■

Diesen Satz werden wir später wesentlich allgemeiner beweisen.

Beispiel 1.4.2 *Wir lösen die simultane Kongruenz*

$$\begin{aligned} x &\equiv -28 \bmod 30 \\ x &\equiv 5 \bmod 7 \end{aligned}$$

Es ist $\mathrm{ggT}(30,7) = 1$*, also ist die Kongruenz lösbar. Mit dem erweiterten Euklidischen Algorithmus finden wir* $x_1 = y_2$ *und* $y_1 = x_2$ *mit*

$$x_1 30 + y_1 7 = 1$$

z.B. $x_1 = -3$*,* $y_1 = 13$*. Somit*

$$x \equiv (-28)\cdot(13\cdot 7) + 5\cdot(-3\cdot 30) \equiv -2998 \equiv 152 \bmod 210$$

d.h. die Lösungsmenge ist

$$152 + 210\cdot\mathbb{Z} = \{152 + k\cdot 210 \mid k \in \mathbb{Z}\}$$

Satz 1.4.3 *Seien* $a_1, a_2 \in \mathbb{Z}$ *und* $n_1, n_2 \in \mathbb{Z}_{>0}$*. Dann sind die simultanen Kongruenzen*

$$x \equiv a_1 \bmod n_1$$
$$x \equiv a_2 \bmod n_2$$

genau dann lösbar, wenn

$$a_1 - a_2 \equiv 0 \bmod \mathrm{ggT}(n_1, n_2)$$

Die Lösung ist eindeutig modulo dem $\mathrm{kgV}(n_1, n_2)$*.*

Dies zeigen wir in Übungsaufgabe 1.8.

1.5 Übungsaufgaben

Übung 1.1 *Zeigen Sie:*

1) *Auf* $M = \mathbb{N}_0 \times \mathbb{N}_0$ *ist durch*

$$(a,b) \sim (c,d) \Leftrightarrow a + d = b + c$$

eine Äquivalenzrelation gegeben.

2) *Die Verknüpfungen*

$$[(a,b)] + [(c,d)] = [(a+c, b+d)]$$
$$[(a,b)] \cdot [(c,d)] = [(a\cdot c + b\cdot d, a\cdot d + b\cdot c)]$$

auf

$$\mathbb{Z} = (\mathbb{N}_0 \times \mathbb{N}_0) \,/\, \sim$$

sind wohldefiniert. Mit der Identifikation $a - b = [(a,b)]$ *entsprechen diese den bekannten Rechenregeln für ganze Zahlen.*

3) $(\mathbb{Z}, +)$ *ist eine abelsche Gruppe mit neutralem Element* $0 = [(0,0)]$ *und*

$$-[(a,b)] = [(b,a)]$$

4) $(\mathbb{Z}\backslash\{0\}, \cdot)$ *ist ein Monoid mit neutralem Element* $1 = [(1,0)]$.

5) *Es gilt das Distributivgesetz.*

Zum Gruppenbegriff siehe Abschnitt 2.2.1.

Übung 1.2 *Sei* $m \in \mathbb{N}$ *und* $a, b \in \mathbb{Z}$. *Dann heißt* a *kongruent zu* b *modulo* m

$$a \equiv b \bmod m$$

wenn $m \mid (a-b)$. *Zeigen Sie, dass "modulo* m *kongruent sein" eine Äquivalenzrelation ist.*

Übung 1.3 *Sei* $P = \{p_1, ..., p_k\}$ *eine endliche Menge von Primzahlen. Zeigen Sie*

$$\prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)^{-1} = \sum_{m \in M} \frac{1}{m}$$

mit

$$M = \{m \in \mathbb{Z}_{\geq 1} \mid m \text{ hat nur Primfaktoren in } P\}$$

Folgern Sie, dass es unendlich viele Primzahlen gibt (Eulers Beweis).

Übung 1.4 *Zeigen Sie:*

1) *Ist* $r \in \mathbb{N}$ *und* $p = 2^r - 1$ *prim, dann ist* r *prim.*

2) *Ist* $r \in \mathbb{N}$ *und* $p = 2^r + 1$ *prim, dann ist* $r = 2^k$ *mit* $k \in \mathbb{N}_0$.

Übung 1.5 *Überprüfen Sie den Primzahlsatz experimentell in Maple (siehe [10]):*

1) *Schreiben Sie eine Prozedur, die*

$$\pi(x) = |\{p \leq x \mid p \in \mathbb{N} \text{ prim}\}|$$

für $x > 0$ *berechnet.*

2) *Vergleichen Sie* $\frac{\pi(x)}{x}$ *mit* $\rho_a :]e^a, \infty[\to \mathbb{R}$, $\rho_a(x) = \frac{1}{\ln(x)-a}$ *für* $a \in \mathbb{Z}_{\geq 0}$, *insbesondere für große* x. *Für welches* a *erhalten Sie die beste Approximation?*

3) *Vergleichen Sie* $\pi(x)$ *mit dem Integrallogarithmus* $\mathrm{Li} : [2, \infty[\to \mathbb{R}$,

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\ln(t)}$$

4) *Für* $x \in \mathbb{R}$ *sei* p_x *die kleinste Primzahl* $p_x \geq x$. *Erstellen Sie für* $x \in \{10^6, ..., 10^{50}\}$ *eine Statistik über die Werte*

$$\frac{p_x - x}{\ln x}$$

Hinweis: Verwenden Sie die Maple-Funktion nextprime.

Übung 1.6 *Sei* P_N *die Wahrscheinlichkeit, dass zufällig gewählte natürliche Zahlen* $n, m \leq N$ *teilerfremd sind.*

1) *Bestimmen Sie* P_N *für* $N = 10^6, 10^{12}$ *und* 10^{18} *approximativ durch Stichproben im Umfang von jeweils* 10^2, 10^4 *und* 10^6 *Versuchen mit Hilfe eines Computeralgebrasystems.*

2) *Zeigen Sie, dass für den Grenzwert gilt*

$$\lim_{N \to \infty} P_N = \frac{6}{\pi^2} \approx 60.7\%$$

Hinweis: Verwenden Sie ohne Beweis die Formel

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{1}{6}\pi^2$$

die man z.B. mit Hilfe von Fourierreihen beweisen kann.

Übung 1.7 *Kürzen Sie*

$$\frac{90189116021}{18189250063}$$

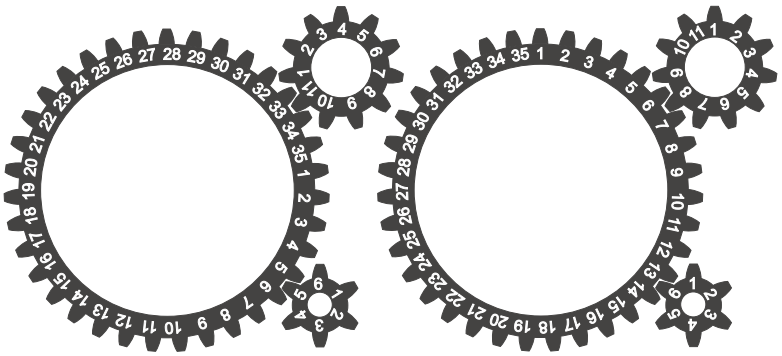


Abbildung 1.1: Zwei Konfigurationen von drei Zahnrädern

Übung 1.8 *Seien $a_1, a_2 \in \mathbb{Z}$ und $n, m \in \mathbb{Z}_{>0}$. Zeigen Sie: Die simultanen Kongruenzen*

$$x \equiv a_1 \bmod n_1$$
$$x \equiv a_2 \bmod n_2$$

sind genau dann lösbar, wenn

$$a_1 - a_2 \equiv 0 \bmod \mathrm{ggT}\,(n_1, n_2)$$

Die Lösung ist eindeutig modulo dem $\mathrm{kgV}\,(n_1, n_2)$.

Übung 1.9 *Lassen sich die beiden Konfigurationen von Zahnrädern in Abbildung 1.1 durch Drehung ineinander überführen? Falls ja, um wieviele Schritte muss man dafür drehen?*

Übung 1.10 *Bestimmen Sie die Menge $L \subset \mathbb{Z}$ aller Lösungen x der simultanen Kongruenzen*

$$x \equiv 1 \bmod 108$$
$$x \equiv 13 \bmod 40$$
$$x \equiv 28 \bmod 225$$

2

Gruppen

2.1 Übersicht

In diesem Kapitel beschäftigen wir uns mit den Grundlagen der Gruppentheorie, die vielfältige Anwendungen in den weiteren Kapiteln über Ringe, Moduln und Körper haben. Als Beispiele für Gruppen betrachten wir Symmetriegruppen von Teilmengen des $\mathbb{R}^n$, z.B. die Mengen der Drehungen und (Dreh-) Spiegelungen, die jeweils einen der Platonischen Körper Tetraeder, Würfel, Oktaeder, Dodekaeder und Ikosaeder (siehe Abbildung 2.1) wieder in sich selbst überführen. Die Gruppeneigenschaft sieht man hier (u.a.) dadurch, dass das Hintereinanderausführen von zwei Symmetrien wieder eine Symmetrie ist und wir jede Symmetrie durch eine andere wieder rückgängig machen können. Zum Beispiel ist in der Symmetriegruppe des Tetraeders die Drehsymmetrie um 120° gleich dem Produkt von zwei Spiegelungen, siehe Abbildung 2.2.

Für Symmetriegruppen spielt der Begriff der Operation einer Gruppe G auf einer Menge M eine wichtige Rolle. Zum Beispiel könnte G die Symmetriegruppe des Tetraeders sein und M der Tetraeder oder die Menge der Eckpunkte, der Kanten oder Seiten des Tetraeders. Eine Gruppenoperation ist eine Abbildung (mit einigen offensichtlichen Zusatzbedingungen)

$$\begin{array}{ccc} G \times M & \longrightarrow & M \\ (g, m) & \longmapsto & g \cdot m \end{array}$$

d.h. ein Gruppenelement g bildet ein Element $m \in M$ auf ein

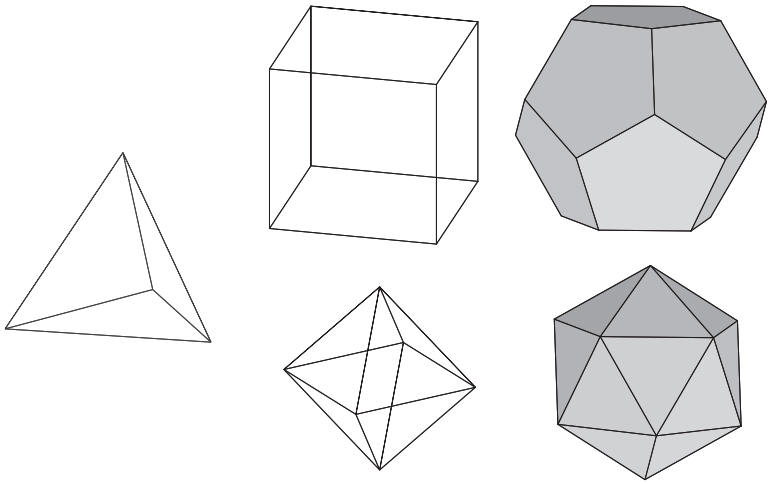


Abbildung 2.1: Die Platonischen Körper

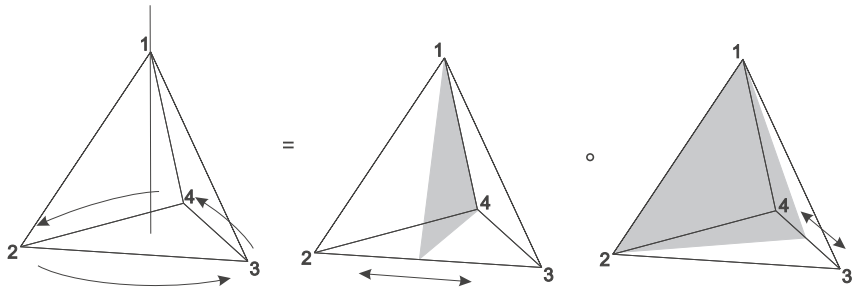


Abbildung 2.2: Komposition von zwei Symmetrien des Tetraeders

anderes Element von M ab, das wir $g \cdot m$ nennen. Starten wir mit einem m und wenden alle Elemente von G an erhalten wir die Bahn von m, zum Beispiel können wir jede Ecke des Tetraeders durch eine Symmetrie auf jede andere Ecke abbilden. Auf diese Weise können wir M in disjunkte Bahnen zerlegen. Als zentralen Satz beweisen wir die Bahnengleichung.

Die beiden wichtigsten Beispiele von Operationen für die Konstruktion und Klassifikation von Gruppen sind jedoch die einer Untergruppe $H \subset G$ durch Translation

$$\begin{array}{ccc} H \times G & \longrightarrow & G \\ (h, g) & \longmapsto & hg \end{array}$$

und von G auf sich selbst durch Konjugation

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (a,b) & \longmapsto & aba^{-1} \end{array}$$

Zur Klassifikation von Gruppen werden wir insbesondere die Sylowsätze beweisen, die wichtige Informationen über die Existenz und Anzahl von Untergruppen einer gegeben Gruppe liefern. Beispielsweise werden wir in diesem Zusammenhang zeigen, dass es zu jedem Primpotenzteiler p^j der Anzahl der Elemente $|G|$ einer Gruppe G eine Untergruppe H gibt $|H| = p^j$.

2.2 Gruppen und Operationen

2.2.1 Grundbegriffe

Definition 2.2.1 *Eine* ***Gruppe*** $(G, \circ)$ *ist eine Menge G zusammen mit einer Verknüpfung*

$$\begin{array}{rccc} \circ: & G \times G & \longrightarrow & G \\ & (a,b) & \mapsto & a \circ b \end{array}$$

die folgende Axiome erfüllt:

(G1) Assoziativität

$$a \circ (b \circ c) = (a \circ b) \circ c \ \forall a, b, c \in G$$

(G2) Es existiert ein neutrales Element, d.h. ein

$$e \in G$$

mit

$$e \circ a = a \circ e = a \ \forall a \in G$$

(G3) Existenz des Inversen, d.h. $\forall a \in G \ \exists a^{-1} \in G$ mit

$$a^{-1} \circ a = a \circ a^{-1} = e$$

Gilt außerdem das Kommutativgesetz

$$a \circ b = b \circ a \ \forall a, b \in G$$

dann heißt G ***abelsch****.*

Eine Menge G zusammen mit einer Verknüpfung

$$\circ : \quad G \times G \quad \longrightarrow \quad G$$

die $(G1)$ erfüllt, nennt man ***Halbgruppe****, $(G, \circ)$ mit $(G1)$ und $(G2)$ heißt* ***Monoid****.*

Die ***Ordnung*** *$|G|$ von G ist die Anzahl der Elemente von G, falls G endlich ist, und sonst ∞.*

Bemerkung 2.2.2 *Setzt man für eine Gruppe G nur die Existenz eines linksneutralen Elements $e \in G$ mit $e \circ a = a \ \forall a \in G$ und von linksinversen Elementen für alle $a \in G$ mit $a^{-1} \circ a = e$ voraus, dann ist e auch rechtsneutral und a^{-1} rechtsinvers.*

1) Für $a, b \in G$ gilt: Ist $ab = e$, dann ist auch $ba = e$.

2) Es ist $a \circ e = a \ \forall a \in G$.

3) Das neutrale Element ist eindeutig.

4) Das Inverse ist eindeutig.

5) Für $a, b \in G$ ist $(ab)^{-1} = b^{-1}a^{-1}$.

6) Für $a \in G$ ist $(a^{-1})^{-1} = a$.

Diese Aussagen zeigen wir in Übung 2.1.

Beispiel 2.2.3 *1) Die Menge der ganzen Zahlen mit der Addition*

$$(\mathbb{Z}, +)$$

ist eine Gruppe.

2) Die Menge der ganzen Zahlen ungleich 0 zusammen mit der Multiplikation

$$(\mathbb{Z} \setminus \{0\}, \cdot)$$

ist ein Monoid.

3) *Ist V ein Vektorraum, dann ist $\mathrm{GL}(V)$ die Menge der Vektorraumautomorphismen von V zusammen mit der Komposition eine Gruppe.*

   Etwa für $V = K^n$ ist $\mathrm{GL}(V) = \mathrm{GL}(n, K)$ die Gruppe der invertierbaren $n \times n$ Matrizen.

4) *Sei X eine beliebige Menge. Die Menge der Selbstabbildungen von X*

$$S(X) = \{f : X \longrightarrow X \mid f \text{ bijektiv}\}$$

   zusammen mit der Komposition ist eine Gruppe.

   Speziell für

$$X = \{1, ..., n\}$$

   ist

$$S_n := S(\{1, ..., n\})$$

   *die Menge der Permutation von n Elementen, d.h. die **symmetrische Gruppe**. Ist $\sigma \in S_n$, dann schreiben wir auch*

$$\sigma = \begin{pmatrix} 1 & \cdots & n \\ \sigma(1) & \cdots & \sigma(n) \end{pmatrix}$$

   *Ein Element von S_n heißt **Transposition**, wenn es genau zwei Elemente von X vertauscht.*

5) *Sei*

$$A = \{\alpha, \beta, \gamma, ...\}$$

   *eine endliche Menge. Ein **Wort** über dem Alphabet A ist eine endliche Folge*

$$w = b_1 b_2 ... b_n$$

   mit $b_i \in A$. Ist $v = a_1 ... a_m$ ein weiteres Wort, dann definiert man die Verknüpfung "Hintereinanderschreiben"durch

$$w \circ v = b_1 ... b_n a_1 ... a_m$$

   Die Menge

$$G = \{w \mid w \text{ ein Wort über } A\}$$

   zusammen mit $\circ$ ist eine Halbgruppe.

   Erlauben wir in G das leere Wort e, dann ist $(G, \circ)$ ein Monoid.

6) *Fügen wir zusätzliche Buchstaben* $\alpha^{-1}, \beta^{-1}, \ldots$ *mit der Rechenregel*

$$\alpha\alpha^{-1} = \alpha^{-1}\alpha = e$$

hinzu, dann erhalten wir die ***freie Gruppe*** *erzeugt von* A.

7) *Sind* G_1, G_2 *Gruppen, dann ist das* ***kartesische Produkt*** $G_1 \times G_2$ *von* G_1 *und* G_2 *mit der Verknüpfung*

$$(a_1, b_1) \circ (a_2, b_2) := (a_1 \circ a_2, b_1 \circ b_2)$$

ebenfalls eine Gruppe.

Definition und Satz 2.2.4 *Sei* $(G, \circ)$ *eine Gruppe. Eine Teilmenge* $H \subset G$ *heißt* ***Untergruppe****, wenn die beiden folgenden äquivalenten Bedingungen erfüllt sind*

1) $a, b \in H \Longrightarrow a \circ b \in H$, $b^{-1} \in H$ *und* $e \in H$

2) $H \neq \varnothing$ *und* $a, b \in H \Longrightarrow a \circ b^{-1} \in H$.

Beweis. (1.) $\Rightarrow$ (2.) ist klar. Ist umgekehrt $H \neq \varnothing$, dann gibt es ein $a \in H$. Für dieses gilt $e = a \circ a^{-1} \in H$ und somit $a^{-1} = e \circ a^{-1} \in H$. Also für $a, b \in H$ gilt $a, b^{-1} \in H$, also

$$a \circ b = a \circ \left(b^{-1}\right)^{-1} \in H$$

■

Beispiel 2.2.5 *Die Menge der invertierbaren Matrizen mit Determinante* 1

$$\mathrm{SL}(n, K) = \{A \in \mathrm{GL}(n, K) \mid \det A = 1\}$$

ist eine Untergruppe von $\mathrm{GL}(n, K)$*, die* ***spezielle lineare Gruppe****.*

Beispiel 2.2.6 *Die Untergruppen von* $(\mathbb{Z}, +)$ *haben die Gestalt*

$$n\mathbb{Z} := \{n \cdot k \mid k \in \mathbb{Z}\}$$

wobei $n \in \mathbb{Z}_{\geq 0}$.

Beweis. $H \subset \mathbb{Z}$ sei eine Untergruppe. Entweder gilt $H = \{0\}$ oder es gibt ein kleinstes Element $n > 0$ in H. Wir zeigen, dass dann $H = n\mathbb{Z}$ gilt: Sei $m \in H$. Division mit Rest liefert eine Darstellung

$$m = qn + r$$

mit $0 \leq r < n$ und $r \in H$. Nach der Definition von n folgt $r = 0$, also $m \in n\mathbb{Z}$. ■

Beispiel 2.2.7 *Sei $n \in \mathbb{N}$. Für $a \in \mathbb{Z}$ heißt die Äquivalenzklasse von a modulo n (siehe auch Übungsaufgabe 1.2)*

$$\begin{aligned}\overline{a} &= \{b \in \mathbb{Z} \mid a \equiv b \bmod n\} \\ &= a + n\mathbb{Z} := \{a + k \cdot n \mid k \in \mathbb{Z}\} \subset \mathbb{Z}\end{aligned}$$

***Restklasse** von a modulo n . Dann ist*

$$\mathbb{Z}_n := \mathbb{Z}/n := \left\{\overline{0}, \overline{1}, \overline{2}, ..., \overline{n-1}\right\}$$

mit

$$\overline{a} + \overline{b} = \overline{a+b}$$

*eine Gruppe, die **Gruppe der Restklassen modulo n**. Ist d ein Teiler von n und $a = \frac{n}{d}$, dann ist*

$$\mathbb{Z}/d \cong \left\{\overline{0}, \overline{a}, \overline{2a}, ...\right\} \subset \mathbb{Z}/n$$

eine Untergruppe.

Die Identifikation der Untergruppe mit $\mathbb{Z}/d$ ist ein Gruppenisomorphismus:

Definition 2.2.8 *Ein **Gruppenhomomorphismus** φ zwischen zwei Gruppen G_1 und G_2 ist eine Abbildung*

$$\varphi : G_1 \longrightarrow G_2$$

die

$$\varphi(ab) = \varphi(a)\,\varphi(b) \quad \forall a, b \in G_1$$

erfüllt, also die Verknüpfungsstruktur erhält.

Bemerkung 2.2.9 *Für einen Gruppenhomomorphismus* $\varphi : G_1 \longrightarrow G_2$ *gilt*

$$\varphi(e_1) = e_2$$

wobei $e_i \in G_i$ *jeweils das neutrale Element bezeichnet.*

Der ***Kern*** *von* φ

$$\ker \varphi = \{a \in G_1 \mid \varphi(a) = e_2\}$$

und das ***Bild*** *von* φ

$$\operatorname{Im} \varphi = \{b \in G_2 \mid b \in \varphi(G_1)\}$$

sind Untergruppen von G_1 *bzw.* G_2.

Siehe auch Übung 2.2.

Lemma 2.2.10 *Ein Gruppenhomomorphismus* $\varphi : G_1 \longrightarrow G_2$ *ist injektiv genau dann, wenn der Kern*

$$\ker \varphi = \{e_1\}$$

nur das neutrale Element e_1 *von* G_1 *enthält.*

Beweis. Für $a, b \in G_1$ gilt

$$\varphi(a) = \varphi(b) \Longleftrightarrow \varphi\left(ab^{-1}\right) = e_2 \Longleftrightarrow ab^{-1} \in \ker \varphi$$

also

$$\ker \varphi = \{e_1\} \Rightarrow \{\varphi(a) = \varphi(b) \Longrightarrow a = b\}$$

Ist umgekehrt φ injektiv, dann folgt aus

$$\varphi(a) = e_2 = \varphi(e_1)$$

dass $a = e_1$. ■

Definition 2.2.11 *Injektive Gruppenhomomorphismen nennt man auch (Gruppen-)* ***Monomorphismen****, surjektive Gruppenhomomorphismen (Gruppen-)* ***Epimorphismen****.*

Ein ***Isomorphismus*** $\varphi : G_1 \longrightarrow G_2$ *von Gruppen ist ein bijektiver Homomorphismus. Die Umkehrabbildung*

$$\varphi^{-1} : G_2 \longrightarrow G_1$$

ist dann ebenfalls ein Homomorphismus. Wir schreiben auch $G_1 \cong G_2$.

Siehe auch Übung 2.2.

Beispiel 2.2.12 *1) Die Inklusion einer Untergruppe $H \hookrightarrow G$ ist ein Monomorphismus.*

2) Die Abbildung

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & n\mathbb{Z} \\ k & \longmapsto & n \cdot k \end{array}$$

ist ein Isomorphismus.

3) Die Abbildung

$$\begin{array}{ccc} (\mathbb{R}, +) & \longrightarrow & (\mathbb{R}_{>0}, \cdot) \\ x & \longmapsto & \exp(x) = e^x \end{array}$$

ist ein Isomorphismus.

4) Im Gegensatz dazu ist

$$\begin{array}{ccc} (\mathbb{C}, +) & \longrightarrow & (\mathbb{C}^*, \cdot) \\ z & \longmapsto & \exp(z) = e^z \end{array}$$

zwar ein Epimorphismus, aber kein Isomorphismus. Der Kern ist

$$\ker(\exp : \mathbb{C} \longrightarrow \mathbb{C}^*) = 2\pi i\mathbb{Z} := \{2\pi i n \mid n \in \mathbb{Z}\}$$

*5) Sei $n \geq 2$. Die **Signatur** oder das **Signum***

$$\begin{array}{rccc} \operatorname{sign}: & S_n & \longrightarrow & (\{\pm 1\}, \cdot) \\ & \sigma & \longmapsto & \operatorname{sign}(\sigma) = \prod\limits_{\substack{i,j=1 \\ i<j}}^{n} \frac{\sigma(i)-\sigma(j)}{i-j} \end{array}$$

ist ein Epimorphismus und

$$\ker(\operatorname{sign}) = A_n$$

*heißt die **alternierende Gruppe**.*

Siehe auch Übungsaufgabe 2.3.

6) Sei $G = \mathrm{GL}(n, K)$. *Dann ist*

$$\det : G \longrightarrow (K^*, \cdot)$$

ein Gruppenhomomorphismus und

$$\ker(\det) = \mathrm{SL}(n, K)$$

7) Mit der Gruppe μ_n *der* n*-ten Einheitswurzeln*

$$\mu_n = \{\zeta \in \mathbb{C} \mid \zeta^n = 1\}$$

mit der Multiplikation als Verknüpfung ist

$$\begin{array}{ccc} (\mathbb{Z}/n, +) & \longrightarrow & \mu_n \\ j & \longmapsto & e^{\frac{2\pi i}{n} j} \end{array}$$

ein Isomorphismus.

8) Sind $a, b \in \mathbb{Z}_{\geq 1}$ *und* $\mathrm{ggT}(a, b) = 1$. *Dann gilt*

$$\mathbb{Z}/ab \cong \mathbb{Z}/a \times \mathbb{Z}/b$$

Dies zeigen wir in Übung 2.6.

Praktisch werden Gruppen oft durch Erzeuger gegeben:

Definition 2.2.13 *Sei* E *eine Teilmenge einer Gruppe* G. *Dann ist* $\langle E \rangle$ *die kleinste Untergruppe von* G, *die* E *enthält, äquivalent der Durchschnitt aller Untergruppen* $U \subset G$, *die* E *enthalten (denn der Durchschnitt von Untergruppen ist eine Untergruppe).*

Wir nennen $\langle E \rangle$ *die* ***von E erzeugte Untergruppe*** *von* G.

Eine Gruppe G *heißt* ***zyklisch****, wenn es ein* $g \in G$ *gibt mit*

$$G = \langle g \rangle$$

Für $g_1, \ldots, g_k \in G$ ist offenbar

$$\langle g_1, \ldots, g_k \rangle = \left\{ \prod_{i=1}^{r} t_i \mid r \geq 0 \text{ und } t_i \in \left\{ g_1, g_1^{-1}, \ldots, g_k, g_k^{-1} \right\} \right\}$$

Beispiel 2.2.14 *1) Die Restklassengruppe* $\mathbb{Z}/n$ *ist zyklisch von* $\overline{1}$ *erzeugt.*

2) Die Gruppe $(\mathbb{Z}, +)$ ist zyklisch von 1 erzeugt.

3) Die Untergruppe $n\mathbb{Z} \subset (\mathbb{Z}, +)$ ist zyklisch erzeugt von n, also $n\mathbb{Z} = \langle n \rangle$. Nach Beispiel 2.2.3 gilt $n\mathbb{Z} \cong \mathbb{Z}$.

Wir werden später zeigen, dass alle zyklischen Gruppen bis auf Isomorphie von der Form $\mathbb{Z}$ oder $\mathbb{Z}/n$ sind (siehe Beispiel 2.3.17).

Definition 2.2.15 *Sei $g \in G$ ein Element einer Gruppe. Dann heißt*

$$\operatorname{ord}(g) = |\langle g \rangle|$$

*die **Ordnung** von g.*

Siehe auch Übungsaufgabe 2.7.

2.2.2 Gruppenoperationen

Gruppen werden in der Mathematik betrachtet, da sie als Mengen von Symmetrien von Objekten auftauchen. Um Symmetriegruppen einzuführen, verwenden wir die Notation einer Operation.

Definition 2.2.16 *Sei $(G, \circ)$ eine Gruppe und M eine Menge. Eine **Operation** von G auf M (von links) ist eine Abbildung*

$$\begin{array}{rccc} \cdot : & G \times M & \longrightarrow & M \\ & (g, m) & \longmapsto & g \cdot m \end{array}$$

die folgende Bedingungen erfüllt:

1)

$$e \cdot m = m$$

für alle $m \in M$.

2)

$$(a \circ b) \cdot m = a \cdot (b \cdot m)$$

für alle $a, b \in G$ und $m \in M$.

Anders formuliert, ist eine Operation von G auf M ein Gruppenhomomorphismus

$$\begin{array}{rccc} \varphi: & G & \longrightarrow & S(M) \\ & g & \mapsto & \varphi(g) = \begin{pmatrix} M & \longrightarrow & M \\ m & \mapsto & g \cdot m \end{pmatrix} \end{array}$$

von G in die Gruppe der Selbstabbildung von M. Wir überprüfen, dass $\varphi(g)$ für $g \in G$ bijektiv und φ ein Homomorphismus ist: Sei $g \cdot m_1 = g \cdot m_2$ für $g \in G$ und $m_1, m_2 \in M$, dann folgt

$$\begin{aligned} m_1 = e \cdot m_1 &= \left(g^{-1} \circ g\right) \cdot m_1 = g^{-1} \cdot (g \cdot m_1) \\ &= g^{-1} \cdot (g \cdot m_2) = \left(g^{-1} \circ g\right) \cdot m_2 = e \cdot m_1 = m_2 \end{aligned}$$

Ist $m \in M$, dann $m = e \cdot m$. Weiter ist

$$\begin{aligned} \varphi(g \circ h) &= (m \mapsto (g \circ h) \cdot m) = (m \mapsto g \cdot (h \cdot m)) \\ &= (m \mapsto g \cdot m) \circ (m \mapsto h \cdot m) \end{aligned}$$

Definition 2.2.17 *Eine Operation von G auf M heißt **treu**, wenn φ injektiv ist, d.h.*

$$\forall a \in G,\ a \neq e\ \exists m \in M \text{ mit } a \cdot m \neq m$$

Beispiel 2.2.18 *1) S_n operiert auf $\{1, ..., n\}$.*

2) Die Gruppe $\mathrm{GL}(n, K)$ operiert auf K^n.

3) S_n operiert auch auf $\mathbb{R}^n$, indem wir eine Permutation

$$\sigma : \{e_1, ..., e_n\} \to \{e_1, ..., e_n\}$$

der Einheitsbasisvektoren

$$e_i = \begin{array}{c} i \\ \\ \end{array} \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \in \mathbb{R}^n$$

$$\sigma(e_i) := e_{\sigma(i)}$$

zu einer linearen Abbildung

$$A_\sigma : \mathbb{R}^n \longrightarrow \mathbb{R}^n$$

fortsetzen. Die zugehörige Matrix

$$A_\sigma = (a_{ij}(\sigma))$$

hat die Eigenschaft, dass in jeder Zeile und Spalte genau ein Eintrag ungleich 0 *steht und dieser den Wert* 1 *hat. Solche Matrizen nennt man* ***Permutationsmatrizen****.*

Beachten Sie

$$A_\sigma \in \mathrm{O}(n)$$

ist eine orthogonale Matrix, d.h. sie lässt den Euklidischen Abstand zum Nullpunkt

$$\|x\| = \sqrt{\textstyle\sum_{i=1}^n x_i^2}$$

invariant. Die Gruppen

$$\begin{array}{rcl} \mathrm{O}(n) & = & \{A \in \mathrm{GL}(n,\mathbb{R}) \mid A^{-1} = A^t\} \\ \cup & & \\ \mathrm{SO}(n) & = & \{A \in \mathrm{O}(n) \mid \det A = 1\} \end{array}$$

heißen ***orthogonale Gruppe*** $\mathrm{O}(n)$ *bzw.* ***spezielle orthogonale Gruppe*** $\mathrm{SO}(n)$ *der Drehungen. Beachten Sie, dass nicht jedes Element von* $\mathrm{SO}(n)$ *eine Permutationsmatrix ist.*

Allgemeiner betrachtet man:

Definition 2.2.19 *Die Menge der Euklidischen Bewegungen des* $\mathbb{R}^n$

$$\mathrm{E}(n) = \{x \mapsto Ax + b \mid A \in \mathrm{O}(n),\ b \in \mathbb{R}^n\}$$

ist mit der Komposition

$$(x \mapsto Ax + b) \circ (x \mapsto Bx + c) = (x \mapsto ABx + Ac + b)$$

eine Gruppe, die ***Bewegungsgruppe****.*

In der linearen Algebra zeigt man, dass sich jede abstandserhaltende Abbildung als Komposition einer Isometrie (d.h. einer

längen- und winkelerhaltenden Abbildung) und einer Translation schreiben lässt. Weiter sind die Isometrien des Euklidischen Raums genau dargestellt durch die orthogonalen Matrizen. Somit sind die Elemente von $\mathrm{E}(n)$ *nichts anderes als die abstandserhaltenden Abbildungen.*

Weiter heißt

$$\mathrm{SE}(n) = \{x \mapsto Ax + b \mid A \in \mathrm{SO}(n),\ b \in \mathbb{R}^n\}$$

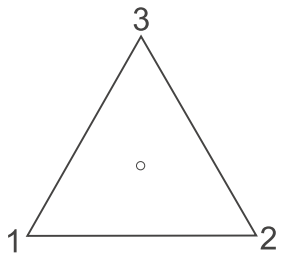
die ***spezielle Bewegungsgruppe****. Die Elemente sind Komposition einer Drehung und einer Translation, erhalten also zusätzlich die Orientierung.*

Sei $M \subset \mathbb{R}^n$ *eine Teilmenge. Die Gruppe*

$$\mathrm{Sym}(M) = \{A \in \mathrm{E}(n) \mid A(M) = M\}$$

heißt ***Symmetriegruppe*** *von* M*.*

Beispiel 2.2.20 *Wir beschreiben die Symmetriegruppe* $\mathrm{Sym}(D)$ *des gleichseitigen Dreiecks* D



Jede Symmetrie ist ein Element der $\mathrm{O}(2)$ *mit* 0*-Punkt im Schwerpunkt des Dreiecks, ist also durch Multiplikation mit einer orthogonalen Matrix gegeben. Wir schreiben die Elemente von* $\mathrm{Sym}(D)$ *mit* $\alpha = \frac{2}{3}\pi$ *als*

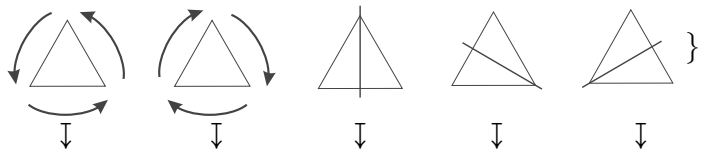
$$\mathrm{id} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \qquad = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \qquad = \begin{pmatrix} -\cos\alpha & -\sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix}$$

$$= \begin{pmatrix} \cos\alpha & \sin\alpha \\ -\sin\alpha & \cos\alpha \end{pmatrix} \qquad = \begin{pmatrix} -\cos\alpha & \sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$$

Jede Symmetrie ist eindeutig durch ihre Wirkung auf den Ecken festgelegt. Nummerieren wir die Ecken, können wir also jedes Element als eine bijektive Abbildung $\{1,2,3\} \to \{1,2,3\}$ *auffassen. Genauer haben wir einen Gruppenisomorphismus* φ

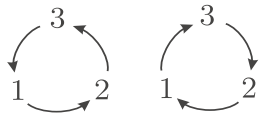
$$\mathrm{Sym}\,(D) = \{\mathrm{id}$$



$$\}$$

$$\varphi \downarrow \qquad \mathrm{id} \qquad (1 \leftrightarrow 2) \qquad (1 \leftrightarrow 3) \qquad (2 \leftrightarrow 3)$$

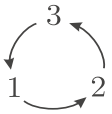
$$S_3 = \{\mathrm{id}$$

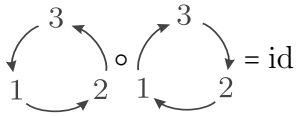


$$(1 \leftrightarrow 2) \quad (1 \leftrightarrow 3) \quad (2 \leftrightarrow 3)\}$$

Mit der Verknüpfung (die gegeben war durch Komposition von Abbildungen) berechnen wir beispielsweise

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





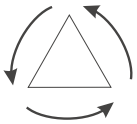
$$= \mathrm{id}$$

Der Isomorphismus φ *wird induziert durch die Operation von* $\mathrm{Sym}\,(D)$ *auf den Ecken des Dreiecks*

$$\mathrm{Sym}\,(D) \times \{1,2,3\} \to \{1,2,3\}$$

Bezeichnet

$$r_{120} =$$



die Drehung um $120°$*, dann bildet die Operation beispielsweise ab*

$$(r_{120}, 1) \mapsto 2, \ (r_{120}, 2) \mapsto 3, \ (r_{120}, 3) \mapsto 1$$

Äquivalent haben wir einen Gruppenhomomorphismus

$$\mathrm{Sym}\,(D) \to S\,(\{1,2,3\}) = S_3$$

der z.B. abbildet

$$r_{120} \mapsto \begin{pmatrix} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

und analog für die anderen Elemente von $\mathrm{Sym}\,(D)$.

Beispiel 2.2.21 *Sei*

$$M = Q = \left\{x \in \mathbb{R}^3 \mid |x_i| \leq 1 \ \forall i\right\}$$

der Einheitswürfel. Die Symmetriegruppe von Q *ist*

$$\mathrm{Sym}\,(Q) = \left\{\begin{pmatrix} \pm 1 & 0 & 0 \\ 0 & \pm 1 & 0 \\ 0 & 0 & \pm 1 \end{pmatrix} \cdot A_\sigma \mid \sigma \in S_3\right\}$$

hat also $2^3 \cdot 6 = 48$ *Elemente: Jede Symmetrie von* Q *muss die Menge der Punkte kleinsten Abstands zum Nullpunkt auf dem Rand* ∂Q *von* Q *in sich überführen. Die Behauptung folgt, da diese Menge aus den Punkten*

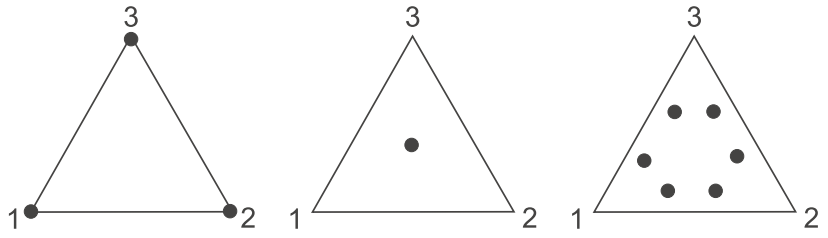
$$\{\pm e_1, \pm e_2, \pm e_3\}$$

besteht.

Beispiel 2.2.22 *Gegeben ein Punkt des gleichseitigen Dreiecks* D*, wollen wir untersuchen, auf welche anderen Punkte dieser unter der Operation*

$$\mathrm{Sym}\,(D) \times D \to D$$

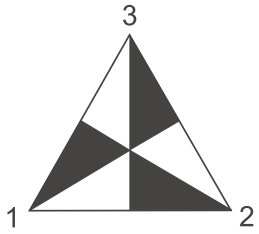
abgebildet werden kann. Diese Menge nennt man die Bahn, die Anzahl der Elemente die Länge der Bahn. Beispiele von Bahnen sind



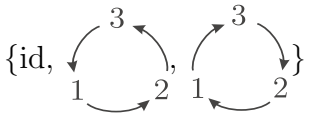
Ebenso kann man die Operation auf der Menge aller Teilmengen von D*, der Potenzmenge* 2^D*, betrachten*

$$\mathrm{Sym}\,(D) \times 2^D \to 2^D$$

In der Bahn der schwarzen Teilmenge liegt außerdem noch die weisse Teilmenge



Andererseits kann man die Menge aller Elemente von $\mathrm{Sym}\,(D)$ *betrachten, die einen gegebenen Punkt (oder Teilmenge) festhalten. Die Ecke* 1 *wird festgehalten von* $\{\mathrm{id}, (2 \leftrightarrow 3)\}$*, der* 0*-Punkt von* $\mathrm{Sym}\,(D)$ *und der Punkt* p *nur von der Identität. Die schwarze Teilmenge wird festgehalten von*



Wir beobachten, dass diese Mengen stets Untergruppen von $\mathrm{Sym}\,(D)$ *sind, und das Produkt der Gruppenordnung mit der Länge der jeweiligen Bahn stets* $|\mathrm{Sym}\,(D)| = 6$ *ergibt. Dies werden wir in Abschnitt 2.2.5 zeigen.*

Zunächst formalisieren wir aber diese Ideen:

Definition 2.2.23 *Sei* $G \times M \longrightarrow M$ *eine Operation. Dann heißt zu* $m \in M$ *die Menge*

$$Gm = \{gm \mid g \in G\} \subset M$$

die ***Bahn*** *(oder der* ***Orbit****) von* m*. Ist* $N \subset M$ *eine Teilmenge, dann heißt*

$$\mathrm{Stab}\,(N) = \{g \in G \mid gN = N\}$$

der ***Stabilisator*** *von der Menge* N*.*

Für $m \in M$ *sei*

$$\mathrm{Stab}\,(m) = \mathrm{Stab}\,(\{m\})$$

Bemerkung 2.2.24 *1)* $\mathrm{Stab}\,(N) \subset G$ *ist eine Untergruppe. Sie hält* N *als Menge fest.*

$$\bigcap_{n \in N} \mathrm{Stab}\,(n) \subset G$$

ist die Untergruppe, die N *punktweise fest lässt.*

2) *Zwei Bahnen Gm_1 und Gm_2 sind entweder gleich oder disjunkt. In der gleichen Bahn zu sein ist also eine Äquivalenzrelation.*

Ist

$$m_3 \in Gm_1 \cap Gm_2$$

dann gibt es g_1, g_2 mit

$$m_3 = g_1 m_1 = g_2 m_2$$

also

$$m_2 = g_2^{-1} g_1 m_1$$

Damit ist $m_2 \in Gm_1$, und somit $Gm_2 \subset Gm_1$, ebenso gilt die andere Inklusion, also $Gm_2 = Gm_1$.

Definition 2.2.25 *Die Menge der Bahnen bezeichnen wir mit $G\backslash M$ (**Quotient** von M nach G) bei Linksoperation und mit M/G bei Rechtsoperation*

$$M \times G \longrightarrow M$$

*Jedes Element $m \in Gm_1$ nennen wir einen **Repräsentanten** der Bahn, denn $Gm = Gm_1$.*

$$\pi : M \longrightarrow G\backslash M$$

*heißt **Quotientenabbildung**.*

Aus obigen Bemerkungen haben wir:

Definition und Satz 2.2.26 *Sei $G \times M \longrightarrow M$ eine Operation. Ein **vollständiges Repräsentantensystem** der Bahnen ist eine Teilmenge $R \subset M$, sodass jede Bahn Gm genau ein Element von R enthält.*

Dann ist M die disjunkte Vereinigung

$$M = \bigcup_{r \in R} G \cdot r$$

Beispiel 2.2.27 *Ist $\sigma \in S_n$, dann zerlegt die Operation von $\langle\sigma\rangle$ die Menge $\{1,...,n\}$ in Bahnen der Form*

$$\langle\sigma\rangle x = \left\{x, \sigma(x), \sigma^2(x), ..., \sigma^{t-1}(x)\right\}$$

*und t minimal mit $\sigma^t(x) = x$. Gibt es nur eine Bahn der Länge $t > 1$ (d.h. alle anderen haben Länge 1), dann heißt σ **Zykel** der Ordnung t, und wir schreiben*

$$\sigma = \left(x, \sigma(x), \sigma^2(x), ..., \sigma^{t-1}(x)\right).$$

Transpositionen sind Zykel der Länge 2.

Satz 2.2.28 *Es gilt:*

1) Jedes Element der S_n ist ein Produkt elementfremder Zykel.

2) Jedes Element der S_n ist ein Produkt von Transpositionen.

Beweis. Sei $\sigma \in S_n$.

1) Sei $\{x_1, ..., x_r\}$ ein vollständiges Repräsentantensystem der Bahnen der Operation von $\langle\sigma\rangle$ auf $\{1,...,n\}$. Schränken wir σ als Abbildung auf die Bahn $\langle\sigma\rangle x_i$ ein, erhalten wir einen Zykel σ_i und
$$\sigma = \sigma_1 \cdot ... \cdot \sigma_r$$

2) Wir können annehmen, dass σ ein Zykel $(y_0, ..., y_{t-1})$ ist und
$$(y_0, ..., y_{t-1}) = (y_0, y_1) \cdot ... \cdot (y_{t-2}, y_{t-1})$$

■

Beispiel 2.2.29 *Sei*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 4 & 1 & 2 & 3 & 9 & 8 & 7 & 6 & 5 \end{pmatrix}$$

Die Operation von $\langle\sigma\rangle$ zerlegt

$$\{1,...,9\} = \{1,2,3,4\} \dot\cup \{5,9\} \dot\cup \{6,8\} \dot\cup \{7\}$$

in disjunkte Bahnen und

$$\begin{aligned}\sigma &= (1,4,3,2)\,(5,9)\,(6,8)\\ &= (1,4)\,(4,3)\,(3,2)\,(5,9)\,(6,8)\end{aligned}$$

Siehe auch Übungsaufgabe 2.4.

Beispiel 2.2.30 *Die symmetrische Gruppe S_3 wird von $(1,2)$ und $(2,3)$ erzeugt*

$$S_3 = \langle (1,2), (2,3) \rangle$$

denn $(1,2)\,(2,3) = (1,2,3)$ und $(1,2)\,(2,3)\,(1,2) = (1,3)$. Allgemein gilt

$$S_n = \langle (1,2), (2,3), ..., (n-1,n) \rangle$$

siehe auch Übungsaufgabe 2.8 und auch 2.9.

2.2.3 Operation durch Translation

Der folgende Satz hat eine zentrale Bedeutung für das praktische Rechnen mit Gruppen (z.B. das Computeralgebrasystem GAP, siehe [5], implementiert Algorithmen zur Berechnung im Wesentlichen aller hier eingeführten Objekte für Untergruppen der symmetrischen Gruppe).

Satz 2.2.31 (Cayley) *Jede Gruppe G ist isomorph zu einer Untergruppe einer Gruppe von Selbstabbildungen $S(X)$ für eine Menge X.*

Zum Beweis des Satzes von Cayley (Übungsaufgabe 2.10) betrachtet man z.B. die Operation von G auf sich selbst

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

Dies ist eine Operation von links und von rechts. Für endliche Gruppen kann man die Verknüpfung mittels einer Tabelle angeben, der **Verknüpfungstafel**.

Beispiel 2.2.32 *Für*

$$G = \mathbb{Z}/4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$$

ist die Verknüpfungstafel

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

In jeder Zeile und Spalte steht jedes Element genau einmal.

Eine Gruppe ist abelsch genau dann, wenn ihre Verknüpfungstafel bezüglich der Diagonalen symmetrisch ist. Das Assoziativgesetz lässt sich der Tabelle nicht unmittelbar ansehen.

Analog zur Operation einer Gruppe auf sich selbst kann man auch die Operation einer Untergruppe betrachten:

Beispiel 2.2.33 *Wie in Beispiel 2.2.6 gezeigt, sind die Untergruppen von* $(\mathbb{Z}, +)$ *von der Form*

$$n\mathbb{Z} = \{n \cdot k \mid k \in \mathbb{Z}\}$$

Eine Gruppenoperation von $n\mathbb{Z}$ *auf* $\mathbb{Z}$ *(von rechts) ist gegeben durch*

$$\begin{aligned} \mathbb{Z} \times n\mathbb{Z} &\to \mathbb{Z} \\ (a, n \cdot k) &\mapsto a + n \cdot k \end{aligned}$$

Die Bahnen sind genau die Restklassen modulo n

$$\overline{a} = a + n\mathbb{Z} = \{a + n \cdot k \mid k \in \mathbb{Z}\}$$

Wir haben in Beispiel 2.2.7 schon gesehen, dass die Menge dieser Bahnen mit der Addition

$$\overline{a} + \overline{b} = (a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z} = \overline{a + b}$$

wieder eine Gruppe $\mathbb{Z}/n$ *ist.*

Zum Beispiel sind für $n = 4$ die Bahnen der 2 bzw. 3

$$\overline{2} = 2 + 4\mathbb{Z} = \{..., -6, -2, 2, 6, 10, 14, ...\}$$
$$\overline{3} = 3 + 4\mathbb{Z} = \{..., -5, -1, 3, 7, 11, 15, ...\}$$

und

$$\overline{2} + \overline{3} = 5 + 4\mathbb{Z} = 1 + 4\mathbb{Z} = \{..., -7, -3, 1, 5, 9, 13, ...\}$$

Man beachte, dass die Addition von Bahnen wohldefiniert ist, denn ist $a+n\mathbb{Z} = a'+n\mathbb{Z}$ und $b+n\mathbb{Z} = b'+n\mathbb{Z}$, dann gilt $a-a' = n\cdot k$ und $b - b' = n \cdot s$, d.h.

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

also

$$\overline{a + b} = \overline{a' + b'}$$

Später werden wir allgemein untersuchen, wann eine Menge von Bahnen einer Untergruppe wieder eine Gruppe ist.

Zunächst formulieren wir dieses Konzept allgemein:

Definition 2.2.34 (Nebenklassen) *Sei $H \subset G$ eine Untergruppe. Dann definiert die Verknüpfung in G eine Operation von H auf G*

$$H \times G \longrightarrow G$$

von links, und ebenso eine von rechts

$$G \times H \longrightarrow G$$

Für $g \in G$ heißen die Bahnen dieser Operation

$$Hg = \{hg \mid h \in H\}$$

bzw.

$$gH = \{gh \mid h \in H\}$$

*rechte bzw. linke **Nebenklassen** von g.*

Satz 2.2.35 *Sei $H \subset G$ eine Untergruppe. Je zwei Nebenklassen von H haben gleich viele Elemente.*

Beweis. Seien $a, b \in G$. Dann stehen aH und bH in Bijektion zueinander durch Multiplikation mit ba^{-1} von links

$$\begin{array}{ccc} aH & \xrightarrow{1:1} & bH \\ ac & \longmapsto & ba^{-1}ac = bc \end{array}$$

Die rechten und linken Nebenklassen aH und Ha stehen in Bijektion vermöge Konjugation mit a^{-1}

$$\begin{array}{ccc} g & \longmapsto & aga^{-1} \\ G & \longrightarrow & G \\ \cup & & \cup \\ aH & \longrightarrow & Ha \end{array}$$

Mit der Operation durch Konjugation werden wir uns in Abschnitt 2.2.4 beschäftigen. ■

Corollar 2.2.36 (Indexformel) *Sei $H \subset G$ eine Untergruppe. Es gilt*

$$|G| = |G/H| \cdot |H|$$

Definition 2.2.37 *Sei $H \subset G$ eine Untergruppe.*

$$[G : H] := |G/H|$$

*heißt **Index** von H in G*

Siehe auch Übungsaufgabe 2.12).
Wir bemerken zunächst, dass

$$\begin{aligned} H &\to aH \\ h &\mapsto ah \end{aligned}$$

eine Bijektion ist, also

$$|aH| = |H|$$

Beweis. (der Indexformel) Nach Definition und Satz 2.2.26 ist G die disjunkte Vereinigung aller aH mit a aus einem vollständigen Repräsentantensystem R, also falls $|G| < \infty$ ist

$$|G| = \sum_{a \in R} |aH| = |R| \cdot |H|$$

(mit Satz 2.2.35). Ist $|G| = \infty$, dann auch $|G/H| = \infty$ oder $|H| = \infty$. ■

Aus der Indexformel (Satz 2.2.36) erhalten wir:

Corollar 2.2.38 *In einer endlichen Gruppe G ist die Ordnung eines Elements $g \in G$ ein Teiler der Gruppenordnung $|G|$, d.h.* $\operatorname{ord}(g) \mid |G|$.

Corollar 2.2.39 *Jede Gruppe G mit $|G|$ prim ist zyklisch.*

Beweis. Aus der Indexformel erhalten wir, dass G nur die Untergruppen $\{e\}$ und G hat. Somit ist für jedes $e \neq g \in G$ schon

$$\{e\} \neq \langle g \rangle = G$$

■

2.2.4 Operation durch Konjugation

Beim Beweis der Gleichmächtigkeit von Nebenklassen (Satz 2.2.35) haben wir die Konjugationsoperation verwendet:

Definition 2.2.40 *Die Abbildung*

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (a,b) & \longmapsto & aba^{-1} \end{array}$$

definiert eine Operation von G auf G von links. Diese Operation heißt ***Konjugation****.*

Die Bahn

$$b^G = \left\{ aba^{-1} \mid a \in G \right\}$$

heißt ***Konjugationsklasse*** *von $b \in G$.*

Beweis. Anwenden von $a_1 a_2$ auf b vermöge Konjugation

$$\begin{array}{rcl} (a_1 a_2, b) & \longmapsto & a_1 a_2 b \left(a_1 a_2\right)^{-1} \\ & & = a_1 a_2 b a_2^{-1} a_1^{-1} \\ & & = a_1 \left(a_2 b a_2^{-1}\right) a_1^{-1} \end{array}$$

■

Beispiel 2.2.41 *Wir bestimmen die Konjugationsklassen der S_3:*

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

Weiter ist

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

und ebenso für jede andere Transposition. Die Konjugationsklassen sind also

$$\{()\}$$
$$\{(1,2),(1,3),(2,3)\}$$
$$\{(1,2,3),(1,3,2)\}$$

Der folgende GAP-Code berechnet die Konjugationsklassen:

```
g:=SymmetricGroup(3);
c:=ConjugacyClasses(g);
Elements(c[2]);
Elements(c[3]);
```

Wir beschreiben die Konjugationsklassen der symmetrischen Gruppe S_n allgemein:

Definition 2.2.42 *Eine **Partition** von $n \in \mathbb{Z}_{\geq 1}$ ist eine Summe $n = n_1 + ... + n_k$ mit $n_1 \geq ... \geq n_k \geq 1$.*

Jedes $\sigma \in S_n$ ist ein Produkt

$$\sigma = \sigma_1 \cdot ... \cdot \sigma_k$$

von disjunkten Zykeln der Längen $n_1 \geq ... \geq n_k \geq 1$. Schreiben wir auch Bahnen der Länge 1, ist

$$n = n_1 + ... + n_k$$

eine Partition. Beispielsweise ordnen wir

$$(2,3,4)(5,6) = (2,3,4)(5,6)(1) \in S_6$$

die Partition $6 = 3 + 2 + 1$ zu.

Ist $\sigma = (x_1, ..., x_n) \in S_n$ und $\tau \in S_n$, dann gilt

$$\left(\tau \cdot \sigma \cdot \tau^{-1}\right)(\tau(x_i)) = \tau(\sigma(x_i))$$

also

$$\tau \cdot \sigma \cdot \tau^{-1} = (\tau(x_1), ..., \tau(x_n))$$

Beispielsweise

$$(2,3,4) \cdot \ (1,2)(3,4,5) \ \cdot (2,3,4)^{-1} = (1,3)(4,2,5)$$

Damit zeigt man (Übungsaufgabe 2.16):

Satz 2.2.43 *Die Menge der Konjugationsklassen von S_n ist bijektiv zu der Menge der Partitionen von n. Die zugeordnete Partition heißt* ***Zykeltyp****.*

Lemma 2.2.44 *Für festes $a \in G$ ist Konjugation mit a ein Gruppenhomomorphismus.*

$$\begin{array}{rccc} \kappa_a: & G & \longrightarrow & G \\ & g & \longmapsto & a(g) = aga^{-1} \end{array}$$

Beweis. Für $g, h \in G$ gilt

$$\begin{aligned} \kappa_a(gh) &= a(gh)\,a^{-1} = aga^{-1}aha^{-1} \\ &= \kappa_a(g) \cdot \kappa_a(h) \end{aligned}$$

■

Definition 2.2.45 *Die Menge der Automorphismen von G (d.h. Isomorphismen $G \to G$) bilden eine Gruppe $\mathrm{Aut}(G)$ die* ***Automorphismengruppe*** *von G.*

Die Abbildung

$$\begin{array}{rccc} \kappa: & G & \longrightarrow & \mathrm{Aut}(G) \\ & a & \longmapsto & \left(\begin{array}{rccc} \kappa_a: & G & \longrightarrow & G \\ & g & \longmapsto & aga^{-1} \end{array} \right) \end{array}$$

ist ein Homomorphismus von G in die Gruppe der Automorphismen $\mathrm{Aut}(G)$.

Die Elemente des Bildes von κ nennt man ***innere Automorphismen****. Diese bilden eine Untergruppe*

$$\mathrm{Inn}(G) = \left\{ g \longmapsto aga^{-1} \mid a \in G \right\} \subset \mathrm{Aut}(G)$$

(siehe auch Übungsaufgabe 2.28).

Der Kern von κ ist die Menge der Gruppenelemente $a \in G$, sodass $\kappa_a = \mathrm{id}_G$ also $aga^{-1} = g$ für alle $g \in G$.

Definition 2.2.46 *Das* ***Zentrum*** *einer Gruppe G ist*

$$Z(G) = \ker(\kappa) = \{a \in G \mid ag = ga \ \ \forall g \in G\}$$

Das Zentrum ist eine abelsche Untergruppe. Es ist eine wichtige Invariante zur Klassifikation von Gruppen. In Übungsaufgabe 2.51 zeigen wir z.B., dass $Z(A_n)$ trivial ist für $n \geq 4$.

Beispiel 2.2.47 *1) Ist G abelsch, dann ist* $\mathrm{Inn}(G) = \{\mathrm{id}\}$.

2) Ist $G = \langle g \rangle = \langle h \rangle$ eine endliche zyklische Gruppe, dann setzt sich die Zuordnung $\varphi(g) := h$ zu einem Automorphismus von G fort durch

$$\varphi\left(g^j\right) = h^j$$

3) Wir bestimmen die inneren und äußeren Automorphismen von $G = \mathbb{Z}/3 = \left\{\overline{0}, \overline{1}, \overline{2}\right\}$. Die Abbildung

$$\begin{aligned} \mathrm{Aut}(G) &\to S\left(\left\{\overline{1}, \overline{2}\right\}\right) \cong \mathbb{Z}/2 \\ \varphi &\mapsto \begin{pmatrix} \overline{1} & \overline{2} \\ \varphi\left(\overline{1}\right) & \varphi\left(\overline{2}\right) \end{pmatrix} \end{aligned}$$

ist ein Gruppenisomorphismus, denn $\mathrm{Aut}(G) \subset S\left(\left\{\overline{0}, \overline{1}, \overline{2}\right\}\right)$, *für jeden Automorphismus gilt $\overline{0} \mapsto \overline{0}$ und die Zuordnung $\overline{1} \mapsto \overline{2}$ setzt sich zu einem Automorphismus*

$$\begin{array}{rccc} \varphi: & G & \to & G \\ & \overline{0} & \mapsto & \overline{0} \\ & \overline{1} & \mapsto & \overline{2} \\ & \overline{2} & \mapsto & \overline{1} \end{array}$$

von G fort. Weiter ist $\mathrm{Inn}(G)$ *trivial wegen* $(1.)$.

4) Die Gruppe S_6 wird von den Elementen $(1,2,3,4,5)$ und $(5,6)$ erzeugt. Der folgende GAP-Code zeigt, dass sich die Zuordnung

$$\begin{array}{lcl} (1,2,3,4,5) & \mapsto & (1,2,3,4,5) \\ (5,6) & \mapsto & (1,2)(3,5)(4,6) \end{array}$$

zu einem Automorphimus φ von S_6 forsetzen lässt:

```
gens:=[(1,2,3,4,5),(5,6)];
newgens:=[(1,2,3,4,5),(1,2)(3,5)(4,6)];
g:=Group(gens);
```

```
hom:=GroupHomomorphismByImages(g,g,gens,newgens);
Kernel(hom);
```

Da φ den Zykeltyp ändert, ist φ kein innerer Automorphismus und somit $\mathrm{Inn}(S_6) \subsetneq \mathrm{Aut}(S_6)$.

Für $n \neq 2, 6$ gilt stets

$$\mathrm{Aut}(S_n) = \mathrm{Inn}(S_n) \cong S_n$$

Dies können wir hier nicht allgemein zeigen, wir behandeln den Fall $n = 3$ in Übungsaufgabe 2.28.

2.2.5 Bahnengleichung

Wir betrachten nun wieder die Operation einer Gruppe G auf einer Menge M und fragen nach der Beziehung zwischen der Bahn eines Elements $m \in M$ und dem Stabilisator von m.

Satz 2.2.48 *Sei*

$$G \times M \longrightarrow M$$

eine Operation, $m \in M$ und

$$H := \mathrm{Stab}(m)$$

Dann gibt es eine natürliche Bijektion

$$\begin{array}{ccc} G/H & \longrightarrow & Gm \\ gH & \longmapsto & gm \end{array}$$

Beweis. Die Abbildung ist wohldefiniert: Ist $gH = g'H$, dann ist $g' \in gH$, also $g' = gh$ mit $h \in H$. Es folgt

$$g'm = ghm = gm$$

da m von h stabilisiert wird. Die Abbildung ist offenbar surjektiv. Sie ist auch injektiv, denn

$$g_1 m = g_2 m \Rightarrow g_1^{-1} g_2 \in H \Rightarrow$$
$$g_2 = g_1 g_1^{-1} g_2 \in g_1 H \Rightarrow g_1 H = g_2 H$$

■

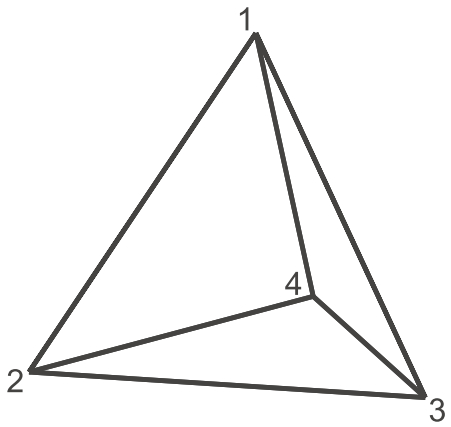


Abbildung 2.3: Tetraeder

Corollar 2.2.49 *Sei $G \times M \longrightarrow M$ eine Operation und $m \in M$. Dann gilt*

$$|Gm| \cdot |\mathrm{Stab}\,(m)| = |G|$$

Beweis. Es ist

$$|Gm| = |G/H|$$

und

$$|G/H| \cdot |H| = |G|$$

nach der Indexformel 2.2.36. ■

Beispiel 2.2.50 (Symmetriegruppe des Tetraeders) *Sei T ein regulärer Tetraeder mit den Ecken $1, ..., 4$ wie in Abbildung 2.3. Die Symmetrien von T sind durch ihre Wirkung auf den Ecken eindeutig bestimmt. Wir können also die Symmetriegruppe* $\mathrm{Sym}\,(T)$ *von T als Untergruppe von S_4 auffassen.*

Die Spiegelung an der Ebene, aufgespannt durch eine Kante und dem Mittelpunkt der gegenüberliegenden Seite, entspricht einer Transposition, z.B. die Spiegelung an der in Abbildung 2.4 eingezeichneten Ebene entspricht $(2, 3)$. Da die S_4 von den Transpositionen erzeugt wird, folgt:

$$\mathrm{Sym}\,(T) \cong S_4$$

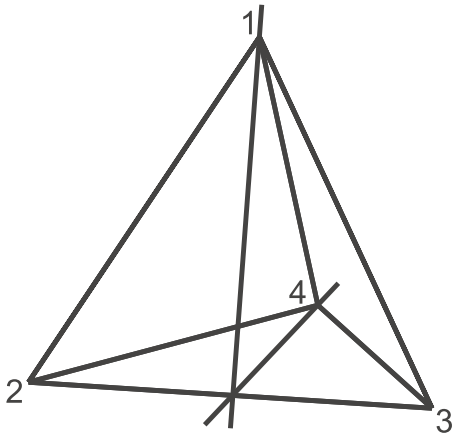


Abbildung 2.4: Spiegelsymmetrie $(2,3)$ des Tetraeders

Beispiel 2.2.51 (Bahnen und Stabilisatoren) *Für die Operation von $G = S_4$ auf dem Tetraeder T mit Mittelpunkt 0 durch Permutation der Vertices von T betrachten wir die Bahnen Gm für die Punkte $m \in T$, die in Abbildung 2.5 markiert sind:*

Bahnen Gm	$\lvert Gm\rvert$	*Stabilisatoren* $\mathrm{Stab}(m)$	$\lvert\mathrm{Stab}(m)\rvert$
$G1 = \{1,2,3,4\}$	4	S_3	6
$Gm_{12} = \{m_{12},\ldots,m_{34}\}$	6	$\mathrm{Stab}(m_{12})$ $= \{e,(12),(34),(12)(34)\}$ $\cong \mathbb{Z}_2 \times \mathbb{Z}_2$	4
Gp	24	$\mathrm{Stab}(p) = \{e\}$	1
$G0 = \{0\}$	1	$\mathrm{Stab}(0) = S_4$	24

Wir bemerken, dass stets

$$|Gm| \cdot |\mathrm{Stab}(m)| = |G|$$

Satz 2.2.52 (Bahnengleichung) *Sei $R \subset M$ ein vollständiges Repräsentantensystem der Bahnen einer Operation $G \times M \longrightarrow M$. Dann gilt*

$$|M| = \sum_{r \in R} \frac{|G|}{|\mathrm{Stab}(r)|}$$

Beweis. M ist nach Definition und Satz 2.2.26 die disjunkte Vereinigung

$$M = \bigcup_{r \in R} G \cdot r$$

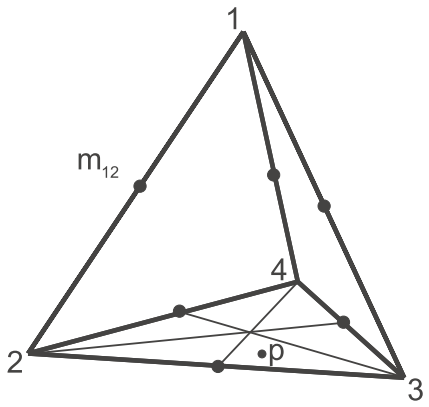


Abbildung 2.5: Bahnen von Punkten des Tetraeders

Also

$$|M| = \sum_{r \in R} |G \cdot r| = \sum_{r \in R} \frac{|G|}{|\mathrm{Stab}\,(r)|}$$

■

Beispiel 2.2.53 *Die Permutation*

$$\begin{aligned}\sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 1 & 2 & 3 & 9 & 7 & 6 & 5 & 8 & 10 \end{pmatrix} \\ &= (1,4,3,2)\,(5,9,8)\,(6,7)\end{aligned}$$

erzeugt eine zyklische Gruppe $G = \langle \sigma \rangle$ *der Ordnung* 12. *Die Operation von* $\langle \sigma \rangle$ *zerlegt*

$$\{1,...,10\} = \{1,2,3,4\} \dot{\cup} \{5,8,9\} \dot{\cup} \{6,7\} \dot{\cup} \{10\}$$

in Bahnen, also gilt die Bahnengleichung

$$\begin{aligned}10 &= 4 + 3 + 2 + 1 \\ &= \frac{12}{3} + \frac{12}{4} + \frac{12}{6} + \frac{12}{12}\end{aligned}$$

denn

$$\begin{aligned}\mathrm{Stab}\,(1) &= \left\{e, \sigma^4, \sigma^8\right\} \\ \mathrm{Stab}\,(5) &= \left\{e, \sigma^3, \sigma^6, \sigma^9\right\} \\ \mathrm{Stab}\,(6) &= \left\{e, \sigma^2, \sigma^4, \sigma^6, \sigma^8, \sigma^{10}\right\} \\ \mathrm{Stab}\,(10) &= \left\{e, \sigma^1, \sigma^2, ..., \sigma^{11}\right\} = G\end{aligned}$$

Eine weitere Anwendung ist die Klassifikation von Graphen bis auf Isomorphie:

Definition 2.2.54 *Ein (ungerichteter)* ***Graph*** *ist ein Paar*

$$G = (E, K)$$

aus einer Menge E von Ecken und einer symmetrischen Teilmenge

$$K \subset E \times E$$

von Kanten. Sind (E, K) und (E', K') Graphen, dann ist ein ***Morphismus von Graphen***

$$\varphi : (E, K) \longrightarrow (E', K')$$

eine Abbildung

$$\varphi : E \longrightarrow E'$$

sodass

$$(\varphi_E \times \varphi_E)(K) \subset K'$$

Ein ***Isomorphismus von Graphen*** *ist ein Morphismus*

$$\varphi : (E, K) \longrightarrow (E', K')$$

sodass

$$\varphi_E : E \longrightarrow E'$$

bijektiv ist und

$$\left(\varphi_E^{-1} \times \varphi_E^{-1}\right)(K') \in K$$

Dann gibt

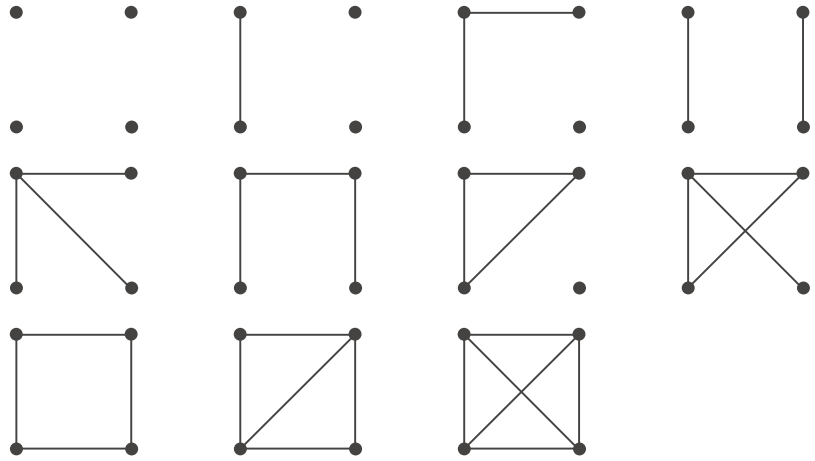
$$\varphi_E \times \varphi_E : E \times E \longrightarrow E' \times E'$$

eine Bijektion

$$K \longrightarrow K'$$

Satz 2.2.55 *Es gibt genau* 11 *Isomorphieklassen von Graphen mit* 4 *Ecken.*

Beweis. Die Graphen



sind offenbar paarweise nicht isomorph. Wir zeigen, dass sie ein vollständiges Repräsentantensystem der Graphen mit 4 Ecken bilden: Sei

$$E = \{1, 2, 3, 4\}$$

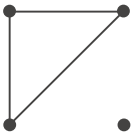
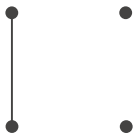
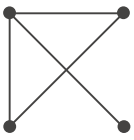
und

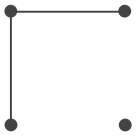
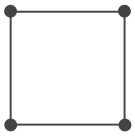
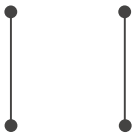
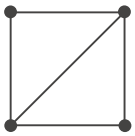
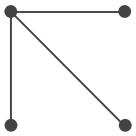
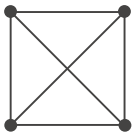
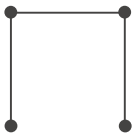
$$M = \{(E, K) \text{ Graph}\}$$

also

$$|M| = 2^{\binom{4}{2}} = 2^6 = 64$$

Die Gruppe $G = S_4$ operiert auf der Menge der Graphen M durch Permutation der Ecken. Wir geben für jeden der obigen Graphen $r = (E, K)$ den Isomorphietyp des Stabilisators und mit Hilfe der Bahnenformel die Länge der Bahn an:

	r	$\mathrm{Stab}(r)$	$\lvert G \cdot r \rvert$		r	$\mathrm{Stab}(r)$	$\lvert G \cdot r \rvert$
1		S_4	1	7		S_3	4
2		$\mathbb{Z}_2 \times \mathbb{Z}_2$	$\frac{24}{4} = 6$	8		$\mathbb{Z}_2$	12

3		$\mathbb{Z}_2$	$\frac{24}{2} = 12$	9		D_4	$\frac{24}{8} = 3$
4		D_4	$\frac{24}{8} = 3$	10		$\mathbb{Z}_2 \times \mathbb{Z}_2$	6
5		S_3	$\frac{24}{6} = 4$	11		S_4	1
6		$\mathbb{Z}_2$	12				

Alle Bahnen zusammen haben also tatsächlich 64 Elemente, also haben wir ein vollständiges Repräsentantensystem gefunden. ■

2.3 Normalteiler

2.3.1 Normalteiler und Quotientengruppe

Sei $H \subset G$ eine Untergruppe und

$$\pi : G \longrightarrow G/H$$

die Quotientenabbildung. Können wir dem Quotienten G/H die Struktur einer Gruppe geben, sodass π ein Gruppenhomomorphismus wird? Wenn ja, dann ist $\ker(\pi) = H$, da

$$\pi(e) = eH = H \in G/H$$

das neutrale Element wäre.

Bemerkung 2.3.1 *Sei*

$$\varphi : G \longrightarrow F$$

ein Gruppenhomomorphismus und

$$H = \ker(\varphi) \subset G$$

Dann gilt für $g \in G$ *und*

$$gHg^{-1} := \left\{ghg^{-1} \mid h \in H\right\}$$

dass

$$gHg^{-1} = H$$

Denn

$$\begin{aligned} & h \in \ker\varphi \Rightarrow \\ \varphi\left(ghg^{-1}\right) &= \varphi(g)\,\varphi(h)\,\varphi(g)^{-1} = \varphi(g)\,\varphi(g)^{-1} = e \\ & \Rightarrow ghg^{-1} \in H \\ & \Rightarrow gHg^{-1} \subset H \end{aligned}$$

somit

$$H \supset gHg^{-1} \supset g\left(g^{-1}Hg\right)g^{-1} = H$$

also gilt Gleichheit.

Gruppen, die diese Eigenschaft des Kerns haben, nennt man Normalteiler:

Definition 2.3.2 *Sei* $H \subset G$ *eine Untergruppe.* H *heißt* ***Normalteiler*** *von* G *(in Zeichen* $H \lhd G$*), wenn*

$$gHg^{-1} = H \ \ \forall g \in G$$

(äquivalent ist $gH = Hg \ \ \forall g \in G$ *oder* $gHg^{-1} \subset H \ \ \forall g \in G$ *oder* $\kappa_g(H) \subset H \ \ \forall g \in G$*).*

Allgemeiner als das obige Beispiel gilt:

Bemerkung 2.3.3 *Ist* $\varphi : G \longrightarrow F$ *ein Gruppenhomomorphismus und* $M \subset F$ *ein Normalteiler, dann ist* $\varphi^{-1}(M) \subset G$ *ein Normalteiler. Ist* φ *surjektiv und* $N \subset G$ *ein Normalteiler, dann ist* $\varphi(N) \subset F$ *ein Normalteiler.*

Dies zeigen wir in Übungsaufgabe 2.22.

Beispiel 2.3.4 *Sei G eine Gruppe.*

1) $\mathrm{Inn}(G)$ *ist ein Normalteiler von* $\mathrm{Aut}(G)$.

2) Das Zentrum $Z(G)$ *ist ein Normalteiler von* G.

Satz 2.3.5 *Sei $H \subset G$ eine Untergruppe. Die Menge G/H trägt genau dann die Struktur einer Gruppe, sodass*

$$\pi : G \longrightarrow G/H$$

ein Gruppenhomomorphismus ist, wenn H ein Normalteiler ist. Wir bezeichnen dann G/H als die ***Quotientengruppe****.*

Beweis. Die Notwendigkeit, dass H Normalteiler ist, haben wir schon gezeigt. Die Bedingung ist auch hinreichend: Sei $H \subset G$ Normalteiler. Ist π Gruppenhomomorphismus, dann muss

$$aH \cdot bH = abH$$

für die Verknüpfung auf G/H gelten. Zu zeigen bleibt: Durch diese Formel wird eine wohldefinierte Verknüpfung gegeben, d.h. haben wir andere Repräsentanten

$$a_2 \in aH \qquad b_2 \in bH$$

müssen wir zeigen, dass

$$a_2 b_2 H = abH$$

Sei

$$a_2 = ah \qquad b_2 = bh'$$

mit $h, h' \in H$. Da H Normalteiler ist, gilt

$$bHb^{-1} = H \Longleftrightarrow bH = Hb$$

also existiert ein $h'' \in H$ mit

$$hb = bh''$$

und damit

$$a_2b_2H = ahbh'H = abh''h'H = abH$$

da $h', h'' \in H$.

Wir zeigen, dass diese wohldefinierte Verknüpfung auf G/H tatsächlich eine Gruppenstruktur definiert:

$$(aHbH)\,cH = aH\,(bHcH)$$

folgt aus $(ab)\,c = a\,(bc)$.

$$eH = H$$

ist das neutrale Element. Das Inverse ist

$$(aH)^{-1} = a^{-1}H$$

■

Beispiel 2.3.6 *Jede Untergruppe einer abelschen Gruppe ist ein Normalteiler. Zum Beispiel sind die Untergruppen* $\langle n\rangle = n\mathbb{Z} \subset (\mathbb{Z}, +)$ *Normalteiler, denn*

$$a + n\mathbb{Z} - a = \{a + kn - a \mid k \in \mathbb{Z}\} = n\mathbb{Z}$$

und die Quotientengruppen sind die Restklassengruppen

$$\mathbb{Z}/\langle n\rangle = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/n$$

Bemerkung 2.3.7 *Jede Untergruppe* $U \subset G$ *vom Index* $[G : U] = 2$ *ist ein Normalteiler von* G.

Der kurze Beweis ist Teil von Übungsaufgabe 2.32.

Gruppen kann man auch konstruieren, indem man auf einer freien Gruppe bestimmte Rechenregeln (Relationen) fordert:

Definition 2.3.8 *Sei*

$$A = \{g_1, ..., g_n\}$$

eine endliche Menge und F *die freie Gruppe erzeugt von* A *(mit neutralem Element* e*). Seien* $r_1, ..., r_s$ *Elemente von* F *und* N *der kleinste Normalteiler von* F*, der* $r_1, ..., r_s$ *enthält. Dann heißt*

$$\langle g_1, ..., g_n \mid r_1 = e, ..., r_s = e\rangle := F/N$$

die Gruppe mit ***Erzeugern*** g_i ***und Relationen*** r_i.

Siehe auch Übungsaufgabe 2.21 für eine Beschreibung der S_n durch Erzeuger und Relationen.

Beispiel 2.3.9 *Die Symmetriegruppe W des Würfels wird nach Übungsaufgabe 2.19 von der Drehung*

$$\alpha = (2,3,5,4)$$

um $90°$ und der Drehspiegelung

$$\beta = (1,5,3,6,2,4)$$

um $60°$ erzeugt. Der folgende GAP-Code zeigt, dass sich W durch Erzeuger und Relationen beschreiben lässt als

$$W \cong \left\langle \alpha, \beta \mid \alpha^4 = e,\ \beta^6 = e,\ (\alpha\beta)^2 = e,\ \left(\alpha^{-1}\beta^2\right)^2 = e \right\rangle$$

```
f:=FreeGroup("a", "b");
g:=f/[f.1^4, f.2^6, (f.1*f.2)^2, (f.1^3*f.2^2)^2];
W:=Group((2,3,5,4), (1,5,3,6,2,4));
IsomorphismGroups(g,W);
```

2.3.2 Konjugationsklassen von Untergruppen

Konjugation liefert eine Operation auf der Menge der Untergruppen einer Gruppe G:

Bemerkung 2.3.10 *Ist $U \subset G$ eine Untergruppe und $g \in G$, dann ist die Menge*

$$gUg^{-1} := \left\{ gug^{-1} \mid u \in U \right\} \subset G$$

als Bild von U unter dem Isomorphismus

$$\left(h \mapsto g \cdot h \cdot g^{-1}\right) \in \mathrm{Inn}\,(G) \subset \mathrm{Aut}\,(G)$$

eine zu U isomorphe Untergruppe von G.

Definition 2.3.11 *G operiert auf der Menge S der Untergruppen von G durch Konjugation*

$$\begin{array}{ccc} G \times S & \to & S \\ (g,U) & \mapsto & gUg^{-1} \end{array}$$

Die Bahnen

$$U^G = \left\{ gUg^{-1} \mid g \in G \right\}$$

für $U \in S$ heißen die ***Konjugationsklassen von Untergruppen****.*

Ein Normalteiler ist also eine Untergruppe $U \subset G$, die invariant unter Konjugation ist. Dies ist der Fall genau dann, wenn die Konjugationsklasse nur ein Element hat, d.h.

$$U^G = \{U\}$$

Wir haben schon an Beipielen gesehen, dass sich Stabilisatoren von Ecken eines Platonischen Körpers gleich verhalten. Der Grund ist, dass sie konjugierte Untergruppen der Symmetriegruppe sind, z.B.:

Beispiel 2.3.12 *Wir betrachten S_4 als Symmetriegruppe des Tetraeders (Abbildung 2.3). Dann ist*

$$\operatorname{Stab}(4) = \langle (1,2), (2,3) \rangle \cong S_3$$

und

$$\begin{aligned} \operatorname{Stab}(1) &= \langle (2,4), (2,3) \rangle \\ &= (1,4) \cdot \langle (1,2), (2,3) \rangle \cdot (1,4)^{-1} \end{aligned}$$

Allgemein zeigen wir:

Satz 2.3.13 *Ist $G \times M \to M$ eine Operation und sind $n, m \in M$ in der selben Bahn etwa $n = g \cdot m$, dann sind die Stabilisatoren konjugiert*

$$\operatorname{Stab}(n) = g \operatorname{Stab}(m) g^{-1}$$

Beweis. Sei $v = gug^{-1}$ mit $u \in \operatorname{Stab}(m)$, dann

$$v \cdot n = vg \cdot m = gu \cdot m = g \cdot m = n$$

also $v \in \operatorname{Stab}(n)$ und somit

$$g \operatorname{Stab}(m) g^{-1} \subset \operatorname{Stab}(n)$$

Aus $m = g^{-1} \cdot n$ folgt analog $g^{-1} \operatorname{Stab}(n) g \subset \operatorname{Stab}(m)$ also

$$\operatorname{Stab}(n) \subset g \operatorname{Stab}(m) g^{-1}$$

■

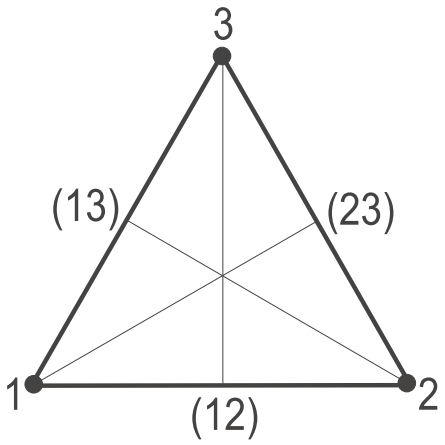


Abbildung 2.6: Symmetriegruppe des Dreiecks und Konjugation

Beispiel 2.3.14 *Sei G die Symmetriegruppe des gleichseitigen Dreiecks, also $G = S_3$ und $|G| = 3! = 6$. Also kann G nach der Indexformel Untergruppen der Ordnungen $1, 2, 3, 6$ haben.*

Ist $|H| = 1$, dann $H = \{e\}$. Die Ordnung $|H| = 2$ hat z.B.

$$H_{12} = \{e, (12)\}$$

H_{12} ist kein Normalteiler: Konjugation mit (23) liefert

$$(23)\, e\, (23)^{-1} = e$$
$$(23)\,(12)\,(23) = (13) \notin H_{12}$$

Es ist

$$(23)\, H_{12}\, (23) = H_{13} = \{e, (13)\}$$

Ist $|H| = 3$, dann

$$H = \{e, (123), (132)\}$$

Dies ist ein Normalteiler und $H \cong A_3$ ist die Untergruppe der Drehungen in G.

Für

$$H = \{\mathrm{id}, (123), (132)\}$$

ist

$$\begin{aligned} G/H &= \{H, (1,2)\, H\} \\ &\cong \mathbb{Z}/2 \cong (\{\pm 1\}, \cdot) \end{aligned}$$

Der Isomorphismus $G/H \to (\{\pm 1\}, \cdot)$ *wird induziert durch den Signumshomomorphismus*

$$\operatorname{sign}: \quad S_3 \quad \to \quad (\{\pm 1\}, \cdot)$$

denn für alle $\sigma \in H$ *ist* $\operatorname{sign}(\sigma) = 1$ *und für alle*

$$\sigma \in (1,2)\, H = \{(1,2), (1,3), (2,3)\}$$

ist $\operatorname{sign}(\sigma) = -1$. *Wir beobachten, dass* $H = A_3 = \ker \operatorname{sign}$. *Wir werden im nächsten Abschnitt 2.3.3 Isomorphismen wie*

$$S_3/\ker \operatorname{sign} \cong (\{\pm 1\}, \cdot)$$

allgemein behandeln.

In Übungsaufgabe 2.25 berechnen wir die Konjugationsklassen von Untergruppen der S_4.

2.3.3 Homomorphiesatz und Isomorphiesätze

Ist $\varphi : G \longrightarrow F$ ein Monomorphismus, dann können wir $G \cong \operatorname{Bild}(\varphi) \subset F$ als Untergruppe von F auffassen. Anderenfalls kann man φ mittels der Quotientengruppenkonstruktion injektiv machen:

Satz 2.3.15 (Homomorphiesatz) *Sei* $\varphi : G \longrightarrow F$ *ein Gruppenhomomorphismus. Dann gilt*

$$G/\ker \varphi \cong \operatorname{Bild}(\varphi)$$

Beweis. Wir definieren

$$\begin{aligned} \widetilde{\varphi} &: G/\ker \varphi \longrightarrow \operatorname{Bild} \varphi \\ \widetilde{\varphi}(a \ker \varphi) &:= \varphi(a) \end{aligned}$$

Dies ist wohldefiniert, da

$$\begin{aligned} a' = ah \in a\ker\varphi \text{ mit } h \in \ker\varphi \\ \Rightarrow \varphi(a') = \varphi(a)\cdot\varphi(h) = \varphi(a)\cdot e = \varphi(a) \end{aligned}$$

$\widetilde{\varphi}$ ist offenbar ein Epimorphismus, surjektiv, und $\widetilde{\varphi}$ ist injektiv, denn

$$\begin{aligned} \widetilde{\varphi}(a\ker\varphi) = e \\ \Rightarrow \varphi(a) = e \Rightarrow a \in \ker\varphi \\ \Rightarrow a\ker\varphi = \ker\varphi = e_{G/\ker\varphi} \end{aligned}$$

■

Also faktorisiert $\varphi : G \longrightarrow F$ in

$$\begin{array}{ccccc} & G & \xrightarrow{\varphi} & F & \\ \text{Projektion} & \downarrow & & \uparrow & \text{Inklusion} \\ & G/\ker\varphi & \cong & \text{Bild}\,\varphi & \end{array}$$

Siehe auch Übungsaufgabe 2.31.

Beispiel 2.3.16 *Da* $Z(G) = \ker\kappa$ *und* $\text{Inn}(G) = \text{Bild}\,\kappa$ *für*

$$\begin{array}{rccc} \kappa: & G & \longrightarrow & \text{Aut}(G) \\ & a & \longmapsto & (g \longmapsto aga^{-1}) \end{array}$$

gilt

$$\text{Inn}(G) \cong G/Z(G)$$

Beispiel 2.3.17 *Ist* $g \in G$*, dann kann die Ordnung* $\text{ord}(g)$ *endlich oder unendlich sein. Ist* $\text{ord}(g)$ *unendlich, dann ist*

$$\begin{array}{rccc} \varphi: (\mathbb{Z},+) & \longrightarrow & \langle g\rangle \subset G \\ k & \longmapsto & g^k \end{array}$$

ein Isomorphismus. Anderenfalls ist $\ker\varphi = \langle n\rangle$ *mit*

$$n = \min\left\{k \geq 1 \mid g^k = e\right\} = \text{ord}(g)$$

und mit dem Homomorphiesatz

$$\mathbb{Z}/\langle n\rangle \cong \langle g\rangle$$

Somit haben wir gezeigt: Hat eine zyklische Gruppe endliche Ordnung, dann ist sie isomorph zu $\mathbb{Z}/\langle n\rangle$ *für ein* $n > 0$*, anderenfalls isomorph zu* $\mathbb{Z}$*.*

Anwendungen des Homomorphiesatzes sind:

Satz 2.3.18 (Erster Isomorphiesatz) *Sei G eine Gruppe, $H \subset G$ eine Untergruppe und N ein Normalteiler von G. Dann gilt*

1) Die Teilmenge

$$HN = \{hn \mid h \in H,\ n \in N\}$$

ist eine Untergruppe von G und N ist ein Normalteiler von HN .

2) $H \cap N$ ist ein Normalteiler von H.

3) Wir haben einen Isomorphismus

$$\begin{array}{ccc} H/H\cap N & \cong & HN/N \\ a\,(H\cap N) & \longmapsto & aN \end{array}$$

Beweis. Wir bemerken zunächst, dass wir im folgenden Beweis nicht wirklich benötigen, dass N ein Normalteiler von G ist, sondern nur, dass N von H **normalisiert** wird, d.h. $hN = Nh$ für alle $h \in H$.

1) Sind $h_1n_1, h_2n_2 \in HN$, dann

$$h_1n_1h_2n_2 = h_1h_2n_1'n_2 \in HN$$

denn es gibt ein $n_1' \in N$ mit $n_1h_2 = h_2n_1'$ wegen $Nh_2 = h_2N$.
Ebenso gilt für das Inverse

$$(h_1n_1)^{-1} = n_1^{-1}h_1^{-1} = h_1^{-1}n' \in HN$$

mit $n' \in N$.

$$N \subset HN$$

ist ein Normalteiler, da $N \subset G$ ein Normalteiler ist, also

$$gNg^{-1} = N \ \forall g \in G$$

und dies somit auch für alle Elemente aus HN gilt.

2) $H \cap N \subset H$ ist eine Untergruppe. Sie ist Normalteiler, da

$$h(H \cap N)h^{-1} \subset hHh^{-1} \cap hNh^{-1} = H \cap N \ \forall h \in H$$

und somit $h(H \cap N)h^{-1} = H \cap N \ \forall h \in H$.

3) Die Abbildung

$$\begin{array}{rccc} \varphi: & H & \longrightarrow & HN/N \\ & a & \longmapsto & aN \end{array}$$

ist ein Gruppenhomomorphismus und surjektiv, da jede Nebenklasse von der Form

$$hnN = hN$$

für $h \in H$ ist. Weiter ist

$$\ker\varphi = \{a \in H \mid aN = N\} = H \cap N$$

Der Homomorphiesatz liefert

$$H/H \cap N = H/\ker\varphi \cong \text{Bild}\,\varphi = HN/N$$

■

Wir haben also ein Diagramm

$$\begin{array}{ccc} N & \lhd & HN \\ \cup & & \cup \\ H \cap N & \lhd & H \end{array}$$

Beispiel 2.3.19 *Sei $G = (\mathbb{Z}, +)$ und $H = m\mathbb{Z}$ und $N = n\mathbb{Z}$ die zyklischen Untergruppen erzeugt von m und n. Dann ist*

$$H \cap N = \text{kgV}(n, m)\,\mathbb{Z}$$

denn $a \in H \cap N \Leftrightarrow n \mid a$ und $m \mid a \Leftrightarrow \text{kgV}(n, m) \mid a$. Zum Beispiel:

$$\begin{aligned} 6\mathbb{Z} &= \{..., -6, 0, 6, 12, 18, 24, 30...\} \\ 10\mathbb{Z} &= \{..., -10, 0, 10, 20, 30, ...\} \end{aligned}$$

und

$$6\mathbb{Z} \cap 10\mathbb{Z} = 30\mathbb{Z} = \{..., -30, 0, 30, 60, ...\}$$

Weiter ist

$$HN = m\mathbb{Z} + n\mathbb{Z} = \{mu + nv \mid u, v \in \mathbb{Z}\} = \mathrm{ggT}\,(n, m)\,\mathbb{Z}$$

denn $\mathrm{ggT}\,(n, m) \mid (un + vm)$ *für alle* $u, v \in \mathbb{Z}$ *und* $\mathrm{ggT}\,(n, m) \in HN$*, da der erweiterte Euklidische Algorithmus* $x, y \in \mathbb{Z}$ *liefert mit*

$$xn + ym = \mathrm{ggT}\,(n, m)$$

Zum Beispiel

$$6\mathbb{Z} + 10\mathbb{Z} = \{..., -2, 0, 2, 4, 6, 10, ...\} = 2\mathbb{Z}$$

da $2 = 2 \cdot 6 + (-1) \cdot 10$*.*

Der erste Isomorphiesatz liefert somit

$$\begin{array}{ccc} m\mathbb{Z} \,/\, \mathrm{kgV}\,(n, m)\,\mathbb{Z} & \cong & \mathrm{ggT}\,(n, m)\,\mathbb{Z} \,/\, n\mathbb{Z} \\ a + \mathrm{kgV}\,(n, m)\,\mathbb{Z} & \mapsto & a + n\mathbb{Z} \end{array}$$

Im Beispiel $m = 6$ *und* $n = 10$ *also*

$$\begin{gathered} 6\mathbb{Z} \,/\, 30\mathbb{Z} \;\cong\; 2\mathbb{Z} \,/\, 10\mathbb{Z} \\ \overline{0} \mapsto \overline{0} \\ \overline{6} \mapsto \overline{6} \\ \overline{12} \mapsto \overline{2} \\ \overline{18} \mapsto \overline{8} \\ \overline{24} \mapsto \overline{4} \end{gathered}$$

Da für $w \mid u$ *die Untergruppe* $u\mathbb{Z} \subset w\mathbb{Z}$ *den Index*

$$|w\mathbb{Z}/u\mathbb{Z}| = \frac{u}{w}$$

hat (und isomorphe Gruppen die selbe Gruppenordnung), folgt

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

also

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

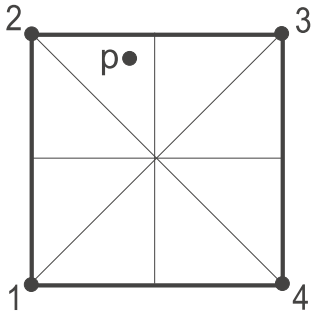


Abbildung 2.7: Symmetriegruppe des Quadrats

Satz 2.3.20 (Zweiter Isomorphiesatz) *Seien M, N Normalteiler von G und $M \subset N$. Dann gilt:*

1) N/M ist ein Normalteiler in G/M.

2) Es gibt einen Isomorphismus

$$(G/M)\,/\,(N/M) \cong G/N$$

Beweis. Die Abbildung

$$\begin{array}{rccc} \varphi: & G/M & \longrightarrow & G/N \\ & aM & \longmapsto & aN \end{array}$$

ist wegen $M \subset N$ ein wohldefinierter Gruppenhomomorphismus und surjektiv. Weiter ist

$$\begin{aligned} \ker\varphi &= \{aM \mid aN = N\} \\ &= \{aM \mid a \in N\} = N/M \end{aligned}$$

also N/M ein Normalteiler in G/M und mit dem Homomorphiesatz

$$(G/M)\,/\,(N/M) = (G/M)\,/\ker\varphi \cong \text{Bild}\,\varphi = G/N$$

■

Beispiel 2.3.21 *Sei $G = D_4 \subset S_4$ die Symmetriegruppe des Quadrats. Der Punkt p hat trivialen Stabilisator und Orbit der Länge 8 und damit $|D_4| = 8$.*

Die Untergruppe der Drehungen um $0°$, $90°$, $180°$ *und* $270°$

$$\mathbb{Z}/4 \cong N = \{(), (1,2,3,4), (1,3)(2,4), (1,4,3,2)\} \subset G$$

hat Index 2*, ist also ein Normalteiler. Dies sehen wir auch direkt: Eine Komposition von Drehungen und Spiegelungen mit einer geraden Zahl von Spiegelungen ist eine Drehung.*

Die verbleibenden 4 *Elemente von* G *sind die Spiegelungen*

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

Die Untergruppe

$$M = \{(), (1,3)(2,4)\} \subset N \subset G$$

ist ein Normalteiler von G *(und damit auch von* N*), denn* M *ist das Zentrum von* G*:*

Die Drehung $(1,3)(2,4)$ *um* $180°$ *(und natürlich das neutrale Element) vertauschen mit allen Drehungen und Spiegelungen. Weitere Elemente liegen nicht im Zentrum, denn die Spiegelungen an den Koordinatenachsen sind zueinander konjugiert, ebenso die Spiegelungen an den Diagonalen und die Drehung um* $90°$ *ist konjugiert zu der Drehung um* $270°$*.*

Wir haben also Normalteiler und Quotientengruppen

$$\begin{array}{lll} D_4 = & G & \\ & \triangledown & G/N = \{N,\ \{(13), (24), (12)(34), (14)(23)\}\} \cong \mathbb{Z}/2 \\ \mathbb{Z}/4 \cong & N & \\ & \triangledown & N/M = \{M,\ \{(1234), (1432)\}\} \cong \mathbb{Z}/2 \\ \mathbb{Z}/2 \cong & M & \end{array}$$

denn G/N *besteht aus genau zwei Nebenklassen,* N *und dessen Komplement in* G*. Ebenso besteht* N/M *aus* M *und dessen Komplement in* N*.*

Die Quotientengruppe G/M *hat* 4 *Elemente,*

$$\left.\begin{array}{l} e := M = \{(), (13)(24)\} \\ a := (1234)M = \{(1234), (1432)\} \end{array}\right\} N/M$$
$$b := (13)M = \{(13), (24)\}$$
$$c := (12)(34)M = \{(12)(34), (14)(23)\}$$

Beachte $N/M = \{e, a\} \subset G/M$. *Die Verknüpfungstafel von* G/M *ist*

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

denn

$$\begin{aligned} bc &= (13)\,(12)\,(34)\,M = (1,2,3,4)\,M = a \\ &= (1,4,3,2)\,M = cb \end{aligned}$$

und offensichtlich $b^2 = e$, $c^2 = e$, *also auch* $a^2 = e$.

Somit ist

$$G/M \cong \mathbb{Z}/2 \times \mathbb{Z}/2$$

und es gilt

$$(G/M)\,/\,(N/M) \cong G/N$$

wie im zweiten Isomorphiesatz behauptet.

Die weiteren Normalteiler von G *sind die Kleinsche Vierergruppe*

$$V_4 = \{(),\,(14)\,(23),\,(13)\,(24),\,(12)\,(34)\}$$

und

$$\{(),\,(13),\,(24),\,(13)\,(24)\}$$

beide von Index 2.

V_4 *hat die Normalteiler (von Index* 2*)*

$$\{(),\,(1,3)\,(2,4)\}$$
$$\{(),\,(1,2)\,(3,4)\}$$
$$\{(),\,(1,4)\,(2,3)\}$$

die jedoch keine Normalteiler in G *sind, somit sehen wir, dass aus* $N_2 \triangleleft N_1 \triangleleft G$ *nicht folgt* $N_2 \triangleleft G$.

Für ein weiteres Beispiel siehe Übungsaufgabe 2.32.

2.3.4 Semidirektes Produkt

Wie setzt sich S_n, $n \geq 3$, aus dem Normalteiler

$$G = A_n = \ker\left(\text{sign} : S_n \to \{\pm 1\}\right)$$

und dem Quotienten

$$S_n/A_n \cong \{\pm 1\} \cong \mathbb{Z}/2$$

den wir aus dem Homomorphiesatz erhalten, zusammen? Es gibt Untergruppen der S_n der Ordnung 2, die isomorph zum Quotienten sind, z.B.

$$H = \langle (1,2) \rangle \overset{\text{sign}}{\to} \{\pm 1\}$$

ist ein Isomorphismus. Wir können jedes Element von S_n schreiben als $g \cdot h$ mit $g \in G$ und $h \in H$, denn S_n ist die disjunkte Vereinigung der Nebenklassen A_n und $(1,2)\,A_n = A_n\,(1,2)$. Die Multiplikation von solchen "Tupeln" $g \cdot h$ ist jedoch nicht die Verknüpfung des kartesischen Produkts $G \times H$

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

die wir schon in Beispiel 2.2.3(7.) kennengelernt haben, d.h. im Allgemeinen ist

$$g_1 \cdot h_1 \cdot g_2 \cdot h_2 \neq g_1 \cdot g_2 \cdot h_1 \cdot h_2$$

Das Vertauschen von h_1 und g_2 ersetzt g_2 durch $h_1 \cdot g_2 \cdot h_1^{-1}$

$$g_1 \cdot h_1 \cdot g_2 \cdot h_2 = g_1 \cdot \left(h_1 \cdot g_2 \cdot h_1^{-1}\right) \cdot h_1 \cdot h_2$$

immerhin ist aber noch $h_1 \cdot g_2 \cdot h_1^{-1} \in G$, denn $G \subset S_n$ war ein Normalteiler. Wir können also die Verknüpfung formulieren als

$$g_1 \cdot h_1 \cdot g_2 \cdot h_2 = g_1 \cdot \kappa_{h_1}(g_2) \cdot h_1 \cdot h_2$$

mit dem Konjugationsautomorphismus κ_{h_1}. Man beachte, dass dieser mit h_1 variiert, d.h. die Verknüpfung ist spezifiziert durch den Gruppenhomomorphismus

$$\begin{array}{rccl} \varphi: & H & \to & \text{Aut}\,(G) \\ & h_1 & \mapsto & \kappa_{h_1} = (g \mapsto h_1 g h_1^{-1}) \end{array}$$

Stellen wir zum Beispiel alle Elemente der S_3 dar als Produkte $g \cdot h$ mit $g \in G = \langle (1,2,3) \rangle$ und $h \in H = \langle (1,2) \rangle$ und multiplizieren etwa

$$(1,3) = (1,2,3) \cdot (1,2) = g_1 \cdot h_1$$

und

$$(1,3,2) = (1,3,2) \cdot () = g_2 \cdot h_2$$

dann erhalten wir nicht das komponentenweise kartesische Produkt

$$g_1 \cdot g_2 \cdot h_1 \cdot h_2 = (1,2,3) \cdot (1,3,2) \cdot (1,2) = (1,2)$$

sondern

$$g_1 \cdot h_1 \cdot g_2 \cdot h_2 = (1,2,3) \cdot \underbrace{\kappa_{(1,2)}(1,3,2)}_{(1,2,3)} \cdot (1,2) = (1,3,2) \cdot (1,2)$$

Diese Idee lässt sich verallgemeinern: Für zwei Gruppen G und H kann man mit Hilfe eines Gruppenhomomorphismus

$$\varphi : H \longrightarrow \mathrm{Aut}(G)$$

die Verknüpfung auf dem kartesischen Produkt $G \times H$ abändern, um eine andere Gruppe zu erhalten. Wir definieren eine neue Verknüpfung auf der Menge $P = G \times H$ durch

$$(g_1, h_1) \circ (g_2, h_2) = (g_1 \cdot \varphi(h_1)(g_2), h_1 \cdot h_2) \tag{2.1}$$

d.h. bevor wir g_1 mit g_2 in G multiplizieren, wenden wir den Automorphismus $\varphi(h_1)$ auf g_2 an.

Bezüglich dieser Verknüpfung sind

$$G \cong G \times \{e_H\} \subset P$$
$$H \cong \{e_G\} \times H \subset P$$

offenbar Untergruppen.

Definition und Satz 2.3.22 *Sei $\varphi : H \longrightarrow \mathrm{Aut}(G)$ ein Gruppenhomomorphismus. Dann ist die Menge $P = G \times H$ mit der*

Verknüpfung aus Gleichung 2.1 eine Gruppe, das ***semidirekte Produkt*** $G \rtimes_\varphi H$ *von* G *und* H *bezüglich* φ*. Weiter ist*

$$G \cong \ G \times \{e_H\} \subset G \rtimes_\varphi H$$

ein Normalteiler, und für die Quotientengruppe gilt

$$(G \rtimes_\varphi H)/G \cong H$$

Dies zeigen wir in Übungsaufgabe 2.33.

Beispiel 2.3.23 *1) Für* $\varphi(h) := \mathrm{id}_G \ \forall h \in H$ *erhalten wir das kartesische Produkt.*

2) Oben haben wir schon gesehen, dass $S_n = A_n \rtimes \mathbb{Z}/2$*. Siehe auch Übung 2.33.*

2.3.5 Klassengleichung

Wir betrachten die Operation einer endlichen Gruppe auf sich selbst von links durch Konjugation (siehe Abschnitt 2.2.4)

$$\begin{array}{ccc} G \times G & \longrightarrow & G \\ (a,b) & \longmapsto & aba^{-1} \end{array}$$

Die Bahnengleichung (Satz 2.2.52) liefert dann für ein vollständiges Repräsentantensystem R der Bahnen (d.h. Konjugationsklassen)

$$|G| = \sum_{r \in R} \frac{|G|}{|\mathrm{Stab}(r)|} = \sum_{r \in R} [G : \mathrm{Stab}(r)]$$

Definition 2.3.24 *Den Stabilisator* $\mathrm{Stab}(r)$ *von* $r \in G$ *unter der Konjugationsoperation nennt man auch den* ***Zentralisator***

$$Z_G(r) = \left\{ g \in G \mid grg^{-1} = r \right\}$$

von r*.*

Als Stabilisator ist $Z_G(r) \subset G$ eine Untergruppe. Man kann den Zentralisator nicht nur für Elemente, sondern auch für beliebige Teilmengen $M \subset G$ durch

$$Z_G(M) = \left\{ g \in G \mid grg^{-1} = r \ \forall r \in M \right\}$$

definieren. Als Spezialfall $M = G$ erhält man das Zentrum $Z(G)$.

Satz 2.3.25 (Klassengleichung) *Sei $R \subset G$ ein vollständiges Repräsentantensystem der Konjugationsklassen. Dann gilt die Klassengleichung*

$$|G| = \sum_{r \in R} [G : Z_G(r)] = |Z(G)| + \sum_{\substack{r \in R \\ r \notin Z(G)}} [G : Z_G(r)]$$

Beweis. Die erste Gleichheit haben wir uns gerade überlegt, für die zweite bemerken wir, dass $Z(G) \subset R$, da die Konjugationsklassen der Elemente im Zentrum einelementig sind, denn ist $r \in Z(G)$, dann gilt $rgr^{-1} = g \ \forall g \in G$ also $g^{-1}rg = r \ \forall g \in G$. ■

Siehe auch Übungsaufgabe 2.35.

Beispiel 2.3.26 *Für $G = D_4$ ist die Klassengleichung*

$$\begin{array}{lrll} & 8 & \text{Klassen } r^{D_4} & Z_{D_4}(r) \\ & \| & & \\ Z(D_4)\left\{\begin{array}{l} \\ \\ \\ \\ \\ \\ \\ \\ \end{array}\right. & 1 & ()^{D_4} & D_4 \\ & + & & \\ & 1 & (1,3)(2,4)^{D_4} & D_4 \\ & + & & \\ & 2 & (1,3)^{D_4} & \{(), (1,3), (1,3)(2,4), (2,4)\} \\ & + & & \\ & 2 & (1,2)(3,4)^{D_4} & \{(), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\} \\ & + & & \\ & 2 & (1,2,3,4)^{D_4} & \{(), (1,2,3,4), (1,3)(2,4), (1,4,3,2)\} \end{array}$$

(wobei wir auch jeweils die Konjugationsklasse und den Zentralisator eines Repräsentanten angeben) und für $G = S_4$

$$\begin{array}{lll} 24 & \text{Klassen } r^{S_4} & Z_{S_4}(r) \\ \| & & \\ 1 & ()^{S_4} & S_4 \\ + & & \\ 3 & (1,2)(3,4)^{S_4} & \langle (1,2), (1,3,2,4) \rangle = D_4 \\ + & & \\ 6 & (1,2)^{S_4} & \{(), (1,2), (3,4), (1,2)(3,4)\} \\ + & & \\ 6 & (1,2,3,4)^{S_4} & \{(), (1,2,3,4), (1,3)(2,4), (1,4,3,2)\} \\ + & & \\ 8 & (1,2,3)^{S_4} & \{(), (1,2,3), (1,3,2)\} \end{array}$$

Mit der Klassengleichung zeigen wir:

Corollar 2.3.27 *Ist G eine Gruppe mit $|G| = p^k$, $k > 0$ und p prim, dann wird $|Z(G)|$ von p geteilt.*

Beweis. Für $r \notin Z(G)$ gibt es ein $g \in G$ mit $rg \neq gr$, d.h.

$$Z_G(r) = \{g \in G \mid gr = rg\} \subsetneq G$$

Somit ist $[G : Z_G(r)] > 1$ und außerdem ein Teiler von $|G| = p^k$, wird also von p geteilt. Wegen der Klassengleichung wird dann auch

$$|Z(G)| = |G| - \sum_{\substack{r \in R \\ r \notin Z(G)}} [G : Z_G(r)]$$

von p geteilt. ■

Zum Beispiel sehen wir sofort, dass die D_4 ein nichttriviales Zentrum hat, also zumindest ein Element $g \neq e$ existieren muss, das mit allen anderen Elementen vertauscht (wie oben schon gesehen, ist dies die Drehung $(1,3)(2,4)$ des Quadrats um 180°).

Lemma 2.3.28 *Sei G eine Gruppe. Ist $G/Z(G)$ zyklisch, dann ist G abelsch.*

Beweis. Sei $G/Z(G) = \langle xZ(G) \rangle$ zyklisch und $g_1, g_2 \in G$. Dann können wir schreiben

$$g_i = x^{k_i} z_i \text{ mit } z_i \in Z(G)$$

(denn g_i liegt in einer Nebenklasse von $Z(G)$ und jede Nebenklasse ist eine Potenz von $xZ(G)$). Somit ist

$$g_1 g_2 = x^{k_1} z_1 x^{k_2} z_2 = x^{k_1+k_2} z_1 z_2 = x^{k_2+k_1} z_2 z_1 = g_2 g_1$$

da z_1, z_2 mit jedem Element von G vertauschen. ■

Corollar 2.3.29 *Ist G eine Gruppe mit $|G| = p^2$ und p prim, dann ist G abelsch.*

Beweis. Da $|Z(G)|$ nach Corollar 2.3.27 von p geteilt wird, ist $|Z(G)| \in \{p, p^2\}$. Für $|Z(G)| = p^2$ gilt $G = Z(G)$ also abelsch. Für $|Z(G)| = p$ ist $|G/Z(G)| = p$, also $G/Z(G)$ mit Corollar 2.2.39 zyklisch. Mit Lemma 2.3.28 ist also G abelsch. ■

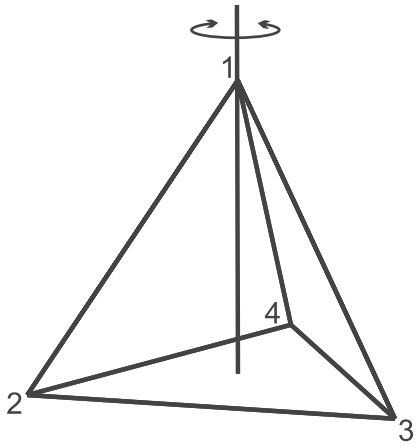


Abbildung 2.8: Dreizählige Drehachse des Tetraeders

2.4 Sylowsätze

Zur Klassifikation von Gruppen ist die Kenntnis des Untergruppenverbands einer gegebenen Gruppe G wichtig. Wir wissen schon, dass die Ordnung jeder Untergruppe $|G|$ teilt.

Andererseits können wir uns fragen, für welche Teiler von $|G|$ wirklich eine Untergruppe von G mit entsprechender Ordnung existiert (und wieviele). Zunächst werden wir zeigen, dass es zumindest zu jedem Primpotenzteiler p^j eine Untergruppe gibt.

Beispiel 2.4.1 *Die Symmetriegruppe* $\mathrm{Sym}\,(T) \cong S_4$ *des regulären Tetraeders* T *hat Ordnung*

$$|\mathrm{Sym}\,(T)| = 24 = 2^3 \cdot 3$$

Wir kennen schon alle Untergruppen der Ordnung 3*: Es sind die zyklischen Gruppen*

$$\{(), (1,2,3), (1,3,2)\}$$
$$\{(), (2,3,4), (2,4,3)\}$$
$$\{(), (1,2,4), (1,4,2)\}$$
$$\{(), (1,3,4), (1,4,3)\}$$

jeweils erzeugt von einer der 4 *Drehungen um* $120°$ *wie in Abbildung*

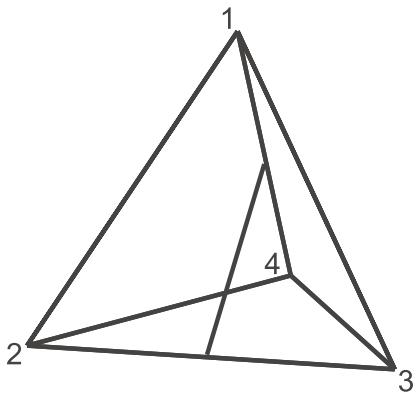


Abbildung 2.9: Kantenmittendiagonale im Tetraeder

2.8. Die Stabilisatoren von Kantenmittendiagonalen wie in Abbildung 2.9 haben Ordnung $2^3 = 8$*, denn sie sind isomorph zur Symmetriegruppe des Quadrats* D_4*. Dies sieht man, wenn man die Zeichenebene senkrecht zur jeweiligen Kantenmittendiagonale legt (Abbildung 2.10). Es gibt* 3 *Untergruppen der Ordnung* 8 *entsprechend den* 3 *Kantenmittendiagonalen.*

Untergruppen der Ordnung 4 *werden z.B. von* 4*-Zykeln, d.h. Drehspiegelungen, erzeugt, Untergruppen der Ordnung* 2 *von Spiegelungen. Insgesamt haben wir gesehen, dass die* S_4 *Untergruppen der Ordnungen* $1, 2, 4, 8$ *und* 3 *hat. Man beachte, dass darüber hinaus auch Untergruppen der* S_4 *der Ordnung* 6 *(Stabilisatoren von Ecken),* 12 *(die Gruppe der Drehsymmetrien von* T*) und natürlich* 24 *existieren.*

Man kann sich nun, motiviert durch das Beispiel der S_4, fragen, ob es eventuell zu jedem Teiler der Gruppenordnung eine Untergruppe mit entsprechender Ordnung gibt. Das folgende Beispiel zeigt, dass dies nicht der Fall ist:

Beispiel 2.4.2 *Die Gruppe* $A_4 = \{\sigma \in S_n \mid \operatorname{sign}\sigma = 1\} \subset S_4$ *der Rotationssymmetrien des Tetraeders (von Ordnung* $|A_4| = \frac{24}{2} = 12$*) hat keine Untergruppe der Ordnung* 6*:*

Angenommen $N \subset A_4$ *ist ein Normalteiler mit* $|N| = 6$*. Sei weiter* H *eine Untergruppe (von Ordnung* $|H| = 3$*) erzeugt von einer Drehung um* 120°*. Mit dem* 1*. Isomorphiesatz gilt*

$$|H| \cdot |N| = |HN| \cdot |H \cap N|$$

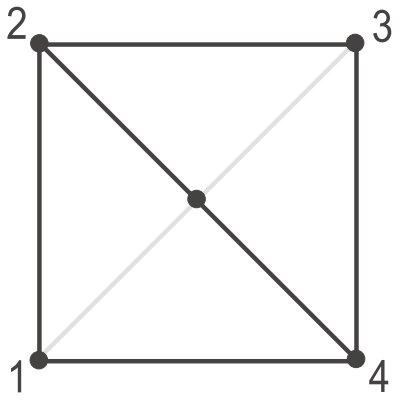


Abbildung 2.10: Tetraeder in Zeichenebene senkrecht zu einer Kantenmittendiagonale

somit

$$12 = |A_4| \geq |HN| = \frac{|H| \cdot |N|}{|H \cap N|} = \frac{3 \cdot 6}{|H \cap N|}$$

also $H \subset N$. *Die Untergruppe* N *enthält somit alle* 3*-Zykel. Diese erzeugen aber schon die ganze* A_4*, denn jeder* $2+2$*-Zykel ist Produkt von* 3*-Zykeln*

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

Es muss also nicht zu jedem Teiler der Gruppenordnung eine Untergruppe geben.

2.4.1 Existenz von p-Gruppen

Definition 2.4.3 *Sei* p *eine Primzahl. Eine* ***p-Gruppe*** *ist eine Gruppe* G*, in der jedes Element* $g \in G$ *als Ordnung eine* p*-Potenz hat, d.h.* $\operatorname{ord}(g) = p^l$ *für ein* $l \geq 0$.

Eine endliche Gruppe G der Ordnung $|G| = p^k$ ist demzufolge eine p-Gruppe, denn die Ordnung jedes Elements teilt die Gruppenordnung. Die Umkehrung für endliche Gruppen ergibt sich als Corollar zu folgendem zentralen Satz:

Satz 2.4.4 *Sei* G *eine endliche Gruppe und* p *eine Primzahl, die* $|G|$ *teilt, etwa*

$$|G| = p^k m$$

mit $p \nmid m$. Dann existiert für jedes l mit $0 \leq l \leq k$ eine Untergruppe $H \subset G$ der Ordnung

$$|H| = p^l$$

Corollar 2.4.5 *Sei G eine endliche Gruppe und p eine Primzahl. Teilt p die Gruppenordnung $|G|$, dann gilt:*

1) (Cauchy) Es gibt ein Element der Ordnung p in G.

2) G ist eine p-Gruppe genau dann, wenn $|G| = p^l$ mit $l \geq 0$.

Beweis. Nach Satz 2.4.4 gibt es eine Untergruppe der Ordnung p. Diese ist zyklisch $H = \langle g \rangle$ mit $\operatorname{ord}(g) = p$.

Die Aussage $|G| = p^l \Rightarrow G$ ist eine p-Gruppe haben wir schon gezeigt. Für die Umkehrung schreibe $|G| = p^l \cdot m$ mit $l \geq 0$, $m > 1$ und $p \nmid m$. Dann existiert ein Element der Ordnung q, wobei q ein Primteiler von m ist. Somit ist G keine p-Gruppe. ■

Beispiel 2.4.6 *Wir illustrieren die Beweisidee des Existenzsatzes 2.4.4 am Beispiel von $G = S_3$, indem wir einen Algorithmus beschreiben, der z.B. eine Untergruppe der Ordnung 3 findet:*

Dazu betrachten wir die Menge X aller 3-elementigen Teilmengen von G und suchen ein $A \in X$, sodass die Länge der Bahn GA von A unter der Translation

$$\begin{aligned} G \times X &\longrightarrow X \\ (g, A) &\longmapsto gA = \{ga \mid a \in A\} \end{aligned}$$

nicht durch 3 teilbar (und somit 2) ist. Dann ist der Stabilisator $\operatorname{Stab}(A)$ eine Untergruppe der Ordnung $\frac{|G|}{|GA|} = 3$.

Zum Beispiel bilden folgende 3-elementigen Teilmengen von G eine Bahn der Länge 6

$$A = \left.\begin{array}{llll} \{ & (), & (1,3), & (2,3) \} \\ \{ & (1,2), & (1,3,2), & (1,2,3) \} \\ \{ & (2,3), & (1,2,3), & () \} \\ \{ & (1,3), & (), & (1,3,2) \} \\ \{ & (1,2,3), & (2,3), & (1,2) \} \\ \{ & (1,3,2), & (1,2), & (1,3) \} \end{array}\right\} = GA$$

Ebenso haben

$$A = \{(), (1,2), (1,3)\}$$

und

$$A = \{(), (1,2), (2,3)\}$$

Bahnen der Länge 6.

Da X insgesamt $\binom{6}{3} = 20$ Elemente hat, fehlt nur noch die folgende (gesuchte) Bahn der Länge 2*:*

$$A = \left.\begin{array}{llll} \{ & (1,2), & (1,3), & (2,3) \quad \} \\ \{ & (), & (1,3,2), & (1,2,3) \quad \} \end{array}\right\} = GA$$

Der Stabilisator von A ist

$$\{(), (1,3,2), (1,2,3)\}$$

also eine Untergruppe der Ordnung 3.

Für die Existenz einer solchen Bahn der gesuchten Länge verwenden wir allgemein folgendes Lemma:

Lemma 2.4.7 *Sei p eine Primzahl, $k, m \in \mathbb{Z}_{\geq 1}$ und $p \nmid m$. Dann sind p^{k-l+1} für $1 \leq l \leq k$ keine Teiler des Binomialkoeffizienten $\binom{p^k \cdot m}{p^l}$.*

Beweis. Die Idee ist $p^{k-l}m$ auszuklammern und dann zu zeigen, dass der verbleibende Term nicht von p geteilt wird.

Allgemein gilt

$$\binom{p^k \cdot m}{p^l} = \frac{p^k m}{p^l} \cdot \left(\prod_{i=1}^{p^l-1} \frac{p^k m - i}{p^l - i} \right) = p^{k-l} m \cdot \binom{p^k \cdot m - 1}{p^l - 1}$$

Es ist also zu zeigen, dass

$$p \nmid \left(\prod_{i=1}^{p^l-1} \frac{p^k m - i}{p^l - i} \right)$$

Dies gilt, da in $i < p^l - 1$ der Primfaktor p höchstens mit Exponent kleiner als $l \leq k$ vorkommt und somit vollständig gekürzt werden kann: Dazu schreiben wir jedes $i \in \{1, ..., p^l - 1\}$ als

$$i = p^{n_i} \cdot t_i$$

mit $n_i \in \mathbb{Z}_{\geq 0}$ und $t_i \in \mathbb{Z}_{\geq 1}$ und $p \nmid t_i$. Dann gilt $n_i < l \leq k$ wegen $i < p^l$. Kürzen liefert

$$\frac{p^k m - i}{p^l - i} = \frac{p^{k-n_i} m - t_i}{p^{l-n_i} - t_i}$$

Weder Zähler noch Nenner in diesem Bruch sind durch p teilbar. Somit ist

$$\binom{p^k \cdot m - 1}{p^l - 1} = \prod_{i=1}^{p^l-1} \frac{p^k m - i}{p^l - i} = \prod_{i=1}^{p^l-1} \frac{p^{k-n_i} m - t_i}{p^{l-n_i} - t_i}$$

ein Produkt von rationalen Zahlen, in denen in gekürzter Darstellung nirgends ein p auftaucht, also $p \nmid \binom{p^k \cdot m-1}{p^l-1}$. ■

Beweis. Wir zeigen nun Satz 2.4.4:

Sei $|G| = p^k m$ mit $p \nmid m$ und $1 \leq l \leq k$ und

$$X = \left\{ A \subset G \mid |A| = p^l \right\}$$

Wir zeigen, dass ein Element von X eine Untergruppe von G ist: G operiert auf X durch

$$\begin{aligned} G \times X &\longrightarrow X \\ (g, A) &\longmapsto gA \end{aligned}$$

Da p^{k-l+1} kein Teiler von

$$|X| = \binom{p^k m}{p^l}$$

ist, gibt es ein $A \in X$ mit

$$p^{k-l+1} \nmid |GA|$$

denn nach der Bahnenformel ist $|X| = \sum_{A \in R} |GA|$ mit einem vollständigen Repräsentantensystem der Bahnen R. Würden also alle $|GA|$ von p^{k-l+1} geteilt, dann auch $|X|$.

Wir halten nun dieses A fest und zeigen, dass $\mathrm{Stab}(A)$ eine Untergruppe der Ordnung p^l ist:

Schreibe

$$\begin{aligned} |\mathrm{Stab}(A)| &= p^r v \\ [G : \mathrm{Stab}(A)] &= p^s w \end{aligned}$$

mit $r, s \in \mathbb{Z}_{\geq 0}$ und $v, w \in \mathbb{Z}_{\geq 1}$ mit $p \nmid v$ und $p \nmid w$. Da $|GA| = [G : \mathrm{Stab}(A)]$ ist

$$s \leq k - l$$

Außerdem ergibt sich mit der Indexformel

$$p^{r+s}vw = [G : \mathrm{Stab}(A)] \cdot |\mathrm{Stab}(A)| = |G| = p^k \cdot m$$

also mit der Eindeutigkeit der Primfaktorzerlegung $r + s = k$.

Somit gilt

$$r = k - s \geq l$$

d.h. $p^l \mid |\mathrm{Stab}(A)|$.

Sei nun $a \in A$. Für jedes $g \in \mathrm{Stab}(A)$ ist $ga \in gA = A$. Somit ist die durch die Verknüpfung in G induzierte Abbildung

$$\begin{aligned} \mathrm{Stab}(A) &\to A \\ g &\mapsto g \cdot a \end{aligned}$$

wohldefiniert und offenbar injektiv, also $p^l \leq |\mathrm{Stab}(A)| \leq |A| = p^l$, d.h. der Stabilisator von A

$$\mathrm{Stab}(A) \subset G$$

ist eine Untergruppe der Ordnung p^l. ■

2.4.2 Sylowuntergruppen

Wir betrachten nun die p-Gruppen maximaler Ordnung.

Definition 2.4.8 *Sei p prim und $|G| = p^k \cdot m$ mit $p \nmid m$. Eine Untergruppe $H \subset G$ heißt p-**Sylowuntergruppe**, wenn $|H| = p^k$.*

Satz 2.4.4 zeigt insbesondere die Existenz einer p-Sylowuntergruppe.

Satz 2.4.9 (Sylowsätze) *Sei G eine endliche Gruppe und p prim.*

1) *Jede p-Gruppe $U \subset G$ liegt in einer p-Sylowuntergruppe $H \subset G$.*

2) *Jede konjugierte Untergruppe einer p-Sylowuntergruppe ist eine p-Sylowuntergruppe, und je zwei p-Sylowuntergruppen sind konjugiert, d.h. die Menge der p-Sylowuntergruppen von G ist eine Konjugationsklasse von Untergruppen von G.*

3) *Sei*

$$s_p = |\{U \mid U \text{ eine p-Sylowuntergruppe von } G\}|$$

die Anzahl der p-Sylowuntergruppen von G. Dann gilt

(a) $s_p \mid |G|$

(b) $s_p \equiv 1 \bmod p$

Corollar 2.4.10 *Schreiben wir $|G| = p^k \cdot m$ mit $p \nmid m$, dann gilt*

$$s_p \mid m$$

Beweis. $s_p \mid p^k m$ und $s_p \equiv 1 \bmod p$, also $p \nmid s_p$. ■

Corollar 2.4.11 *Sei $|G| = p^k \cdot m$ mit $p \nmid m$. H ist eine p-Sylowuntergruppe von G genau dann, wenn H eine maximal große p-Gruppe mit $H \subset G$ ist.*

Beweis. Sei $H \subset G$ eine maximal große p-Gruppe. Dann liegt H nach dem 1. Sylowsatz in einer p-Sylowuntergruppe H'. Wäre $H \subsetneq H'$ dann wäre H' eine größere p-Gruppe, ein Widerspruch zur Maximalität von H.

Ist $|H| = p^k$, dann ist H eine p-Gruppe und angenommen H' ist eine p-Gruppe mit $H \subset H'$, dann $p^k \mid |H'| = p^l$, also $l \geq k$. Da k maximal war mit $p^k \mid |G|$, ist $k = l$. ■

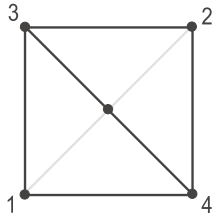
Beispiel 2.4.12 *Es ist*

$$|S_4| = 4! = 24 = 3 \cdot 2^3$$

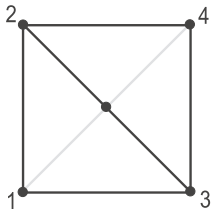
die 2-Sylowuntergruppen von S_4 haben also Ordnung $2^3 = 8$. Nach den Sylowsätzen gilt

$$s_2 \equiv 1 \bmod 2$$
$$s_2 \mid 3$$

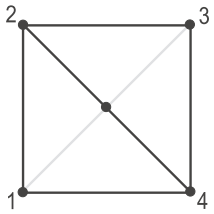
also $s_2 \in \{1,3\}$. *Betrachte die Stabilisatoren von Geraden durch gegenüberliegende Kantenmitten im Tetraeder wie in Abbildung 2.9. Diese Gruppen haben Ordnung* 8, *und es gibt* $3 = \frac{6}{2}$ *solche Kantenmittendiagonalen im Tetraeder, also ist* $s_2 = 3$. *Explizit sind die* 2*-Sylowuntergruppen*



$$\{(), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3),\\ (1,2), (3,4),\\ (1,3,2,4), (1,4,2,3)\}$$



$$\{(), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3),\\ (2,3), (1,4),\\ (1,2,4,3), (1,3,4,2)\}$$



$$\{(), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3),\\ (1,3), (2,4),\\ (1,2,3,4), (1,4,3,2)\}$$

Für die 3*-Sylowuntergruppen gilt*

$$s_3 \equiv 1 \bmod 3$$
$$s_3 \mid 8$$

also $s_3 \in \{1,4\}$. *Der Tetraeder hat* 4 *dreizählige Drehachsen, die jeweils einer zyklischen Untergruppe der Ordnung* 3 *entsprechen (explizit* $\langle(1,2,3)\rangle$, $\langle(1,2,4)\rangle$, $\langle(1,3,4)\rangle$ *und* $\langle(2,3,4)\rangle$*). Somit ist* $s_3 = 4$.

Zum Beweis der Sylowsätze benötigen wir:

Lemma 2.4.13 *Sei* $H \subset G$ *eine* p*-Gruppe,* S *eine* p*-Sylowuntergruppe von* G. *Ist* H *im* ***Normalisator***

$$N_G(S) = \left\{g \in G \mid gSg^{-1} = S\right\}$$

von S *enthalten, dann ist* $H \subset S$.

Beweis. Schreibe $|G| = p^k \cdot m$ und $p \nmid m$. Da $S \subset N(S)$ nach Konstruktion von $N_G(S)$ ein Normalteiler und $H \subset N_G(S)$ eine Untergruppe ist, liefert der 1. Isomorphiesatz

$$HS/S \cong H/(H \cap S)$$

Damit ist $|HS/S|$ ein Teiler von $|H|$ und damit eine p-Potenz, also ist auch

$$|HS| = |HS/S| \cdot |S| \geq |S| = p^k$$

eine p-Potenz. Somit muss $|HS| = p^k$ sein und daher $HS = S$, was $H \subset S$ impliziert. ■

Zum Normalisator siehe auch Übung 2.34.

Lemma 2.4.14 *Ist $U \subset G$ eine p-Sylowuntergruppe und $H \subset G$ eine p-Gruppe, dann gilt*

$$\exists b \in G : H \subset bUb^{-1}$$

und bUb^{-1} ist wieder eine p-Sylowuntergruppe.

Beweis. Die Konjugationsoperation

$$\begin{aligned} G \times U^G &\longrightarrow U^G = \left\{ gUg^{-1} \mid g \in G \right\} \\ (g, S) &\longmapsto gSg^{-1} \end{aligned}$$

auf der Konjugationsklasse U^G der Untergruppe U hat per Definition nur eine einzige Bahn (eine solche Operation heißt **transitiv**). Somit ist

$$|G| = \left|U^G\right| \cdot |N_G(U)|$$

wobei wir bemerken, dass $\mathrm{Stab}_G(U) = N_G(U)$. Schreibe $|G| = p^k \cdot m$ mit $p \nmid m$, d.h. $|U| = p^k$. Da $U \subset N_G(U)$ eine Untergruppe ist, gilt

$$p^k \mid |N_G(U)|$$

und somit

$$p \nmid \left|U^G\right|$$

Operieren wir statt dessen nur mit der Untergruppe $H \subset G$

$$\begin{aligned} H \times U^G &\longrightarrow U^G \\ (a, S) &\longmapsto aSa^{-1} \end{aligned}$$

dann zerfällt U^G in eine disjunkte Vereinigung von Bahnen. Sei $V \subset U^G$ ein vollständiges Repräsentantensystem. Dann gilt

$$\left|U^G\right| = \sum_{S \in V} \frac{|H|}{|\mathrm{Stab}_H(S)|} = \sum_{S \in V} p^{j_S}$$

mit $j_S \geq 0$, da H eine p-Gruppe war.

Da $p \nmid |U^G|$, muss es ein $S \in V$ geben mit $j_S = 0$, d.h.

$$H = \mathrm{Stab}_H(S)$$

und somit $H \subset N_G(S)$.

Weiter können wir $S \in U^G$ darstellen als $S = bUb^{-1}$ mit $b \in G$.

Mit Lemma 2.4.13 folgt also

$$H \subset S = bUb^{-1}$$

und diese Gruppe hat p^k Elemente, ist also eine p-Sylowuntergruppe.

■

Beweis. Wir zeigen den 1. Sylowsatz:

Nach Satz 2.4.4 gibt es eine p-Sylowuntergruppe $U \subset G$. Nach Lemma 2.4.14 existiert ein $b \in G$ mit $bUb^{-1} \supset H$. ■

Beweis. Wir zeigen den 2. Sylowsatz:

Wir wenden den 1. Sylowsatz auf eine p-Sylowuntergruppe H an. Da zwei p-Sylowuntergruppen gleich viele Elemente haben, ist $H = bUb^{-1}$, also liegen alle p-Sylowuntergruppen in der selben Konjugationsklasse von Untergruppen. In Lemma 2.4.14 haben wir schon gesehen, dass jede Konjugierte einer p-Sylowuntergruppe wieder eine p-Sylowuntergruppe ist. ■

Beweis. Wir zeigen den 3. Sylowsatz:

Sei U eine p-Sylowuntergruppe, U^G die Menge der p-Sylowuntergruppen (nach dem 2. Sylowsatz) und

$$s_p = \left|U^G\right|$$

Wie oben gesehen, ist

$$s_p = [G : \mathrm{Stab}_G(U)] = \frac{|G|}{|\mathrm{Stab}_G(U)|}$$

ein Teiler von $|G|$.

Für den zweiten Teil betrachten wir die Operation

$$\begin{aligned} U \times U^G &\longrightarrow U^G \\ (a, S) &\longmapsto aSa^{-1} \end{aligned}$$

Sei $V \subset U^G$ ein vollständiges Repräsentantensystem der Bahnen. Die Bahn von U enthält offenbar nur U, also insbesondere $U \in V$. Keine andere Bahn besteht nur aus einem einzigen Element, denn wäre $S \in V$ mit

$$aSa^{-1} = S \ \forall a \in U$$

dann wäre $U \subset N_G(S)$, also mit Lemma 2.4.13 schon $U \subset S$ und somit $U = S$, da beide Gruppen die selbe Ordnung haben.

Mit der Bahnenformel gilt also

$$s_p = \left|U^G\right| = \sum_{S \in V} \frac{|U|}{\mathrm{Stab}_U(S)} = 1 + \sum_{S \in V,\ S \neq U} p^{j_S} \equiv 1 \bmod p$$

(denn U ist eine p-Gruppe) und $j_S \geq 1$. ■

In Übung 2.36 überprüfen wir für die S_4 die Sylowsätze. Weitere Übungsaufgaben zu den Sylowsätzen sind 2.37, 2.40, 2.38, 2.43, 2.44, 2.45 und 2.39.

2.4.3 Anwendung der Sylowsätze

Der folgende Satz ist eine typische Anwendung der Sylowsätze auf Klassifikationsprobleme in der Gruppentheorie. Als Corollar erhalten wir zum Beispiel, dass jede Gruppe der Ordnung 15 schon zyklisch ist.

Satz 2.4.15 *Seien p und q Primzahlen, $p < q$ und p kein Teiler von $q-1$. Dann ist jede Gruppe G der Ordnung $p \cdot q$ zyklisch, d.h.*

$$G \cong \mathbb{Z}/pq$$

Beweis. Nach dem 3. Sylowsatz ist $s_p = 1 + kp$ und $s_p \mid q$. Wäre $s_p = q$, dann $p \mid (q-1)$, ein Widerspruch. Somit ist

$$s_p = 1$$

Sei also $S(p) \subset G$ die einzige p-Sylowuntergruppe. Es gilt $S(p) \cong \mathbb{Z}/p$.

Genauso ist $s_q = 1 + k'q$ und $s_q \mid p$. Wäre $s_q = p$, dann $p > q$, ein Widerspruch, also

$$s_q = 1$$

Sei $S(q) \subset G$ die einzige q-Sylowuntergruppe. Es gilt $S(q) \cong \mathbb{Z}/q$.

Wir zeigen

$$G \cong S(p) \times S(q)$$

Dann folgt mit dem Chinesischen Restsatz

$$G \cong \mathbb{Z}/p \times \mathbb{Z}/q \cong \mathbb{Z}/pq$$

Wegen $s_p = 1$ und $s_q = 1$ sind $S(p), S(q) \subset G$ Normalteiler. Da $S(p)$ und $S(q)$ teilerfremde Ordnung haben, ist

$$S(p) \cap S(q) = \{e\}$$

Mit dem 1. Isomorphiesatz ist

$$S(p) \cdot S(q) \subset G$$

eine Untergruppe und

$$(S(p) \cdot S(q)) / S(q) \cong S(p) / (S(p) \cap S(q)) = S(p)$$

also

$$|S(p) \cdot S(q)| = p \cdot q$$

und damit

$$S(p) \cdot S(q) = G$$

Somit ist die Abbildung

$$\begin{array}{rccc} \varphi: & S(p) \times S(q) & \to & G \\ & (a,b) & \mapsto & a \cdot b \end{array}$$

bijektiv.

Da $S(p), S(q) \subset G$ Normalteiler sind, gilt für alle $a \in S(p)$ und $b \in S(q)$

$$aba^{-1}b^{-1} \in S(p) \cap S(q) = \{e\}$$

also $ab = ba$.

Damit ist

$$\varphi((a,b)(c,d)) = \varphi(ac,bd) = acbd = abcd = \varphi(a,b)\varphi(c,d)$$

also φ ein Homomorphismus. ■

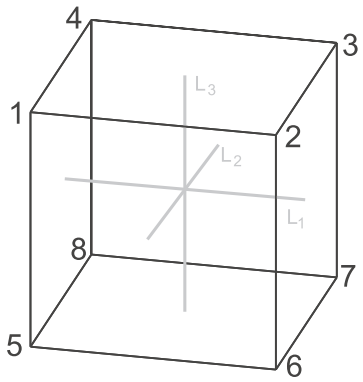


Abbildung 2.11: Würfel mit Seitenmittendiagonalen

Corollar 2.4.16 *Jede Gruppe der Ordnung* 15 *ist zyklisch.*

Siehe auch Übungsaufgabe 2.42.

Beispiel 2.4.17 *Wir wenden die Sylowsätze auf die Symmetriegruppe G des Würfels an. In Beispiel 2.2.21 hatten wir schon gesehen, dass $|G| = 48 = 2^4 \cdot 3$. Also gilt für die Anzahl der 2-Sylowuntergruppen (der Ordnung* 16*)*

$$s_2 \mid 3$$
$$s_2 \equiv 1 \bmod 2$$

also $s_2 \in \{1, 3\}$. Die Stabilisatoren $\mathrm{Stab}(L_i)$ der Seitenmittendiagonalen L_1, L_2, L_3 (siehe Abbildung 2.11) haben Ordnung 16*, denn sie sind isomorph zum direkten Produkt*

$$\mathrm{Stab}(L_i) \cong D_4 \times \mathbb{Z}/2$$

Wir können G durch Nummerieren der Ecken als Untergruppe der S_8 auffassen. Dann ist etwa

$$\mathrm{Stab}(L_1) = \langle (1,2,3,4)(5,6,7,8), (1,3)(5,7), (1,5)(2,6)(3,7)(4,8) \rangle$$

erzeugt von der Drehung um 90° *und einer Spiegelung an einer Diagonalebene (die zusammen eine D_4 erzeugen) und der Spiegelung an der Ebene senkrecht zu L_3. Da die Drehung um* 90°

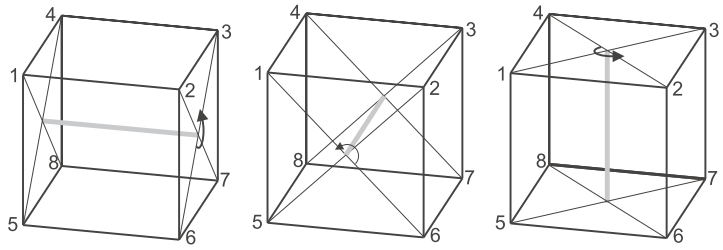


Abbildung 2.12: Drehungen des Würfels um Seitenmittendiagonalen um 180°

um L_1 *jedoch* L_2 *und* L_3 *vertauscht, sind die* $\mathrm{Stab}(L_i)$ *paarweise verschieden, also*

$$s_2 = 3$$

Der Durchschnitt $\bigcap_{k=1}^{3} \mathrm{Stab}(L_k)$ *enthält:*

- *die Identität*
- *die* 3 *Drehungen* r_1, r_2, r_3 *um* 180° *um die Seitenmittendiagonalen* L_1, L_2, L_3*, siehe Abbildung 2.12, beispielsweise*

$$r_2 = (1,6)\,(2,5)\,(4,7)\,(3,8)$$

- *die* 3 *Spiegelungen* $\delta_1, \delta_2, \delta_3$ *an Ebenen senkrecht zu den Seitenmittendiagonalen, siehe Abbildung 2.13, zum Beispiel*

$$\delta_3 = (1,5)\,(2,6)\,(3,7)\,(4,8)$$

- *und die Punktspiegelung* δ *in Abbildung 2.14, als Permutation gegeben durch*

$$\delta = (1,7)\,(2,8)\,(3,5)\,(4,6)\,.$$

Somit gilt

$$\begin{aligned}\bigcap_{k=1}^{3} \mathrm{Stab}(L_k) &= \mathrm{Stab}(L_i) \cap \mathrm{Stab}(L_j) \\ &= \{\mathrm{id}, r_1, r_2, r_3, \delta_1, \delta_2, \delta_3, \delta\}\end{aligned}$$

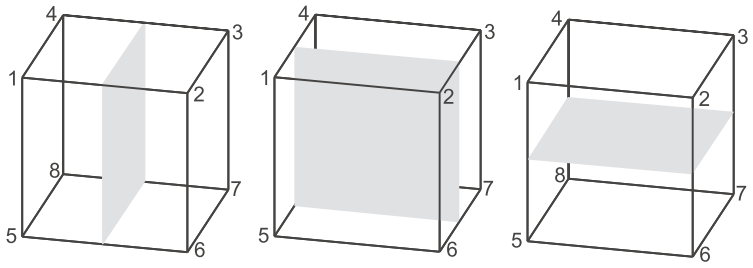


Abbildung 2.13: Spiegelungen des Würfels an den Koordinatenebenen

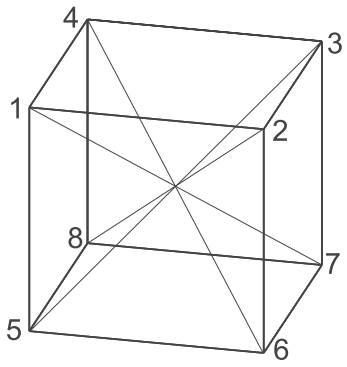


Abbildung 2.14: Punktspiegelung des Würfels

für alle $i \neq j$*, denn* $\mathrm{Stab}(L_i) \cap \mathrm{Stab}(L_j) \subsetneqq \mathrm{Stab}(L_i)$*. Die 2-Sylowuntergruppen enthalten also zusammen genau* $8 + 3 \cdot 8 = 32$ *Elemente (*12 *der Ordnung* 4 *und* 19 *der Ordnung* 2*).*

Für die Anzahl der 3*-Sylowuntergruppen (von Ordnung* 3*) haben wir*

$$s_3 \mid 16$$
$$s_3 \equiv 1 \bmod 3$$

also $s_3 \in \{1, 4, 16\}$*. Wäre* $s_3 = 16$*, dann gäbe es (neben den oben gefundenen* 32 *Elementen von 2-Potenzordnung) noch* $16 \cdot 2 = 32$ *Elemente der Ordnung* 3*, ein Widerspruch. Die Gruppen von Drehungen um die* 4 *Eckendiagonalen haben jeweils Ordnung* 3*, z.B.* $\langle (2,4,5)\,(6,3,8) \rangle$*, siehe Abbildung 2.15, also*

$$s_3 = 4$$

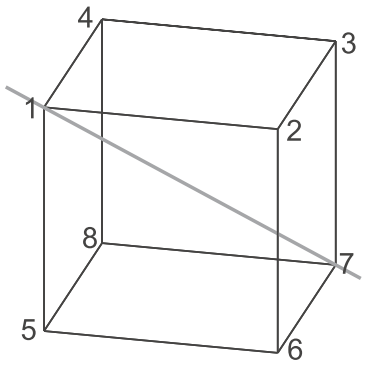


Abbildung 2.15: Eckendiagonale im Würfel

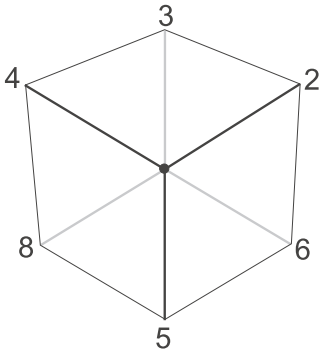


Abbildung 2.16: Drehspiegelung des Würfels

Die 3*-Sylowuntergruppen enthalten zusammen* $2 \cdot 4 = 8$ *Elemente der Ordnung* 3*.*

Die restlichen 8 *Elemente von* G *liegen in keiner Sylowuntergruppe. Es sind die Drehspiegelungen der Ordnung* 6 *um Kantenmittendiagonalen, beispielsweise*

$$(1,7)\,(2,3,4,8,5,6)$$

siehe Abbildung 2.16. Diese zeigt den Würfel in einer Zeichenebene senkrecht zur Drehachse.

2.5 Übungsaufgaben

Übung 2.1 *Sei G eine Menge zusammen mit einer Verknüpfung*

$$\begin{array}{rccc} \circ: & G \times G & \longrightarrow & G \\ & (a,b) & \mapsto & a \circ b \end{array}$$

die folgende Axiome erfüllt:

(G1) Assoziativität

$$a \circ (b \circ c) = (a \circ b) \circ c \ \forall a, b, c \in G$$

(G2') Es existiert ein linksneutrales Element, d.h. ein

$$e \in G$$

mit

$$e \circ a = a \ \forall a \in G$$

(G3') Existenz des Linksinversen, d.h. $\forall a \in G \ \exists a^{-1} \in G$ mit

$$a^{-1} \circ a = e$$

Zeigen Sie:

1) *Für $a, b \in G$ gilt: Ist $ab = e$, dann ist auch $ba = e$.*
2) *Es ist $a \circ e = a \ \forall a \in G$.*
3) *Das neutrale Element ist eindeutig.*
4) *Das Inverse ist eindeutig.*
5) *Für $a, b \in G$ ist $(ab)^{-1} = b^{-1}a^{-1}$.*
6) *Für $a \in G$ ist $(a^{-1})^{-1} = a$.*

Übung 2.2 *Sei $\varphi : G_1 \longrightarrow G_2$ ein Gruppenhomomorphismus und $e_i \in G_i$ jeweils das neutrale Element. Zeigen Sie:*

1) *$\varphi(e_1) = e_2$.*

2) *Für* $a \in G_1$ *gilt* $\varphi(a)^{-1} = \varphi(a^{-1})$.

3) *Kern* $\ker(\varphi) \subset G_1$ *und Bild* $\mathrm{Im}(\varphi) \subset G_2$ *von* φ *sind Untergruppen.*

4) *Ist* φ *ein Isomorphismus, dann ist auch die Umkehrabbildung*

$$\varphi^{-1} : G_2 \longrightarrow G_1$$

ein Gruppenisomorphismus.

Übung 2.3 *Zeigen Sie, dass*

$$\begin{array}{rccl} \mathrm{sign}: & S_n & \longrightarrow & (\{\pm 1\}, \cdot) \\ & \sigma & \longmapsto & \mathrm{sign}(\sigma) = \prod\limits_{\substack{i,j=1 \\ i<j}}^{n} \frac{\sigma(i)-\sigma(j)}{i-j} \end{array}$$

ein Gruppenepimorphismus ist.

Übung 2.4 *Schreiben Sie*

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 1 & 4 & 2 & 6 & 5 & 7 \end{pmatrix}, \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 3 & 1 & 4 & 5 & 7 & 6 \end{pmatrix},$$

$\sigma \circ \tau$ *und* $\tau \circ \sigma$ *sowohl als Produkt disjunkter Zykel als auch als Produkt von Transpositionen. Bestimmen Sie jeweils Ordnung und* sign.

Übung 2.5 *Lässt sich bei dem bekannten Schiebespiel folgende Konfiguration*

2	1	3	4
5	6	7	8
9	10	11	12
13	14	15	

in die Ausgangsstellung

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

überführen?

Übung 2.6 *1) Zeigen Sie: Sind* $a, b \in \mathbb{Z}$ *mit* $a, b \geq 1$ *und* $\mathrm{ggT}(a, b) = 1$. *Dann gilt*

$$\mathbb{Z}/(a \cdot b) \cong \mathbb{Z}/a \times \mathbb{Z}/b$$

2) Bestimmen Sie das Urbild von $(2 + 6\mathbb{Z}, -7 + 35\mathbb{Z})$ *unter dem Gruppenisomorphismus*

$$\mathbb{Z}/210 \cong \mathbb{Z}/6 \times \mathbb{Z}/35$$

Übung 2.7 *1) Sei* G *eine Gruppe und seien* $x, y \in G$ *mit* $x \cdot y = y \cdot x$ *und* $\langle x \rangle \cap \langle y \rangle = \{e\}$. *Zeigen Sie:*

$$\mathrm{ord}(x \cdot y) = \mathrm{kgV}(\mathrm{ord}(x), \mathrm{ord}(y))$$

2) Sei

$$\sigma = c_1 \cdot \ldots \cdot c_r \in S_n$$

Produkt disjunkter Zykel c_i *der Längen* m_i. *Bestimmen Sie* $\mathrm{ord}(\sigma)$.

3) Welche Ordnungen treten bei den Elementen von S_4 *bzw.* S_7 *auf?*

Übung 2.8 *Zeigen Sie:*

1) Ist

$$\sigma = \begin{pmatrix} 1 & \cdots & n-1 & n \\ \sigma(1) & & \sigma(n-1) & k \end{pmatrix} \in S_n$$

dann ist

$$(n-1, n) \cdot \ldots \cdot (k, k+1) \cdot \sigma \in S_{n-1}$$

2) Die symmetrische Gruppe S_n *wird erzeugt von den Transpositionen* $(1,2), (2,3), \ldots, (n-1, n)$, *d.h.*

$$S_n = \langle (1,2), (2,3), \ldots, (n-1, n) \rangle$$

Übung 2.9 *Sei* $G \subset S_n$ *eine Untergruppe mit* $(1,2) \in G$ *und* $(1, 2, \ldots, n) \in G$. *Zeigen Sie*

$$G = S_n$$

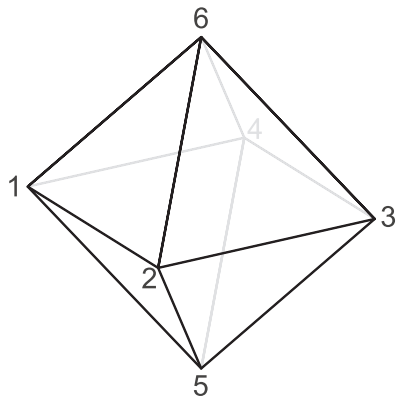


Abbildung 2.17: Symmetriegruppe des Oktaeders als Untergruppe von S_6

Übung 2.10 *Zeigen Sie: Jede endliche Gruppe ist isomorph zu einer Untergruppe einer S_n.*

Übung 2.11 *Sei $G = \mathrm{Sym}(O)$ die Symmetriegruppe des Oktaeders O.*

1) *Durch Nummerieren der Ecken von O wie in Abbildung 2.17 ist ein Monomorphismus $f_1 : G \to S_6$ gegeben. Finden Sie Erzeuger von $f_1(G)$ und zeigen Sie Ihre Behauptung mit Hilfe von GAP.*

2) *Durch Nummerieren der Seiten von O wie in Abbildung 2.18 ist ein Monomorphismus $f_2 : G \to S_8$ gegeben. Finden Sie Erzeuger von $f_2(G)$ und zeigen Sie Ihre Behauptung mit Hilfe von GAP.*

3) *Interpretieren Sie die in (1) und (2) gefundenen Erzeuger geometrisch.*

4) *Finden Sie mit GAP alle Ordnungen, die für Elemente von G auftreten und jeweils die Anzahl der Elemente dieser Ordnung.*

5) *Bestimmen Sie mit GAP einen Isomorphismus von $f_1(G) \to f_2(G)$.*

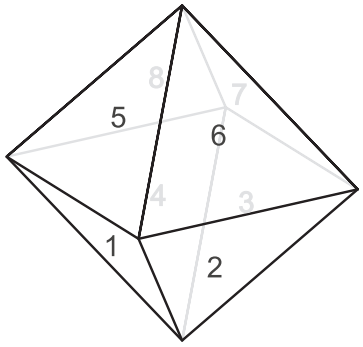


Abbildung 2.18: Symmetriegruppe des Oktaeders als Untergruppe der S_8

Übung 2.12 *Sei*

$$G = \mathrm{SL}(2,\mathbb{Z}) = \left\{ A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{Z}^{2\times 2} \mid \det A = 1 \right\}$$

und $\mathbb{F}_3$ *ein Körper mit* 3 *Elementen.*

1) Zeigen Sie, dass der natürliche Gruppenhomomorphismus

$$\mathrm{SL}(2,\mathbb{Z}) \to \mathrm{SL}(2,\mathbb{F}_3)$$

surjektiv ist.

2) Sei

$$H = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) \mid \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod 3 \right\}$$

Bestimmen Sie den Index $[G : H]$.

Übung 2.13 *Sei* $A = \{a_1, .., a_n\}$ *eine endliche Menge und* F *die freie Gruppe über dem Alphabet* A. *Zeigen Sie, dass* F *folgende universelle Eigenschaft hat: Zu jeder Gruppe* G *und* n *Elementen* $g_1, ..., g_n \in G$ *gibt es genau einen Gruppenhomomorphismus* $\varphi : F \to G$ *mit* $\varphi(a_i) = g_i$.

Bemerkung: Ist φ *surjektiv, so nennt man* $g_1, ..., g_n$ *Erzeuger von* G.

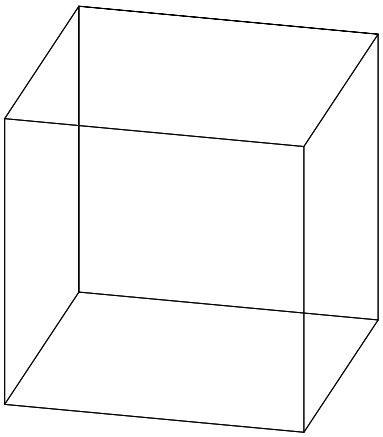
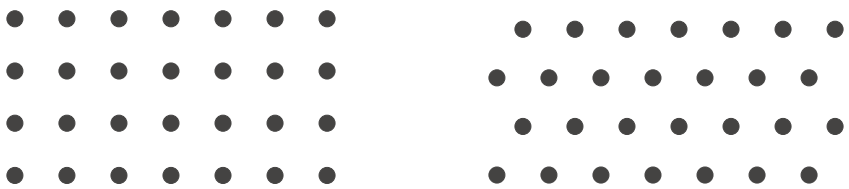


Abbildung 2.19: Würfel

Übung 2.14 *Bestimmen Sie jeweils die Symmetriegruppe* $\mathrm{Sym}(N) \subset \mathrm{E}(2)$ *für die Gitter*

1) $N = \mathbb{Z}^2 \subset \mathbb{R}^2$

2) $N = \left\{ a\,(1,0\ ) + b\left(\tfrac{1}{2}, \tfrac{1}{2}\sqrt{3}\ \right) \mid a, b \in \mathbb{Z} \right\} \subset \mathbb{R}^2$



Übung 2.15 *Bestimmen Sie die Symmetriegruppen von Würfel (Abb. 2.19), Oktaeder (Abb. 2.20), Dodekaeder (Abb. 2.21) und Ikosaeder (Abb. 2.22). Ermitteln Sie zunächst die Gruppenordnung. Beachten Sie, dass Sie den Oktaeder wie in Abbildung 2.23 in den Würfel einzeichnen können. Das gleiche gilt für Oktaeder und Ikosaeder.*

Übung 2.16 *1) Zeigen Sie: Die Menge der Konjugationsklassen von* S_n *steht in Bijektion mit der Menge der Partitionen von* n*.*

2) Bestimmen Sie alle Konjugationsklassen der S_4*.*

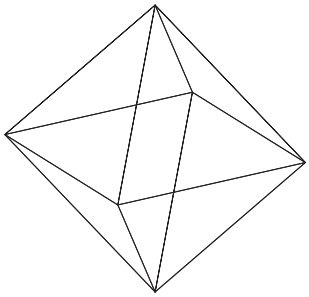


Abbildung 2.20: Oktaeder

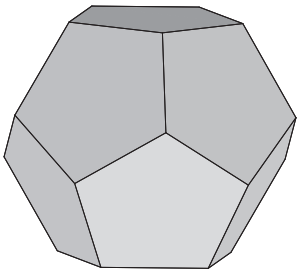


Abbildung 2.21: Dodekaeder

3) Interpretieren Sie die Konjugationsklassen der S_4 geometrisch, indem Sie die S_4 als Symmetriegruppe des Tetraeders (Abbildung 2.3) auffassen.

Übung 2.17 *Sei $G = \mathrm{Sym}(W)$ die Symmetriegruppe des Würfels W mit Ecken $(\pm 1, \pm 1, \pm 1)$. Welche Längen von Bahnen treten für die Operation $G \times W \to W$ auf, welche bei der induzierten Operation auf der Potenzmenge $G \times 2^W \to 2^W$?*

Übung 2.18 *Ein (ungerichteter) Graph ist ein Tupel (V, E) aus einer Menge V und einer Teilmenge $E \subset \binom{V}{2}$ der zweielementigen Teilmengen von V. Dann heißt V Knoten- oder Vertexmenge und E Kantenmenge (edges) des Graphen.*

Zwei Graphen $G_1 = (V_1, E_1)$ und $G_2 = (V_2, E_2)$ heißen isomorph, wenn es eine bijektive Abbildung $\varphi : V_1 \to V_2$ gibt, sodass

$$\{v, w\} \in E_1 \iff \{\varphi(v), \varphi(w)\} \in E_2$$

für alle $v, w \in V_1$.

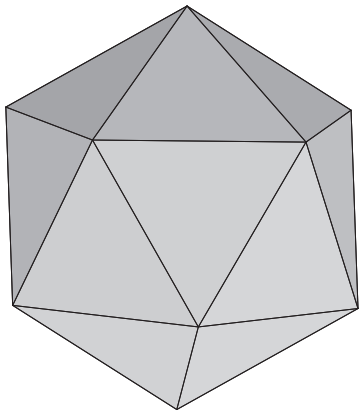
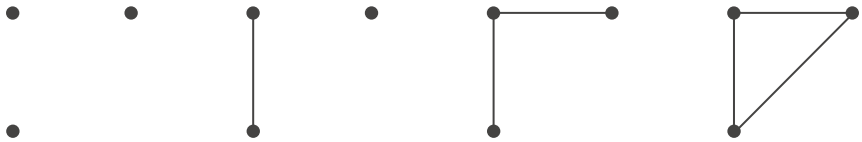


Abbildung 2.22: Ikosaeder

Beispielsweise gibt es genau 4 *Isomorphieklassen von Graphen mit* 3 *Knoten*



Zeigen Sie, dass es genau 34 *Isomorphieklassen von Graphen mit* 5 *Knoten gibt.*

Hinweis: Betrachten Sie die Operation der S_5 *auf der Menge aller Graphen mit Knoten* $\{1,2,3,4,5\}$.

Übung 2.19 *Zeigen Sie: Die Symmetriegruppe* G *des Würfels wird von der Drehung*

$$\alpha = (2,3,5,4)$$

um $90°$ *und der Drehspiegelung*

$$\beta = (1,5,3,6,2,4)$$

um $60°$ *erzeugt, und diese erfüllen die Relationen*

$$\alpha^4 = e \qquad \beta^6 = e \qquad (\alpha\beta)^2 = e \qquad (\alpha^{-1}\beta^2)^2 = e$$

Dabei nummerieren wir wie in Abbildung 2.24 mit $1,\ldots,6$ *die Seiten des Würfels.*

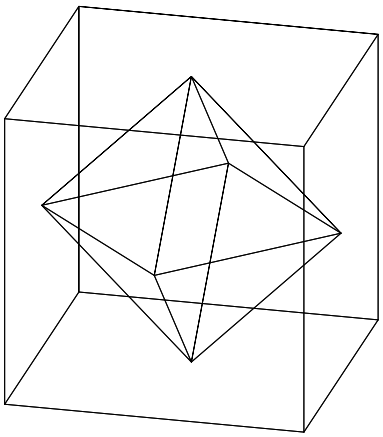


Abbildung 2.23: Dualität von Würfel und Oktaeder

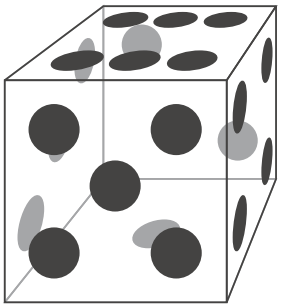


Abbildung 2.24: Symmetriegruppe des Würfels als Untergruppe der S_6

Übung 2.20 *Bestimmen Sie die Symmetriegruppe $G \subset \mathrm{O}(3)$ des Ikosaeders (Abbildung 2.22), indem Sie Erzeuger von G, d.h. geeignete orthogonale Matrizen, angeben.*

Übung 2.21 *Sei*

$$G := \left\langle s_1, \ldots, s_{n-1} \mid s_i^2 = e,\ s_i s_j = s_j s_i \text{ falls } |i-j| \geq 2,\ s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1} \forall i, j \right\rangle$$

Zeigen Sie

$$G \cong S_n$$

Geben Sie solche $s_i \in S_n$ an.

Übung 2.22 *Sei $\varphi : G \longrightarrow F$ ein Gruppenhomomorphismus. Zeigen Sie:*

1) *Ist $M \subset F$ ein Normalteiler, dann ist $\varphi^{-1}(M) \subset G$ ein Normalteiler.*

2) *Ist φ surjektiv und $N \subset G$ ein Normalteiler, dann ist $\varphi(N) \subset F$ ein Normalteiler.*

Übung 2.23 *Sei F die freie Gruppe erzeugt von x und y. Zeigen Sie:*

1) *Die von $G = \langle x^2, xyx^{-1}, y\rangle$ erzeugte Untergruppe ist ein Normalteiler vom Index 2.*

2) *Die Gruppe G ist isomorph zu einer freien Gruppe erzeugt von 3 Elementen.*

Übung 2.24 *Bestimmen Sie für die S_4 welche Untergruppen in welchen Untergruppen Normalteiler sind.*

Übung 2.25 *Finden Sie mit Hilfe von GAP alle Konjugationsklassen von Untergruppen der S_4. Bestimmen Sie auch jeweils die Mächtigkeit der Konjugationsklassen und die Gruppenordnung der Elemente. Welche Untergruppen der S_4 sind Normalteiler?*

Interpretieren Sie die Konjugationsklassen von Untergruppen geometrisch, indem Sie die S_4 als Symmetriegruppe des Tetraeders T auffassen und Untergruppen als Stabilisatoren $\mathrm{Stab}(A)$ von Teilmengen von $A \subset T$ beschreiben.

Hinweis: Verwenden Sie die GAP-Befehle `SymmetricGroup`, `LatticeSubgroups`, `ConjugacyClassesSubgroups`, `Size` *und* `Representative`.

Übung 2.26 *Bestimmen Sie mit Hilfe von GAP sämtliche Normalteiler von S_4 und von der Symmetriegruppe $G = \mathrm{Sym}(W)$ des Würfels W.*

Übung 2.27 *Sei $S_4 \cong \mathrm{Sym}(T) \subset \mathrm{Sym}(\mathbb{R}^3)$ die Symmetriegruppe des Tetraeders T mit den Ecken*

$$e_1 = (1,-1,-1) \quad e_2 = (-1,1,-1) \quad e_3 = (-1,-1,1) \quad e_4 = (1,1,1)$$

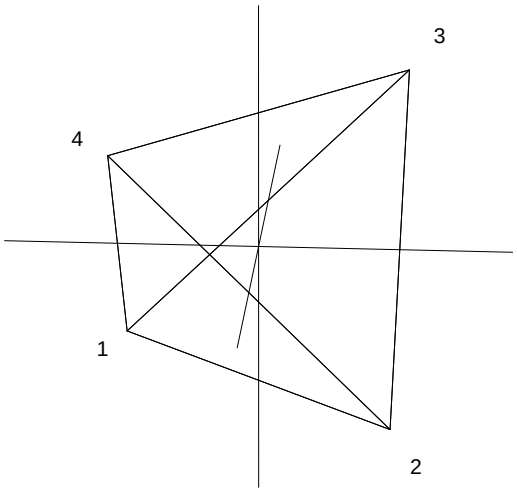


Abbildung 2.25: Tetraeder mit Kantenmittendiagonalen

Jede Symmetrie des Tetraeders T permutiert die Koordinatenachsen von $\mathbb{R}^3$, siehe Abbildung 2.25. Dies induziert einen Gruppenhomomorphismus

$$\varphi : S_4 \to S_3$$

Bestimmen Sie

1) *das Bild von $(1,2)$ und von $(1,2,3,4)$ unter φ.*

2) *den Kern von φ.*

Übung 2.28 *Sei G eine Gruppe und $\mathrm{Aut}(G)$ die Gruppe der Automorphismen von G und $\mathrm{Inn}(G)$ die Gruppe der inneren Automorphismen, d.h. Automorphismen $\varphi_a : G \to G$ der Gestalt $g \mapsto aga^{-1}$ mit $a \in G$. Zeigen Sie:*

1) *$\mathrm{Aut}(G)$ ist vermöge Komposition eine Gruppe und $\mathrm{Inn}(G)$ ist ein Normalteiler.*

2) *Bestimmen Sie für $G = \mathbb{Z}_2 \times \mathbb{Z}_2$, $G = S_3$ und $G = \mathbb{Z}/4\mathbb{Z}$ jeweils die Gruppen der inneren und äußeren Automorphismen $\mathrm{Inn}(G)$ und $\mathrm{Aut}(G)$ und die Quotientengruppe $\mathrm{Aut}(G)/\mathrm{Inn}(G)$.*

Übung 2.29 *Bestimmen Sie für die Symmetriegruppe des Quadrats $G = D_4$ die innere Automorphismengruppe* $\mathrm{Inn}(G)$ *und die äußere Automorphismengruppe* $\mathrm{Out}(G) = \mathrm{Aut}(G) / \mathrm{Inn}(G)$.

Übung 2.30 *Zeigen Sie:*

1) *Die Gruppe S_6 wird von den Elementen $(1,2,3,4,5)$ und $(5,6)$ erzeugt.*

2) *Die Zuordnung*

$$\begin{array}{lcl} (1,2,3,4,5) & \mapsto & (1,2,3,4,5) \\ (5,6) & \mapsto & (1,2)(3,5)(4,6) \end{array}$$

lässt sich zu einem Automorphismus φ von S_6 fortsetzen. φ ist kein innerer Automorphismus und somit $\mathrm{Inn}(S_6) \subsetneqq \mathrm{Aut}(S_6)$.

Übung 2.31 *Zeigen Sie, dass die Kleinsche Vierergruppe*

$$V_4 = \{(), (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}$$

ein Normalteiler in S_4 ist und für die Quotientengruppe gilt

$$S_4/V_4 \cong S_3$$

Geben Sie eine geometrische Interpretation, indem Sie die S_4 als Symmetriegruppe des Tetraeders auffassen.

Übung 2.32 1) *Sei H eine Untergruppe von G. Zeigen Sie: Ist $[G : H] = 2$, dann ist H ein Normalteiler in G.*

2) *Zeigen Sie: Die alternierende Gruppe*

$$A_4 = \{\sigma \in S_4 \mid \mathrm{sign}\,\sigma = 1\} \subset S_4$$

ist ein Normalteiler in S_4 und $V_4 \subset A_4$. Beschreiben Sie den Normalteiler $A_4/V_4 \subset S_4/V_4$ und den Isomorphismus

$$(S_4/V_4) / (A_4/V_4) \cong S_4/A_4$$

Übung 2.33 *Seien G und H Gruppen und $\varphi : H \to \mathrm{Aut}(G)$ ein Homomorphismus. Mit der Verknüpfung*

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 \cdot \varphi(h_1)(g_2), h_1 \cdot h_2)$$

wird $G \times H$ zu einer Gruppe P, dem semidirekten Produkt von G und H bzgl. φ.

1) *Zeigen Sie, dass $\tilde{H} = \{e_G\} \times H \subset P$ eine Untergruppe und $\tilde{G} = G \times \{e_H\}$ ein Normalteiler von P ist, dass $\tilde{G} \cong G$ und $P/\tilde{G} \cong H$.*

2) *Welche Gruppen erhält man für $H = \mathbb{Z}_2$, $G = \mathbb{Z}_3$ und φ definiert durch $\varphi(\bar{1}) = (\mathbb{Z}_3 \to \mathbb{Z}_3, \quad \bar{a} \mapsto -\bar{a})$ bzw. $\varphi(\bar{1}) = \mathrm{id}_{\mathbb{Z}_3}$.*

Übung 2.34 *Sei H eine Untergruppe von G. Der Normalisator von H ist*

$$N_G(H) = \left\{ g \in G \mid gHg^{-1} = H \right\}$$

Zeigen Sie:

1) *$H \subset N_G(H)$ ist ein Normalteiler und $N_G(H)$ ist die bezüglich Inklusion größte Untergruppe von G, in der H ein Normalteiler ist.*

2) *Bestimmen Sie den Normalisator $N_G(H)$ von $H = \langle (1,2,3) \rangle \subset S_4$.*

3) *Geben Sie ein Beispiel einer Gruppe G und einer Untergruppe $H \subset G$, sodass*

$$N_G(H) \subsetneq \left\{ g \in G \mid gHg^{-1} \subset H \right\}$$

Zeigen Sie, dass $\{g \in G \mid gHg^{-1} \subset H\}$ dann keine Untergruppe von G ist.

Übung 2.35 *Sei*

$$\mathrm{P}(n) = \left\{ (r_1, \ldots, r_t) \mid t \in \mathbb{Z}_{\geq 1},\ r_1, \ldots, r_t \in \mathbb{Z}_{\geq 0},\ r_t > 0 \text{ und } \sum_{k=1}^{t} r_k \cdot k = n \right\}$$

die Menge aller Partitionen von $n \in \mathbb{Z}_{\geq 1}$. Zeigen Sie:

$$1 = \sum_{(r_1, \ldots, r_t) \in \mathrm{P}(n)} \frac{1}{\prod_{k=1}^{t} k^{r_k} r_k!}$$

Hinweis: Verwenden Sie die Klassengleichung der S_n.

Übung 2.36 *Überprüfen Sie für die S_n, $n = 3, ..., 7$ in GAP, dass es von den Sylowuntergruppen jeweils nur eine Konjugationsklasse gibt, d.h. den 2. Sylowsatz, und auch den 3. Sylowsatz.*

Übung 2.37 *Bestimmen Sie die Anzahl und Isomorphietyp der 5-Sylowuntergruppen von S_5.*

Übung 2.38 *Sei G die Symmetriegruppe des Ikosaeders (Abbildung 2.22).*

1) *Basteln Sie einen Ikosaeder.*

2) *Bestimmen Sie die Gruppenordnung von G.*

3) *Bestimmen Sie für jeden Primteiler p von $|G|$ die Anzahl der p-Sylowuntergruppen von G, und interpretieren Sie die Sylowuntergruppen geometrisch.*

Übung 2.39 *Eine Gruppe G heißt einfach, wenn sie keine nichttrivialen Normalteiler hat (d.h. wenn $\{e\}$ und G selbst die einzigen Normalteiler sind). Zeigen Sie, dass es keine einfache Gruppe der Ordnung 84 gibt.*

Übung 2.40 1) *Sei G eine endliche Gruppe und n_a die Anzahl der Elemente der Ordnung a. Zeigen Sie, dass die Summe*

$$|G| = \sum_{a \text{ teilt } |G|} n_a$$

durch Zusammenfassen von Termen der Klassengleichung von G entsteht.

2) *Welche Klassengleichungen können für eine Gruppe G der Ordnung 10 auftreten? Bestimmen Sie auch jeweils die n_a.*

Übung 2.41 *Betrachten Sie die Gruppe R der Drehsymmetrien des Ikosaeders.*

1) *Bestimmen Sie die Ordnung von R.*

2) *Beschreiben Sie die Elemente von R geometrisch.*

3) *Bestimmen Sie die Klassengleichung von R.*

4) Zeigen Sie, dass R einfach ist.

Übung 2.42 *1) Geben Sie Primzahlen $p < q$ an, für die es eine nichtzyklische Gruppe der Ordnung pq gibt.*

2) Seien p, q Primzahlen und G eine Gruppe der Ordnung $|G| = p \cdot q$. Zeigen Sie, dass G nicht einfach ist, d.h. einen nicht-trivialen Normalteiler besitzt.

Übung 2.43 *Sei p eine Primzahl und $\mathbb{F}_p$ der Körper mit p Elementen. Bestimmen Sie die Ordnung von $\mathrm{SL}(2, \mathbb{F}_p)$, eine der p-Sylow-Untergruppen und die Anzahl s_p der p-Sylow-Untergruppen.*

Übung 2.44 *Bestimmen Sie die Sylowuntergruppen der Würfelgruppe.*

Übung 2.45 *Sei G eine einfache Gruppe der Ordnung 60.*

1) Bestimmen Sie die Anzahl der 3- und 5-Sylowuntergruppen von G.

2) Zeigen Sie, dass A_5 eine Untergruppe der Ordnung 12 hat.

3) Zeigen Sie: Hat G eine Untergruppe der Ordnung 12, dann ist G isomorph zu A_5.

4) Zeigen Sie: G is isomorph zu A_5.

Übung 2.46 *Sei G die Symmetriegruppe des regelmäßigen 5-Ecks (Abbildung 2.26). Bestimmen Sie*

1) Erzeuger von G, und beweisen Sie mit Hilfe von GAP Ihre Behauptung.

2) Die Elemente von G.

3) Alle Untergruppen von G und welche davon Normalteiler sind.

4) Die Sylowuntergruppen von G.

5) Die Konjugationsklassen von G, deren geometrische Interpretation und die Klassengleichung von G.

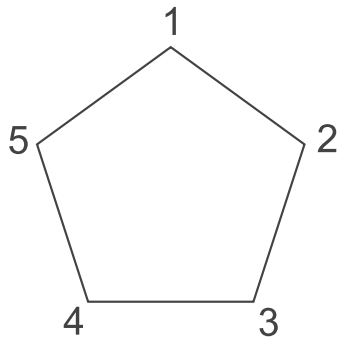


Abbildung 2.26: Regelmäßiges 5-Eck

Hinweis: Verwenden Sie die GAP-Funktionen

- `Group`
- `Order`
- `LatticeSubgroups`
- `ConjugacyClassesSubgroups`
- `Size`
- `Representative`
- `ConjugacyClasses`.

Übung 2.47 *1) Sei D_4 die Symmetriegruppe des Quadrats, wie in Abbildung 2.27. Bestimmen Sie mit Hilfe von GAP die Automorphismengruppe $\mathrm{Aut}(G)$ und die Gruppe der inneren Automorphismen $\mathrm{Inn}(G)$, das Zentrum $Z(G)$, und zeigen Sie $\mathrm{Aut}(G) \cong D_4$.*

2) Zeigen Sie: Die Gruppe S_6 wird von den Elementen $(1,2,3,4,5)$ und $(5,6)$ erzeugt und die Zuordnung

$$\begin{array}{lcl} (1,2,3,4,5) & \mapsto & (1,2,3,4,5) \\ (5,6) & \mapsto & (1,2)(3,5)(4,6) \end{array}$$

lässt sich zu einem Automorphismus φ von S_6 fortsetzen. φ ist kein innerer Automorphismus und somit $\mathrm{Inn}(S_6) \subsetneq \mathrm{Aut}(S_6)$.

Hinweis: Verwenden Sie die GAP-Befehle

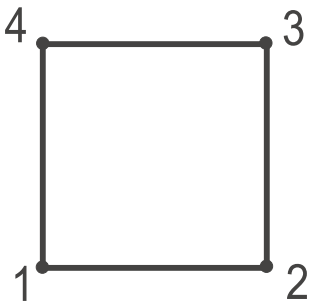


Abbildung 2.27: Quadrat mit Nummerierung

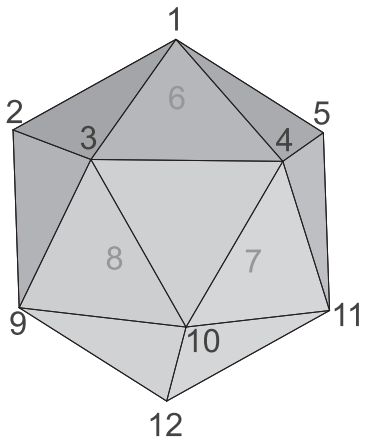


Abbildung 2.28: Ikosaeder mit Nummerierung der Ecken

- `AutomorphismGroup`
- `InnerAutomorphismsAutomorphismGroup`
- `IsomorphismGroups`
- `GroupHomomorphismByImages`
- `Kernel`.

Übung 2.48 *Finden Sie Erzeuger der Symmetriegruppe G des Ikosaeders als Untergruppe der S_{12}, und bestimmen Sie die Klassengleichung von G. Finden Sie alle Sylowuntergruppen von G.*

Übung 2.49 *Sei*

$$A = \{g_1, ..., g_n\}$$

eine endliche Menge und F die freie Gruppe erzeugt von A (mit neutralem Element e). Seien $r_1, ..., r_s$ Elemente von F und N der kleinste Normalteiler von F, der $r_1, ..., r_s$ enthält. Dann heißt

$$\langle g_1, ..., g_n \mid r_1 = e, ..., r_s = e \rangle := F/N$$

die Gruppe mit Erzeugern g_i und Relationen r_i. Zeigen Sie mit Hilfe von GAP, dass für die Symmetriegruppe des Würfels gilt

$$W \cong \left\langle \alpha, \beta \mid \alpha^4 = e,\ \beta^6 = e,\ (\alpha\beta)^2 = e,\ \left(\alpha^{-1}\beta^2\right)^2 = e \right\rangle$$

Hinweis: Verwenden Sie den GAP-Befehl `FreeGroup`.

Übung 2.50 *Bestimmen Sie mit Hilfe von GAP das semidirekte Produkt $G \rtimes_\varphi H$ von $G = \langle (1,2,3,4) \rangle$ und $H = \langle (1,2) \rangle$ bezüglich dem Gruppenhomomorphismus*

$$\begin{array}{rccl} \varphi: & H & \to & \mathrm{Aut}(G) \\ & h & \mapsto & \kappa_h = (g \mapsto hgh^{-1}) \end{array}$$

Welche Gruppe erhalten Sie?

Überprüfen Sie für $G = A_4$ und H und φ wie oben, dass

$$G \rtimes_\varphi H \cong S_4$$

Hinweis: Verwenden Sie den GAP-Befehl `SemidirectProduct`.

Übung 2.51 *Zeigen Sie, dass für $G = A_n$, $n \geq 4$ das Zentrum*

$$Z(G) = \{a \in G \mid ab = ba \ \forall b \in G\}$$

trivial ist.

3

Ringe

3.1 Übersicht

Im ersten Kapitel hatten wir uns mit dem Ring der ganzen Zahlen $\mathbb{Z}$ und dessen grundlegenden Eigenschaften beschäftigt, insbesondere mit der Existenz einer eindeutigen Primfaktorisierung, dem Euklidischen Algorithmus zur Bestimmung des größten gemeinsamen Teilers und dem Chinesischen Restsatz. Hier wollen wir untersuchen, inwieweit sich diese Eigenschaften auch bei anderen Ringen wiederfinden lassen. Außerdem werden wir einem Ring die sogenannte Einheitengruppe zuordnen und diese dann mit Hilfe der Methoden der Gruppentheorie aus Kapitel 2 untersuchen.

In Verallgemeinerung der ganzen Zahlen ist ein **kommutativer Ring mit 1** eine Menge R mit Verknüpfungen + (Addition) und $\cdot$ (Multiplikation), sodass

1) $(R, +)$ eine abelsche Gruppe (mit neutralem Element 0) ist,

2) $(R, \cdot)$ ein kommutatives Monoid (mit neutralem Element 1) ist,

3) das von $\mathbb{Z}$ bekannte Distributivgesetz

$$a \cdot (b + c) = a \cdot b + a \cdot c$$

für alle $a, b, c \in R$ gilt.

Neben $\mathbb{Z}$ ist zum Beispiel auch die Restklassengruppe

$$\mathbb{Z}/n\mathbb{Z} = \left\{\overline{0}, ..., \overline{n-1}\right\}$$

ein Ring durch Multiplikation der Repräsentanten

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

Dies ist wohldefiniert, denn

$$(a + k_1 \cdot n) \cdot (b + k_2 \cdot n) = a \cdot b + n \cdot (k_1 \cdot b + k_2 \cdot a + k_1 \cdot k_2 \cdot n)$$

Beispielsweise sind die Verknüpfungen auf $\mathbb{Z}/4\mathbb{Z}$ gegeben durch

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Wir sehen, dass $\overline{3}$ bezüglich $\cdot$ ein Inverses hat, denn

$$\overline{3} \cdot \overline{3} = \overline{1}$$

Allgemein bezeichnet man ein Element $a \in R$ als **Einheit**, wenn ein $b \in R$ existiert mit

$$a \cdot b = 1$$

Die Menge der Einheiten $R^\times$ ist bezüglich $\cdot$ eine Gruppe, die **Einheitengruppe**, zum Beispiel hat $(\mathbb{Z}/4\mathbb{Z})^\times$ die Gruppentafel

$\cdot$	$\overline{1}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{3}$	$\overline{1}$

Dagegen ist $\overline{2}$ keine Einheit, es gilt sogar

$$\overline{2} \cdot \overline{2} = \overline{0}$$

Allgemein heißt $a \in R$ **Nullteiler** von R, wenn ein $0 \neq b \in R$ existiert mit

$$a \cdot b = 0$$

Jede Einheit ist ein Nichtnullteiler, denn ist a eine Einheit und $a \cdot b = 0$, dann ist $b = a^{-1}ab = 0$. In den Übungen werden wir zeigen, dass in einem endlichen Ring R jedes Element entweder Einheit oder Nullteiler ist.

Im Ring $\mathbb{Z}$ gibt es (außer 0) keine Nullteiler. Allgemein heißt ein (kommutativer) Ring ohne nicht-triviale Nullteiler **Integritätsring**. Man kann dann durch Einführen von Brüchen jedes Element außer 0 zu einer Einheit machen. Die Verknüpfungen sind

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd} \quad \text{und} \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$$

wir brauchen also $b, d \neq 0 \Rightarrow bd \neq 0$. Zum Beispiel bilden wir so $\mathbb{Q}$ aus $\mathbb{Z}$. Ein Ring, in dem jedes Element ungleich 0 eine Einheit ist, heißt **Körper**. Durch Bruchrechnung mit Elementen eines Integritätsrings erhält man den sogenannten Quotientenkörper.

Die folgenden weiteren Klassen verallgemeinern die wesentlichen Eigenschaften der ganzen Zahlen:

	Eigenschaften	Beispiel für $R = \mathbb{Z}$
{Integritätsringe}	Quotientenkörperkonstruktion	$\mathbb{Q}$
$\cup$		
{Faktorielle Ringe}	Eindeutige Primfaktorisierung (bis auf Einheiten), Existenz des ggT	$120 = 2^3 \cdot 3 \cdot 5$ $84 = 2^2 \cdot 3 \cdot 7$ $\mathrm{ggT}(120, 84) = 2^2 \cdot 3$
$\cup$		
{Hauptidealringe}	Jedes Ideal (d.h. eine Untergruppe in der auch alle R-Vielfache liegen) wird von einem Element erzeugt	$120\mathbb{Z} + 84\mathbb{Z} = \underbrace{12\mathbb{Z}}_{\mathrm{ggT}(120,84)}$
$\cup$		
{Euklidische Ringe}	Euklidischer Algorithmus zur Bestimmung des ggT	$120 = 1 \cdot 84 + 36$ $84 = 2 \cdot 36 + 12$ $36 = 3 \cdot 12 + 0$

Wir bemerken noch, dass die von 120 und 84 erzeugte Untergruppe

$$120\mathbb{Z} + 84\mathbb{Z} = \{120 \cdot n_1 + 84 \cdot n_2 \mid n_1, n_2 \in \mathbb{Z}\} \subset \mathbb{Z}$$

für $r \in \mathbb{Z}$ auch

$$r \cdot (120 \cdot n_1 + 84 \cdot n_2) = 120 \cdot (r \cdot n_1) + 84 \cdot (r \cdot n_2)$$

enthält, also ein Ideal ist. Wie in Beispiel 2.3.19 gezeigt, wird sie schon von $\mathrm{ggT}(120, 84) = 12$ erzeugt.

3.2 Grundbegriffe

Definition 3.2.1 *Ein* ***Ring*** $(R, +, \cdot)$ *ist eine Menge* R *zusammen mit zwei Verknüpfungen*

$$+ : R \times R \longrightarrow R, \ (a, b) \longmapsto a + b$$
$$\cdot : R \times R \longrightarrow R, \ (a, b) \longmapsto a \cdot b$$

für die gilt

(R1) $(R, +)$ *ist eine abelsche Gruppe,*

(R2) die Multiplikation $\cdot$ *ist assoziativ,*

(R3) die Verknüpfungen sind distributiv, d.h.

$$a \cdot (b + c) = a \cdot b + a \cdot c$$
$$(a + b) \cdot c = a \cdot c + b \cdot c$$

für alle $a, b, c \in R$.

Existiert darüber hinaus ein ***Einselement****, d.h.*

(R4) $\exists\ 1 \in R,\ 1 \neq 0$ *mit*

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

für alle $a \in R$ *so spricht man von einem* ***Ring mit 1*** *(als neutrales Element des Monoids* $(R, \cdot)$ *ist die* 1 *eindeutig), und ist*

(R5) die Multiplikation $\cdot$ ***kommutativ****, d.h.*

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

für alle $a, b \in R$*, so nennt man* R *einen* ***kommutativen Ring****.*

Ist $\varnothing \neq U \subset R$ mit $+$ und $\cdot$ ein Ring, dann bezeichnen wir U als ***Unterring*** *von R.*

Wir schreiben für das Null- und Einselement auch 0_R und 1_R, falls im Kontext verschiedene Ringe vorkommen.

Beispiel 3.2.2 *1) $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind kommutative Ringe mit 1.*

2) Sei V ein K-Vektorraum. Dann ist der Endomorphismenring $\mathrm{End}(V)$ von V ein Ring, der nicht kommutativ ist.

3) Die geraden Zahlen $2\mathbb{Z} \subset \mathbb{Z}$ bilden einen kommutativen Ring ohne 1.

4) Sei X ein topologischer Raum (z.B. $X \subset \mathbb{R}^n$), dann ist

$$\mathcal{C}(X, \mathbb{R}) = \{f : X \longrightarrow \mathbb{R} \mid f \text{ stetig}\}$$

ein kommutativer Ring mit 1.

5) Sei R ein Ring und $X \neq \varnothing$ eine Menge. Dann ist

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

ein Ring mit den Verknüpfungen

$$(f+g)(x) = f(x) + g(x)$$
$$(f \cdot g)(x) = f(x) \cdot g(x)$$

Ist R kommutativ, dann auch $\mathrm{Abb}(X, R)$. Hat R ein Einselement, dann ist

$$X \longrightarrow R,\ x \mapsto 1$$

das Einselement von $\mathrm{Abb}(X, R)$.

6) Sind $R_1, ..., R_n$ Ringe, dann ist das kartesische Produkt $R_1 \times ... \times R_n$ ein Ring mit komponentenweiser Addition

$$(a_1, ..., a_n) + (b_1, ..., b_n) = (a_1 + b_1, ..., a_n + b_n)$$

(d.h. mit der Struktur des direkten Produkts der Gruppen $(R_i, +)$) und ebenso komponentenweiser Multiplikation

$$(a_1, ..., a_n) \cdot (b_1, ..., b_n) = (a_1 \cdot b_1, ..., a_n \cdot b_n)$$

Definition 3.2.3 *Seien R und S Ringe. Ein* ***Ringhomomorphismus***

$$\varphi : R \longrightarrow S$$

ist eine Abbildung, die

$$\varphi(a+b) = \varphi(a) + \varphi(b)$$

und

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$$

für alle $a, b \in R$ erfüllt (insbesondere ist $\varphi : (R,+) \longrightarrow (S,+)$ ein Gruppenhomomorphismus). Sind R und S Ringe mit 1, so verlangen wir (in der Regel) außerdem

$$\varphi(1_R) = 1_S$$

Das Bild von $\varphi(R) \subset S$ ist ein Unterring, ebenso der Kern

$$\ker \varphi = \{r \in R \mid \varphi(r) = 0\} \subset R$$

Für einen Ring R mit 1 ist $\ker \varphi$ ein Ring mit 1 nur in dem Spezialfall der Nullabbildung, denn

$$1_R \in \ker \varphi \Longleftrightarrow \varphi(r) = \varphi(r \cdot 1_R) = \varphi(r) \cdot \varphi(1_R) = 0 \ \ \forall r \in R \Longleftrightarrow \ker \varphi = R$$

Auf diese Eigenschaft des Kerns werden wir im Abschnitt 3.3 über Ideale zurückkommen.

Definition 3.2.4 *Einen Ring S zusammen mit einem Ringhomomorphismus $\varphi : R \longrightarrow S$ nennen wir auch eine* ***R-Algebra****, wenn*

1) *φ injektiv ist und*

2) *jedes Element von R mit jedem Element von S vertauscht, d.h.*

$$\varphi(R) \subset Z(S) := \{z \in S \mid zs = sz \ \ \forall s \in S\}$$

Der Unterring $Z(S) \subset S$ heißt ***Zentrum*** *von S. Die Bedingung (2) impliziert, dass R kommutativ sein muss und ist zum Beispiel für einen kommutativen Ring S automatisch erfüllt.*

Für R-Algebren S_1 und S_2 mit $\iota_i : R \to S_i$ injektiv, heißt ein Ringhomomorphismus $\varphi : S_1 \longrightarrow S_2$ ***Homomorphismus von R-Algebren****, wenn er mit den ι_i verträglich ist, d.h. $\varphi \circ \iota_1 = \iota_2$.*

Beispiel 3.2.5 *1) Ist K ein Körper und $L \supset K$ ein Oberkörper, dann ist L eine K-Algebra.*

2) Ein K-Vektorraum V ist eine K-Algebra, wenn auf V eine Multiplikation

$$\cdot : V \times V \to V$$

gegeben ist, sodass $(V, +, \cdot)$ ein Ring mit 1 ist und für alle $a, b \in V$ und $\lambda \in K$ gilt

$$\lambda(a \cdot b) = (\lambda a) \cdot b = a \cdot (\lambda b)$$

Der Monomorphismus $\varphi : K \to V$ mit $\varphi(\lambda) = \lambda 1_V$ repräsentiert die Skalarmultiplikation, d.h.

$$\lambda a = \varphi(\lambda) \cdot a$$

für $\lambda \in K$ und $a \in V$.

3) Beispielsweise ist der K-Vektorraum $K^{n\times n}$ der $n\times n$-Matrizen eine K-Algebra mit der Matrizenmultiplikation $\cdot : K^{n\times n} \times K^{n\times n} \to K^{n\times n}$ und

$$\begin{array}{rccl} \varphi: & K & \longrightarrow & K^{n\times n} \\ & \lambda & \longmapsto & \lambda E = \begin{pmatrix} \lambda & & \\ & \ddots & \\ & & \lambda \end{pmatrix} \end{array}$$

Für die Skalarmultiplikation gilt also

$$\lambda M = \varphi(\lambda) \cdot M = (\lambda m_{ij}) \in K^{n\times n}$$

mit $\lambda \in K$ und $M = (m_{ij}) \in K^{n\times n}$.

Man beachte auch, dass Vielfache der Einheitsmatrix E (der 1 des Rings $K^{n\times n}$) mit jeder anderen Matrix kommutieren, obwohl $K^{n\times n}$ nicht kommutativ ist.

4) Allgemeiner, ist V ein K-Vektorraum, dann ist $\mathrm{End}(V)$ eine K-Algebra.

5) $\mathrm{Abb}(X,R)$ *ist eine* R*-Algebra.*

6) $\mathcal{C}(X,\mathbb{R})$ *ist eine* $\mathbb{R}$*-Algebra.*

Beispiel 3.2.6 *Ist* R *ein beliebiger Ring mit* 1*, dann ist*

$$\begin{array}{rccl} \chi: & \mathbb{Z} & \longrightarrow & R \\ & n & \longmapsto & n\cdot 1_R := \underbrace{1_R+\ldots+1_R}_{n\text{-mal}} \end{array}$$

ein Ringhomomorphismus.

Durch χ *wird* R *zu einer* $\mathbb{Z}$*-Algebra, denn für alle* $n\in\mathbb{Z}$ *und* $r\in R$ *gilt*

$$\chi(n)\cdot r=(1_R+\ldots+1_R)\cdot r=\underbrace{r+\ldots+r}_{n\text{-mal}}=r\cdot(1_R+\ldots+1_R)=r\cdot\chi(n)$$

(und χ *ist durch die Eigenschaft* $\chi(1)=1_R$ *eindeutig bestimmt).*

Ein wichtiges Beispiel für Homomorphismen von Algebren ist das Einsetzen in ein Polynom.

Definition 3.2.7 *Sei* R *ein kommutativer Ring mit* 1*. Der* ***Polynomring*** $R[x]$ *über* R *in der Unbestimmten* x *ist die Menge aller Abbildungen* $a:\mathbb{N}_0\to R$ *mit* $a(j)=0$ *für alle bis auf endlich viele* $j\in\mathbb{N}_0$*. Die Abbildung*

$$j\mapsto\begin{cases}1 & \text{für } j=n\\ 0 & \text{sonst}\end{cases}$$

bezeichnen wir als x^n*. Dann hat jedes* $0\neq f\in R[x]$ *eine eindeutige Darstellung*

$$f=a_0x^0+a_1x^1+\ldots+a_nx^n$$

mit $n\in\mathbb{N}_0$*,* $a_i\in R$*,* $a_n\neq 0$*. Wir nennen* $\deg(f):=n$ *den* ***Grad*** *von* f *und setzen* $\deg(0)=-\infty$*.*

Durch $R\to R[x]$*,* $a_0\mapsto a_0x^0$ *ist* $R[x]$ *eine kommutative* R*-Algebra mit* 1 *und wir können* $1_{R[x]}=1\cdot x^0=1_R$ *identifizieren. Polynome werden auf die übliche Weise addiert und multipliziert:*

$$\begin{aligned}&(a_0+a_1x+\ldots+a_nx^n)+(b_0+b_1x+\ldots+b_nx^n)\\&=(a_0+b_0)+(a_1+b_1)x+\ldots+(a_n+b_n)x^n\end{aligned}$$

(man beachte, dass wir annehmen können, dass beide Polynome den selben Grad haben, indem wir Koeffizienten gleich 0 *zulassen)*

$$\begin{aligned}&(a_0 + a_1x + ... + a_nx^n) \cdot (b_0 + b_1x + ... + b_mx^m)\\ &= c_0 + c_1x + ... + c_{n+m}x^{n+m}\end{aligned}$$

wobei

$$c_k = \sum_{j=0}^{k} a_j b_{k-j}$$

Polynomringe in mehr als einer Variablen definieren wir induktiv als

$$R[x_1, ..., x_n] = R[x_1, ..., x_{n-1}][x_n]$$

Bemerkung 3.2.8 *Für einen Körper* K *könnte man versuchen,* $K[x]$ *als Unteralgebra von* $\mathrm{Abb}(K, K)$ *aufzufassen. Dieser Ansatz versagt für endliche Körper* $\mathbb{F}_q$ *(mit* q *Elementen), denn* $\mathrm{Abb}(\mathbb{F}_q, \mathbb{F}_q)$ *hat nur endlich viele Elemente,* $\mathbb{F}_q[x]$ *aber unendlich viele.*

Siehe auch Übung 3.12.

Satz 3.2.9 (Universelle Eigenschaft des Polynomrings) *Sei* R *ein kommutativer Ring mit* 1 *und* S *eine* R*-Algebra und* $s \in S$ *ein Element. Dann gibt es genau einen* R*-Algebrenhomomorphismus*

$$\varphi : R[x] \longrightarrow S$$

mit

$$x \longmapsto s$$

den sogenannten ***Substitutionshomomorphismus****. Das Bild* $R[s] := \mathrm{Bild}(\varphi)$ *von* φ *heißt die von* s *erzeugte* ***Unteralgebra****. Genauso geht man in mehreren Variablen vor.*

Beweis. Durch

$$\varphi(a_0 + a_1x + ... + a_nx^n) := a_0 + a_1s + ... + a_ns^n$$

ist der eindeutig bestimmte Homomorphismus gegeben, beispielsweise die Multiplikativität

$$\begin{aligned}\varphi\left(\left(\sum_{i=1}^{n} a_i x^i\right)\cdot\left(\sum_{j=1}^{m} b_j x^j\right)\right) &= \varphi\left(\sum_{k=1}^{n+m}\left(\sum_{i=1}^{k} a_i b_{k-i}\right)x^k\right)\\ &= \sum_{k=1}^{n+m}\left(\sum_{i=1}^{k} a_i b_{k-i}\right)s^k\\ &= \sum_{i=1}^{n}\sum_{j=1}^{m} a_i s^i b_j s^j\\ &= \left(\sum_{i=1}^{n} a_i s^i\right)\cdot\left(\sum_{j=1}^{m} b_j s^j\right)\end{aligned}$$

wobei wir verwenden, dass s^i und b_j vertauschen. Weiter ist $R[s] \subset S$ ein Ring und $R \subset R[s]$. ■

Beispiel 3.2.10 *1) Sei K ein Körper. Einsetzen eines Endomorphismus $A \in K^{n\times n} = \mathrm{End}(K^n)$ in Polynome*

$$\begin{array}{rccc}\varphi_A\colon & K[x] & \longrightarrow & \mathrm{End}(K^n)\\ & x & \longmapsto & A\end{array}$$

ist ein Substitutionshomomorphismus. Zum Beispiel sind das charakteristische Polynom χ_A und das Minimalpolynom p_A von A im Kern von φ_A.

2) Sei $d \in \mathbb{Z}$. Betrachte für $\sqrt{d} \in \mathbb{C}$ den Substitutionshomomorphismus

$$\mathbb{Z}[x] \to \mathbb{C},\ x \mapsto \sqrt{d}$$

Dann ist

$$\mathbb{Z}\left[\sqrt{d}\right] = \left\{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\right\}$$

denn $\sqrt{d}^2 = d \in \mathbb{Z}$.

3) Sei $d \in \mathbb{Z}$ mit $d \equiv 1 \bmod 4$. Dann ist

$$\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{a + b\frac{1+\sqrt{d}}{2} \mid a, b \in \mathbb{Z}\right\}$$

denn

$$\left(\frac{1+\sqrt{d}}{2}\right)^2 = \frac{1+d}{4} + \frac{2}{4}\sqrt{d} = \underbrace{\frac{d-1}{4}}_{\in\mathbb{Z}} + \frac{1+\sqrt{d}}{2}$$

da $d-1$ von 4 geteilt wird.

3.3 Ideale

In diesem Abschnitt wollen wir untersuchen, inwieweit wir der Quotientengruppe die Struktur eines Rings geben können. Sei R ein kommutativer Ring mit 1. Jede Untergruppe $I \subset (R,+)$ ist ein Normalteiler, wir können also die Quotientengruppe R/I bilden und der surjektive Gruppenhomomorphismus

$$\begin{array}{rccc} \pi: & (R,+) & \longrightarrow & (R/I,+) \\ & r & \longmapsto & \bar{r} = r + I \end{array}$$

hat $\ker \pi = I$ und das neutrale Element von R/I bezüglich + ist $0 + I = I$.

Wollen wir auch eine induzierte Multiplikation auf R/I, sodass π ein Ringhomomorphismus ist, dann muss die Multiplikation repräsentantenweise definiert werden, denn

$$(r_1 + I) \cdot (r_2 + I) = \pi(r_1) \cdot \pi(r_2) = \pi(r_1 r_2) = r_1 r_2 + I$$

Im Allgemeinen wird die repräsentantenweise Multiplikation jedoch nicht wohldefiniert sein. Ist $r_2' = r_2 + b$ mit $b \in I$ ein anderer Repräsentant von $r_2 + I$, dann gilt

$$r_1 \cdot r_2' = r_1 \cdot r_2 + r_1 \cdot b$$

also sollte $r_1 \cdot b \in I$ für alle $r_1 \in R$ und $b \in I$ gelten. Untergruppen von $(R,+)$ mit dieser Eigenschaft nennt man Ideale:

Definition 3.3.1 *Sei R ein kommutativer Ring mit 1. Ein **Ideal** ist eine nicht leere Teilmenge $I \subset R$ mit*

$$\begin{aligned} a + b &\in I \\ ra &\in I \end{aligned}$$

für alle $a, b \in I$ und $r \in R$.

Wir bemerken, dass mit $a \in I$ auch das additiv Inverse $-a \in I$ ist.

Insgesamt haben wir also gezeigt (als leichte Übung folgt das Distributivgesetz in R/I direkt aus dem in R):

Satz 3.3.2 *Sei $I \subset R$ ein Ideal. Dann trägt die Quotientengruppe R/I die Struktur eines kommutativen Rings mit 1 mit repräsentantenweiser Multiplikation*

$$(r_1 + I) \cdot (r_2 + I) := r_1 r_2 + I$$

*Das neutrale Element von R/I bezüglich $\cdot$ ist $1+I$. Wir bezeichnen R/I als **Quotientenring** von R nach I.*

Ideale spielen also eine wichtige Rolle in der Ringtheorie.

Beispiel 3.3.3 *1) Sei $\varphi : R \longrightarrow S$ ein Ringhomomorphismus. Dann ist der Kern*

$$\ker \varphi = \{r \in R \mid \varphi(r) = 0\} \subset R$$

ein Ideal, denn ist $\varphi(r) = 0$ und $r' \in R$, dann ist auch

$$\varphi(r' \cdot r) = \varphi(r') \cdot \varphi(r) = 0$$

2) Seien $a_1, ..., a_n \in R$. Dann ist

$$(a_1, ..., a_n) := \{\textstyle\sum_{i=1}^{n} r_i a_i \mid r_i \in R\}$$

*ein Ideal, das von von dem **Erzeugendensystem** $a_1, ..., a_n$ erzeugte Ideal. Mit Ringen, in denen jedes Ideal von dieser Form ist, werden wir und in Abschnitt 3.6 genauer beschäftigen.*

3) Sind $I_1, I_2 \subset R$ Ideale, dann auch deren Durchschnitt $I_1 \cap I_2$.

4) Eine weitere wichtige Klasse sind Ringe, in denen ein Ideal stets von einem einzigen Element erzeugt wird, die sogenannten Hauptidealringe, die wir in den Abschnitten 3.8 und 3.9 behandeln werden. Zum Beispiel sind die Ideale von $\mathbb{Z}$ alle von der Form

$$n\mathbb{Z} = \{na \mid a \in \mathbb{Z}\} = (n)$$

mit $n \in \mathbb{Z}$:

In Beispiel 2.2.6 hatten wir schon gezeigt, dass dies genau die Untergruppen von $(\mathbb{Z}, +)$ sind. Weiter ist $n\mathbb{Z} \subset \mathbb{Z}$ ein Ideal, denn für $m \in \mathbb{Z}$ und $n \cdot k \in n\mathbb{Z}$ ist $m \cdot (n \cdot k) = n \cdot (m \cdot k) \in n\mathbb{Z}$.

5) *Sei* $I = (n) \subset \mathbb{Z}$, *dann ist die Restklassengruppe modulo* n

$$\mathbb{Z}/n = \left\{\bar{0}, \bar{1}, ..., \overline{n-1}\right\} = \mathbb{Z}/(n)$$

ein kommutativer Ring mit 1.

Satz 3.3.4 (Homomorphiesatz) *Sei* $\varphi : R \longrightarrow S$ *ein Ringhomomorphismus. Dann gilt*

$$R/\ker\varphi \cong \text{Bild}\,\varphi$$

Beweis. Aus Satz 2.3.15 erhalten wir einen Isomorphismus

$$\begin{aligned}\widetilde{\varphi} : R/\ker\varphi &\longrightarrow \text{Bild}\,\varphi\\ \bar{r} = r + \ker\varphi &\longmapsto \varphi(r)\end{aligned}$$

der additiven abelschen Gruppen. Weiter ist $\widetilde{\varphi}$ ein Ringhomomorphismus, denn

$$\begin{aligned}\widetilde{\varphi}((r_1 + \ker\varphi)(r_2 + \ker\varphi)) &= \widetilde{\varphi}(r_1 r_2 + \ker\varphi) = \varphi(r_1 r_2)\\ &= \varphi(r_1)\varphi(r_2) = \widetilde{\varphi}(r_1 + \ker\varphi)\widetilde{\varphi}(r_2 + \ker\varphi)\end{aligned}$$

■

Bemerkung 3.3.5 *Allgemeiner kann man* φ *über* R/I *für jedes Ideal* $I \subset \ker\varphi$ *faktorisieren.*

3.4 Integritätsringe

3.4.1 Einheiten und Nullteiler

Definition 3.4.1 *Sei* R *ein Ring.*

1) *Ein Element* $a \in R$ *heißt rechter (linker)* ***Nullteiler*** *von* R, *wenn ein* $x \in R\backslash\{0\}$ *existiert mit* $xa = 0$ *(bzw.* $ax = 0$*).*

2) *Ein Ring ohne rechte und linke Nullteiler außer* 0 *heißt* ***nullteilerfrei****.*

   Nullteilerfreie kommutative Ringe nennt man ***Integritätsringe****.*

3) *Sei R ein Ring mit 1. Ein Element $u \in R$ heißt* ***Einheit*** *von R, wenn ein $w \in R$ existiert mit*

$$uw = wu = 1$$

Die Menge der Einheiten wird mit $R^\times$ bezeichnet. Mit u ist offenbar auch w eine Einheit und $(R^\times, \cdot)$ ist eine Gruppe, die ***Einheitengruppe*** *von R. Das Inverse $w = u^{-1}$ ist in $R^\times$ eindeutig (Übung 2.1).*

Siehe auch Übungsaufgaben 3.8 und 3.9.

Definition 3.4.2 *Einen Ring R mit 1, sodass*

$$R^\times = R \setminus \{0\}$$

nennt man ***Schiefkörper****. Ein kommutativer Schiefkörper ist ein* ***Körper****.*

Bemerkung 3.4.3 *Jeder Unterring eines Integritätsrings ist selbst ein Integritätsring.*

Beispiel 3.4.4 *1) $\mathbb{Z}$ ist ein Integritätsring. Die Einheiten sind $+1$ und -1, also*

$$\mathbb{Z}^\times = \{+1, -1\} \cong \mathbb{Z}/2$$

2) *Jeder Körper K ist ein Integritätsring. Die Einheiten sind $K^\times = K \setminus \{0\}$.*

3) *$\mathbb{Z}/(6) = \{\overline{0}, \overline{1}, \ldots \overline{5}\}$ ist kein Integritätsring, $\overline{2}, \overline{3}, \overline{4}$ (und natürlich $\overline{0}$) sind Nullteiler, $\overline{1}, \overline{5}$ sind Einheiten. Siehe auch Übungsaufgaben 3.2 und 3.5.*

4) *Sei R ein Integritätsring. Dann ist auch $R[x]$ ein Integritätsring, denn für*

$$f = a_0 + a_1 x + \ldots + a_n x^n \quad \text{und} \quad g = b_0 + b_1 x + \ldots + b_m x^m$$

mit $a_n, b_m \neq 0$ ist

$$f \cdot g = (c_0 + c_1 x + \ldots + c_{n+m} x^{n+m})$$

und

$$c_{n+m} = a_n \cdot b_m \neq 0$$

Für die Einheitengruppe gilt

$$R[x]^\times = R^\times$$

denn falls $f \cdot g = 1$, *dann*

$$0 = \deg(1) = \deg(f \cdot g) = \deg(f) + \deg(g) = n + m$$

also $n = m = 0$.

Induktiv folgt, dass $R[x_1, ..., x_n]$ *ein Integritätsring ist.*

5) *Der Ring* $\mathcal{C}([0,1], \mathbb{R})$ *der stetigen Funktionen* $[0,1] \longrightarrow \mathbb{R}$ *ist kein Integritätsring, da stetige Funktionen ungleich* 0 *existieren, deren Produkt die Nullfunktion gibt. Die Einheiten* $\mathcal{C}([0,1], \mathbb{R})^\times$ *sind die stetigen Funktionen ohne Nullstellen.*

6) *Die Einheiten des Rings der* ***Gaußschen Zahlen***

$$\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$$

sind

$$\mathbb{Z}[i]^\times = \{1, -1, i, -i\}$$

denn sind $z_j = a_j + ib_j \in \mathbb{Z}[i]$, *dann gilt*

$$|z_1 \cdot z_2| = |z_1| \cdot |z_2|$$

und $|z_j|^2 = a_j^2 + b_j^2 \in \mathbb{Z}$. *Ist also* $z_1 \cdot z_2 = 1$, *dann folgt*

$$a_j^2 + b_j^2 = |z_j|^2 = 1$$

mit $a_j, b_j \in \mathbb{Z}$ *also* $z_1, z_2 \in \{1, -1, i, -i\}$ *und dies sind offenbar Einheiten.*

Weiter ist $\mathbb{Z}[i]$ *ein Integriätsring, denn wäre* $z_1 \cdot z_2 = 0$, *dann auch* $|z_1| = 0$ *oder* $|z_2| = 0$. *Es gilt aber* $0 = |z_j|^2 = a_j^2 + b_j^2$ *genau dann, wenn* $a_j = b_j = 0$.

Zum formalen Potenzreihenring siehe Übung 3.12.

Beispiel 3.4.5 *Die* ***Quaternionen***

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$$

mit den Regeln

$$i^2 = j^2 = k^2 = ijk = -1$$

sind ein Beispiel für einen Schiefkörper, der kein Körper ist. Aus obigen Regeln folgt

$$\begin{array}{ccccc} ij & = & k & = & -ji \\ jk & = & i & = & -kj \\ ki & = & j & = & -ik \end{array}$$

Satz 3.4.6 *Jeder endliche Integritätsring ist ein Körper.*

Dies zeigen wir in Übung 3.5.

Bemerkung 3.4.7 *Für Integritätsringe können wir analog zur Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$ den* ***Quotientenkörper*** *bilden, siehe Übungsaufgabe 3.10.*

Definition 3.4.8 *Sei K ein Körper und*

$$\begin{array}{rccc} \chi: & \mathbb{Z} & \longrightarrow & K \\ & n & \longmapsto & n \cdot 1_K \end{array}$$

die charakteristische Abbildung. Der Kern ist ein Ideal

$$\ker \chi = (p)$$

mit $p \geq 0$. Zwei Fälle können auftreten:

1) *$p = 0$, d.h. χ ist injektiv. In diesem Fall lässt sich χ zu einem Monomorphismus $\mathbb{Q} \hookrightarrow K$ fortsetzen (siehe Übung 3.10), d.h. wir haben Monomorphismen*

$$\begin{array}{ccc} \mathbb{Z} & \to & K \\ \downarrow & \nearrow & \\ \mathbb{Q} & & \end{array}$$

(mit der Einbettung $j : \mathbb{Z} \to \mathbb{Q}$, $n \mapsto \frac{n}{1}$).

2) $p > 0$. *Dann ist*

$$\mathbb{Z}/(p) \hookrightarrow K$$

nach dem Homomorphiesatz 3.3.4 ein Unterring von K *und damit ein Integritätsring. Somit muss* p *eine Primzahl sein, denn wäre* $p = a \cdot b$ *mit* $a, b > 1$, *dann* $\bar{a} \cdot \bar{b} = \bar{0}$, *also* $\bar{a}, \bar{b} \neq \bar{0}$ *Nullteiler. Dann ist*

$$\mathbb{F}_p := \mathbb{Z}/(p)$$

der Körper mit p *Elementen (siehe auch Übung 3.5).*

In beiden Fällen nennt man

$$\operatorname{char}(K) = p \geq 0$$

die ***Charakteristik*** *des Körpers* K.

3.4.2 Primideale und maximale Ideale

Hier wollen wir untersuchen, wann der Quotientenring nach einem Ideal ein Integritätsring oder ein Körper ist. Im folgenden Abschnitt geben wir eine geometrische Interpretation dazu.

Definition 3.4.9 *Sei* R *ein kommutativer Ring mit* 1. *Ein Ideal* $P \subsetneq R$ *heißt* ***Primideal****, wenn* $\forall a, b \in R$ *gilt*

$$a \cdot b \in P \Longrightarrow a \in P \text{ oder } b \in P$$

Ein Ideal $m \subsetneq R$ *heißt* ***maximales Ideal****, wenn für Ideale* $I \subset R$ *gilt*

$$m \subset I \subsetneq R \Longrightarrow m = I$$

Beispiel 3.4.10 *Sei* $(n) = n\mathbb{Z} \subset \mathbb{Z}$ *ein Ideal,* $n > 0$. *Dann gilt*

$$(n) \text{ ist ein Primideal} \Longleftrightarrow n \text{ ist eine Primzahl}$$

Ist p *prim, dann gilt*

$$ab \in (p) \Rightarrow p \mid a \cdot b \Rightarrow p \mid a \text{ oder } p \mid b \Rightarrow a \in (p) \text{ oder } b \in (p)$$

Ist (ab) *ein Primideal mit* $a, b > 0$, *dann* $a \in (ab)$ *oder* $b \in (ab)$, *d.h.* ab *teilt* a *oder* b *und somit* $b = 1$ *oder* $a = 1$.

Ist p prim, dann ist (p) auch schon ein maximales Ideal: Sei $(p) \subsetneqq I \subset \mathbb{Z}$. Dann existiert ein $q \in I$ mit $p \nmid q$, also $\mathrm{ggT}(q,p) = 1$. Damit liegt auch 1 in I, also $I = R$.

Wir bemerken noch, dass $(0) \subset \mathbb{Z}$ ein Primideal ist, aber nicht maximal, denn

$$(0) \subsetneqq (p) \subsetneqq \mathbb{Z}$$

Satz 3.4.11 *Sei R ein kommutativer Ring mit 1 und $I \subsetneqq R$ ein Ideal. Dann gilt*

1) I prim $\Longleftrightarrow$ R/I ist ein Integritätsring.

2) I maximal $\Longleftrightarrow$ R/I ist ein Körper.

Beweis.

1) Ist I prim, dann

$$\overbrace{(a+I)(b+I)}^{ab+I} = 0_{R/I} = I \Leftrightarrow a \cdot b \in I$$
$$\Rightarrow a \in I \text{ oder } b \in I$$
$$\Rightarrow a + I = I = 0_{R/I} \text{ oder } b + I = I = 0_{R/I}$$

das heißt R/I ist ein Integritätsring.

Sei umgekehrt R/I ein Integritätsring. Dann gilt

$$a \cdot b \in I \Leftrightarrow (a+I)(b+I) = I = 0_{R/I}$$
$$\Rightarrow a + I = 0_{R/I} = I \text{ oder } b + I = 0_{R/I} = I$$
$$\Rightarrow a \in I \text{ oder } b \in I$$

2) Sei $m \subset R$ maximal und $a + m \neq 0_{R/m} = m \Rightarrow a \notin m \Rightarrow$

$$R = m + (a) = \{w + ba \mid w \in m,\ b \in R\}$$
$$\Leftrightarrow \exists b \in R \text{ und } w \in m \text{ mit } a \cdot b + w = 1$$
$$\Leftrightarrow (a+m)(b+m) = 1 + m = 1_{R/m}$$

Somit ist R/m ein Körper und

$$(a+m)^{-1} = b + m$$

Umgekehrt: Ist R/m ein Körper und $a \notin m$, dann gibt es ein $b \in R$ mit

$$(a+m)(b+m) = 1_{R/m}$$

$\Leftrightarrow m + (a) = R$. Ist also $m \subsetneqq I$, dann ist $I = R$.

■

Siehe auch Übungsaufgabe 3.15 und 3.13.

3.5 Ideale und affine Varietäten

Wir wollen nun Primideale und maximale Ideale des Polynomrings geometrisch interpretieren. Dieser Abschnitt ist als Einschub zu verstehen, wir werden einige Aussagen nicht beweisen.

Sei K ein Körper.

Definition 3.5.1 *Eine **affine Varietät** ist die gemeinsame Nullstellenmenge von Polynomen* $f_1, ..., f_r \in K[x_1, ..., x_n]$

$$V(f_1, ..., f_r) = \{p \in K^n \mid f_1(p) = 0, ..., f_r(p) = 0\}$$

Beispiel 3.5.2 *1)* $V(1) = \varnothing$.

2) $V(0) = K^n$.

3) Sind

$$f_i = \sum_{j=1}^{n} a_{ij} x_j - b_i$$

lineare Polynome, dann ist

$$V(f_1, ..., f_r) = \{p \in K^n \mid A \cdot p = b\}$$

die Lösungsmenge des linearen Gleichungssystems $Ax = b$ *mit* $A = (a_{ij})$ *und* $b = (b_i)$. *Wir können dann* $V(f_1, ..., f_r)$ *mit Hilfe des Gauß-Algorithmus bestimmen.*

4) Ist $g = \frac{a}{b} \in K(x_1) = Q(K[x_1])$ *eine rationale Funktion und*

$$f = x_2 \cdot b(x_1) - a(x_1) \in K[x_1, x_2]$$

dann ist $V(f) \subset K^2$ *der Graph von* g. *Siehe zum Beispiel Abbildung 3.1 für den Funktionsgraphen*

$$V\left(x_2 x_1 - x_1^3 + 1\right)$$

von

$$g(x_1) = \frac{x_1^3 - 1}{x_1}$$

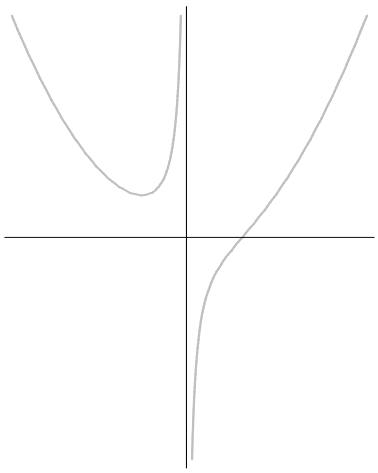


Abbildung 3.1: Funktionengraph

Eine wichtige Beobachtung ist, dass $V(f_1, ..., f_r)$ nur von dem von $f_1, ..., f_r$ erzeugten Ideal

$$I = (f_1, ..., f_r) \subset K[x_1, ..., x_n]$$

abhängt: Gilt $f_1(p) = 0, ..., f_r(p) = 0$, dann verschwindet auch jede R-Linearkombination

$$\left(\sum_{i=1}^{r} s_i \cdot f_i\right)(p) = \sum_{i=1}^{r} s_i(p) f_i(p) = 0$$

für alle $s_i \in K[x_1, ..., x_n]$. Deshalb definiert man:

Definition 3.5.3 *Ist $I \subset K[x_1, ..., x_n]$ ein Ideal, dann heißt*

$$V(I) = \{p \in K^n \mid f(p) = 0 \ \forall f \in I\}$$

*die **Verschwindungsmenge** von I. Dies ist eine affine Varietät, denn jedes $I \subset k[x_1, ..., x_n]$ ist endlich erzeugt (wie wir in Abschnitt 3.6 zeigen).*

Definition 3.5.4 *Ist $S \subset K^n$ eine Teilmenge, dann ist*

$$I(S) = \{f \in K[x_1, ..., x_n] \mid f(p) = 0 \ \forall p \in S\}$$

*(wie wir oben gesehen haben) ein Ideal, das **Verschwindungsideal** von S.*

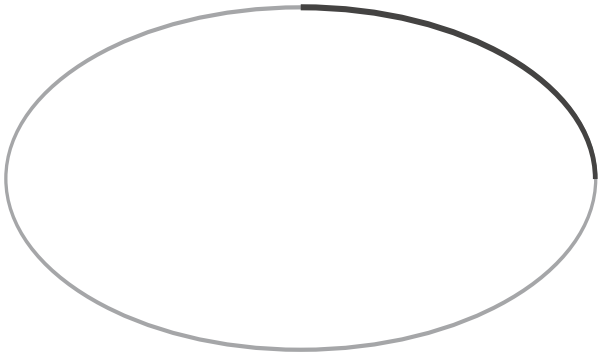


Abbildung 3.2: Ellipsenabschnitt

Beispiel 3.5.5 *Betrachten wir den Ellipsenabschnitt*

$$S = \left\{(x_1, x_2) \in \mathbb{R}^2 \mid x_1^2 + 2x_2^2 = 1 \text{ und } x_1, x_2 \geq 0\right\}$$

in Abbildung 3.2, dann ist

$$I(S) = \left(x_1^2 + 2x_2^2 - 1\right)$$

*und $V(I(S))$ die ganze Ellipse. Dies ist der Abschluss von S in der sogenannten **Zariskitopologie**.*

Durch I und V sind also inklusionsumkehrende Abbildungen zwischen der Menge der Untervarietäten von K^n und der Ideale von $K[x_1, ..., x_n]$ gegeben (jedoch keine $1:1$–Korrespondenz). Mit Idealen und deren Varietäten beschäftigt sich die **algebraische Geometrie**.

Definition 3.5.6 *Wir nennen die Varietät $V(I) \subset K^n$ **irreduzibel**, wenn sie sich nicht als*

$$V(I) = V(J_1) \cup V(J_2)$$

mit $V(J_1), V(J_2) \subsetneqq V(I)$ schreiben lässt.

Dann gilt (ohne Beweis):

Satz 3.5.7 *Durch*

$$\{\text{Primideale von } K[x_1, ..., x_n]\} \underset{I}{\overset{V}{\rightleftarrows}} \{\text{irreduzible affine Var. in } K^n\}$$

ist dann eine $1:1$–Korrespondenz gegeben.

Wir überprüfen dies an einigen Beispielen:

Beispiel 3.5.8 *1) Das Ideal* $(x_2) \subset K[x_1, x_2]$ *ist ein Primideal, denn*

$$K[x_1, x_2]/(x_2) \cong K[x_1]$$

ist ein Integritätsring. Dagegen ist $(x_1 \cdot x_2)$ *kein Primideal, denn*

$$\overline{x_1} \cdot \overline{x_2} = \overline{x_1 \cdot x_2} = \overline{0} \in K[x_1, x_2]/I$$

und $\overline{x_1}, \overline{x_2} \neq \overline{0}$*. Geometrisch entsprechen die Primideale* (x_1) *und* (x_2) *jeweils einer der Koordinatenachsen und* $(x_1 \cdot x_2)$ *deren Vereinigung, also*

$$V(x_1 \cdot x_2) = V(x_1) \cup V(x_2)$$

2) Das Ideal $(x_2 - x_1^2) \subset K[x_1, x_2]$ *ist ein Primideal, denn*

$$\begin{array}{rcl} K[x_1, x_2]/(x_2 - x_1^2) & \to & K[t] \\ x_1 & \mapsto & t \\ x_2 & \mapsto & t^2 \end{array}$$

ist ein Isomorphismus und $K[t]$ *ein Integritätsring. Die Verschwindungsmenge* $V(x_2 - x_1^2)$ *ist eine Parabel.*

Das Ideal

$$I = \left(\left(x_2 - x_1^2\right) \cdot \left(x_1 - x_2^2\right)\right)$$

ist kein Primideal, und

$$V(I) = V\left(x_2 - x_1^2\right) \cup V\left(x_1 - x_2^2\right)$$

siehe Abbildung 3.3. Die Elemente

$$\overline{x_2 - x_1^2},\ \overline{x_1 - x_2^2} \in K[x_1, x_2]/I$$

sind Nullteiler.

3) Das Ideal $(x_1, x_2) \subset K[x_1, x_2]$ *ist ein maximales Ideal, denn* $K[x_1, x_2]/(x_1, x_2) \cong K$ *ist ein Körper.*

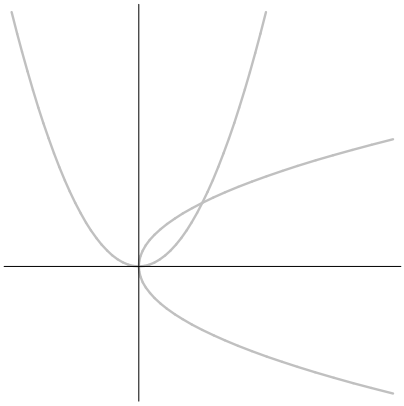


Abbildung 3.3: Reduzible affine Varietät

Ist $K = \mathbb{C}$ (allgemeiner K algebraisch abgeschlossen), dann entsprechen die Punkte genau den maximalen Idealen, d.h. wir haben eine $1:1$-Korrespondenz

$$\begin{array}{ccc} \{\text{maximale Ideale in } K[x_1,...,x_n]\} & \underset{I}{\overset{V}{\rightleftarrows}} & K^n \\ (x-a_1,...,x-a_n) & & (a_1,...,a_n) \end{array}$$

Siehe auch die Übungen 3.22, 3.15 und 3.23.

Beispiel 3.5.9 *Ist $(f) \subset \mathbb{C}[x_1,x_2]$ ein Primideal erzeugt von einem Polynom f vom Grad 3 und $V\left(f, \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}\right) = \varnothing$, dann heißt $C = V(I)$ **elliptische Kurve**. Abbildung 3.4 zeigt die Punkte mit reellen Koordinaten von einer elliptischen Kurve.*

Auf der Menge der Punkte einer elliptischen Kurve existiert die Struktur einer abelschen Gruppe mit der Verknüpfung wie Abbildung 3.5. Was ist das neutrale Element?

Von besonderem Interesse in der Zahlentheorie sind die $\mathbb{Q}$-rationalen Punkte

$$C(\mathbb{Q}) = \left\{p \in \mathbb{Q}^2 \mid f(p) = 0\right\}$$

von C. Der Satz von Mordell besagt, dass $C(\mathbb{Q})$ als Gruppe endlich erzeugt ist.

Die Struktur von endlich erzeugten abelschen Gruppen ist bekannt: Wir werden später zeigen, dass jede endlich erzeugte

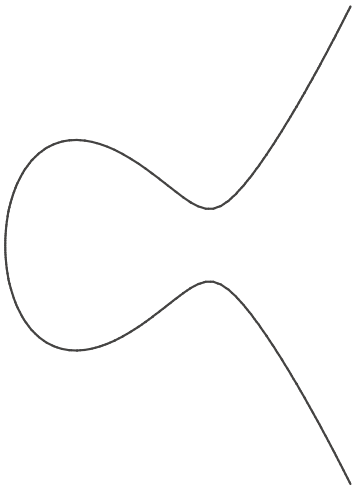


Abbildung 3.4: Elliptische Kurve

abelsche Gruppe ein Produkt von Faktoren $\mathbb{Z}$ und $\mathbb{Z}/n$ (d.h. von zyklischen Gruppen) ist.

Die Frage nach der Anzahl von $\mathbb{Z}$-Faktoren von $C(\mathbb{Q})$ ist Gegenstand aktueller Forschung in der Zahlentheorie (z.B zur Vermutung von Birch und Swinnerton-Dyer).

3.6 Noethersche Ringe

Wie lassen sich Ideale beschreiben? Eine Möglichkeit ist durch ein Erzeugendensystem:

Definition 3.6.1 *Sei R ein kommutativer Ring mit 1 und $a_1, ..., a_n \in R$. In Beispiel 3.3.3 hatten wir gesehen, dass*

$$(a_1, ..., a_n) := \left\{ \sum_{i=1}^{n} b_i a_i \mid b_i \in R \right\} \subset R$$

ein Ideal ist. Wir nennen Ideale dieser Art ***endlich erzeugt****.*

Satz 3.6.2 *Sei R ein kommutativer Ring mit 1. Die folgenden Bedingungen sind äquivalent.*

1) Jedes Ideal $I \subset R$ ist endlich erzeugt.

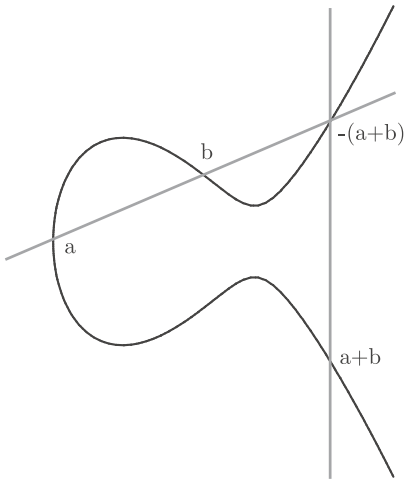


Abbildung 3.5: Gruppenstruktur auf elliptischen Kurven

2) Jede aufsteigende Kette

$$I_1 \subset I_2 \subset I_3 \subset ... \subset I_n \subset ...$$

von Idealen wird stationär, d.h. es gibt ein m, sodass

$$I_m = I_{m+1} = I_{m+2} = ...$$

gilt.

3) Jede nicht leere Menge von Idealen besitzt bezüglich Inklusion ein maximales Element.

Erfüllt R diese äquivalenten Eigenschaften, dann nennt man R ***noethersch****.*

Diese Ringe heißen noethersch nach Emmy Noether (1882-1935), die die allgemeine Strukturtheorie dieser Ringe formuliert und damit die Sätze von Kronecker und Lasker allgemeiner und einfacher bewiesen hat.

Beweis. (1) $\Longrightarrow$ (2): Sei $I_1 \subset I_2 \subset ...$ eine Kette von Idealen. Dann ist

$$I = \bigcup_{j=1}^{\infty} I_j$$

ebenfalls ein Ideal: Sind $a, b \in I$, dann existeren $j_1, j_2 \in \mathbb{N}$ mit $a \in I_{j_1}$, $b \in I_{j_2}$, also

$$a + b \in I_{\max(j_1,j_2)} \subset I$$

Nach (1) ist I endlich erzeugt, also gibt es $a_1, ..., a_n \in I$ mit $I = (a_1, ..., a_n)$. Für jedes a_k existiert ein j_k mit $a_k \in I_{j_k}$. Für

$$m := \max \{j_k \mid k = 1, ..., n\}$$

gilt dann $a_1, ..., a_n \in I_m$, also

$$I = (a_1, ..., a_n) \subset I_m \subset I_{m+1} \subset ... \subset I$$

und somit

$$I_m = I_{m+1} = ...$$

(2) $\Longrightarrow$ (3): Angenommen (3) ist nicht erfüllt. Dann gibt es eine Menge M von Idealen, sodass für jedes $I \in M$ ein $I' \in M$ existiert mit $I \subsetneq I'$. Induktiv können wir also eine Folge

$$I_1 \subsetneq I_2 \subsetneq I_3 \subsetneq ...$$

von Idealen aus M konstruieren, die nicht stationär wird, d.h. (2) ist nicht erfüllt.

(3) $\Longrightarrow$ (1): Sei I ein beliebiges Ideal. Die Menge

$$M = \{J \subset I \mid J \text{ ist endlich erzeugt}\}$$

ist nicht leer, z.B. $(0) \in M$. Sei J ein maximales Element von M, also gibt es $a_1, ..., a_n \in J$ mit $J = (a_1, ..., a_n)$. Wir zeigen $I = J$: Angenommen dies gilt nicht, dann gibt es ein $a \in I \backslash J$ mit

$$J \subsetneq (a_1, ..., a_n, a) \subset I$$

Dies widerspricht der Maximalität von J. ■

Beispiel 3.6.3 *1) Der Ring der ganzen Zahlen $\mathbb{Z}$ ist noethersch, denn die Ideale von $\mathbb{Z}$ sind alle von der Form*

$$(n) = n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$$

also endlich erzeugt (von einem einzigen Element).

2) Ein Körper K hat nur die Ideale (0) und $K = (1)$, siehe auch Übungsaufgabe 3.4. Insbesondere ist K noethersch.

Hilbert hat 1890 gezeigt, dass der Polynomring $K[x_1, ...x_n]$ noethersch ist.

Satz 3.6.4 (Hilbertscher Basissatz) *Sei R ein noetherscher Ring, dann ist $R[x]$ ebenfalls noethersch.*

Daraus erhalten wir mit Induktion nach der Anzahl der Variablen

$$R[x_1, ..., x_n] = R[x_1, ..., x_{n-1}][x_n]$$

und da K und $\mathbb{Z}$ noethersch sind:

Corollar 3.6.5 *Sei K ein Körper. Dann ist der Polynomring $K[x_1, ...x_n]$ in n Variablen noethersch.*
Ebenso ist $\mathbb{Z}[x_1, ...x_n]$ noethersch.

Der Beweis des Hilbertschen Basissatzes betrachtet die Leitkoeffizienten in R von Polynomen in $R[x]$.

Definition 3.6.6 *Sei R ein kommutativer Ring mit 1 und*

$$f(x) = a_k x^k + ... + a_1 x + a_0 \in R[x]$$

ein Polynom. Ist $a_k \neq 0$, also $\deg(f) = k$, dann heißt der Term größten Grades

$$\mathrm{LT}(f) = a_k x^k$$

***Leitterm** von f und*

$$\mathrm{LC}(f) = a_k$$

***Leitkoeffizient** von f.*
*Ist der Leitkoeffizient $a_k = 1$, dann heißt f **normiert**.*

Beweis. Angenommen $R[x]$ ist nicht noethersch. Dann gibt es ein nicht endlich erzeugtes Ideal $I \subset R[x]$. Sei $f_1 \in I$ mit $\deg(f_1)$ minimal, $f_2 \in I \setminus (f_1)$ mit $\deg(f_2)$ minimal, und induktiv

$$f_k \in I \setminus (f_1, ..., f_{k-1})$$

mit $\deg(f_k)$ minimal. Dann gilt

$$\deg(f_1) \leq \deg(f_2) \leq ... \leq \deg(f_k) \leq ...$$

und wir erhalten eine aufsteigende Kette von Idealen in R

$$(\mathrm{LC}(f_1)) \subset (\mathrm{LC}(f_1), \mathrm{LC}(f_2)) \subset ... \subset (\mathrm{LC}(f_1), ..., \mathrm{LC}(f_k)) \subset ...$$

Wir zeigen, dass diese strikt aufsteigend ist (und somit R nicht noethersch): Angenommen

$$(\mathrm{LC}(f_1), ..., \mathrm{LC}(f_k)) = (\mathrm{LC}(f_1), ..., \mathrm{LC}(f_{k+1}))$$

Dann können wir schreiben

$$\mathrm{LC}(f_{k+1}) = \sum_{j=1}^{k} b_j \mathrm{LC}(f_j)$$

mit $b_j \in R$. Somit hat

$$g := \sum_{j=1}^{k} b_j \cdot x^{\deg(f_{k+1})-\deg(f_j)} \cdot f_j \in I$$

den selben Leitkoeffizienten wie f_{k+1}, also

$$\deg(g - f_{k+1}) < \deg(f_{k+1})$$

ein Widerspruch, da f_{k+1} mit minimalem Grad gewählt war. ■

3.7 Faktorielle Ringe

Im ganzen Abschnitt ist R ein Integritätsring.

3.7.1 Teilbarkeit und Zerlegung in irreduzible Elemente

Definition 3.7.1 *Seien $a, b \in R$. Dann heißt a ein **Teiler** von b, wenn es ein $c \in R$ gibt mit*

$$a \cdot c = b$$

Wir schreiben $a \mid b$.

Lemma 3.7.2 *In einem Integritätsring R gilt:*

1) *(Kürzungsregel) Für $a, b, c \in R$, $c \neq 0$ folgt aus $ac = bc$, dass schon $a = b$.*

2) *Für alle $a \in R$ gilt $a \mid 0$ und $a \mid a$ und $1 \mid a$.*

3) *Seien $a, b, c \in R$. Gilt $c \mid b$ und $b \mid a$, dann $c \mid a$.*

4) *Ist $a \in R$ und $u \in R^\times$ und $a \mid u$, dann ist $a \in R^\times$.*

5) *Seien $a, b, d \in R$ mit $d \mid a$ und $d \mid b$. Dann gilt $d \mid (xa + yb)$ für alle $x, y \in R$.*

6) *Seien $a, b \in R$. Dann ist $(a) \subset (b) \iff b \mid a$.*

7) *Seien $a, b \in R$. Dann gilt*

$$a \mid b \text{ und } b \mid a \iff \exists u \in R^\times \text{ mit } a = u \cdot b \iff (a) = (b)$$

Dies überlegen wir uns in Übung 3.16.

Definition 3.7.3 *1) Zwei Elemente $a, b \in R$ heißen **assoziiert**, wenn $u \in R^\times$ mit $a = u \cdot b$. Wir schreiben dann $a \sim b$. Dies ist eine Äquivalenzrelation.*

*2) Ein Element $q \in R$, $q \neq 0$, $q \notin R^\times$ heißt **irreduzibel**, wenn gilt*

$$q = a \cdot b \text{ mit } a, b \in R \Longrightarrow a \in R^\times \text{ oder } b \in R^\times$$

*3) Ein Element $p \in R$, $p \neq 0$, $p \notin R^\times$ heißt **Primelement**, wenn gilt*

$$p \mid a \cdot b \text{ mit } a, b \in R \Longrightarrow p \mid a \text{ oder } p \mid b$$

Die Beziehung zu den Begriffen Primideal und maximalen Ideal aus Abschnitt 3.4.2 stellt folgende Bemerkung her:

Bemerkung 3.7.4 *Für $q \in R$, $q \neq 0$, $q \notin R^\times$ gilt*

$$(q) \text{ ist ein maximales Ideal} \Longrightarrow q \text{ ist irreduzibel}$$
$$(q) \text{ ist ein Primideal} \iff q \text{ ist Primelement}$$

Ist q irreduzibel, dann muss (q) nicht maximal sein, betrachte zum Beispiel $q = xy - 1 \in \mathbb{C}[x, y]$, siehe auch Übung 3.15.

Beweis. Sei (q) maximal und $q = a \cdot b$ mit $a, b \notin R^\times$, dann $(q) \subsetneq (a)$, denn sonst $a = q \cdot b'$, also $1 = b \cdot b'$, ein Widerspruch.

Die zweite Äquivalenz folgt sofort aus $a \in (q) \Leftrightarrow q \mid a$. ■

Satz 3.7.5 *Ist R ein Integritätsring und $p \in R$, dann gilt*

$$p \text{ prim} \implies p \text{ irreduzibel}$$

Beweis. Sei p prim und $p = a \cdot b$, dann $p \mid a \cdot b$ also ohne Einschränkung $p \mid a$ und somit $a = p \cdot r$. Dann folgt $p = p \cdot r \cdot b$ also mit der Kürzungsregel in Integritätsringen $1 = r \cdot b$ und somit $b \in R^\times$. ■

Satz 3.7.6 *Ist R noethersch, dann gilt: Jedes $a \in R$, $a \neq 0$, $a \notin R^\times$ ist ein Produkt*

$$a = q_1 \cdot \ldots \cdot q_r$$

von irreduziblen Elementen.

Beweis. Ist a irreduzibel, ist nichts zu zeigen. Sei a reduzibel, etwa $a = a_1 b_1$ mit $a_1, b_1 \notin R^\times$. Wenn a_1 und b_1 irreduzibel sind, sind wir fertig. Ist ohne Einschränkung a_1 nicht irreduzibel, dann existieren $a_2, b_2 \notin R^\times$ mit $a_1 = a_2 b_2$. Somit erhalten wir eine Folge von Elementen a_i und eine Kette von Hauptidealen

$$(a) \subset (a_1) \subset (a_1) \subset \ldots$$

die stationär werden muss. ■

3.7.2 Zerlegung in Primelemente

Definition 3.7.7 *Ein Integritätsring heißt **faktoriell**, wenn jedes $a \in R$, $a \neq 0$, $a \notin R^\times$ ein Produkt*

$$a = p_1 \cdot \ldots \cdot p_r$$

von Primelementen p_i ist.

Beispiel 3.7.8 *1) $\mathbb{Z}$ ist faktoriell.*

2) Der Integritätsring

$$R = K[x, y, z, w] / (xy - zw)$$

ist nicht faktoriell, denn

$$\bar{x}\bar{y} = \bar{z}\bar{w}$$

Primelemente sind stets irreduzibel, in faktoriellen Ringen gilt auch die Umkehrung:

Satz 3.7.9 *Sei R faktoriell und $q \in R$, dann gilt*

$$q \text{ prim} \iff q \text{ irreduzibel}$$

Beweis. Ist q irreduzibel, dann ist q kein Produkt von mindestens zwei Nichteinheiten, also auch nicht von Primelementen. In der Darstellung $a = p_1 \cdot \ldots \cdot p_r$ muss also $r = 1$ und $q = p_1$ prim sein. ■

Satz 3.7.10 *Ein Integritätsring R ist faktoriell genau dann, wenn jedes $a \in R$, $a \neq 0$, $a \notin R^\times$ ein bis auf Permutation und Einheiten eindeutiges Produkt von irreduziblen Elementen ist.*

Das heißt, a lässt sich schreiben als

$$a = p_1 \cdot \ldots \cdot p_r$$

mit p_i irreduzibel, und sind

$$p_1 \cdot \ldots \cdot p_r = a = q_1 \cdot \ldots \cdot q_s$$

zwei solche Darstellungen, dann ist $r = s$ und es existiert eine Permutation $\sigma \in S_r$ sodass $p_i \sim q_{\sigma(i)}$.

Beweis. Sei R faktoriell, also gibt es eine Zerlegung in irreduzible (äquivalent prime) Elemente. Zur Eindeutigkeit: Seien

$$p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s$$

zwei solche Zerlegungen. Da p_1 prim ist, gilt $p_1 \mid q_j$ für ein j, ohne Einschränkung $j = 1$, also

$$q_1 = w \cdot p_1$$

und $w \in R^\times$ (wegen q_1 irreduzibel und p_1 prim).

Mit der Kürzungsregel folgt aus

$$p_1 \cdot \ldots \cdot p_r = w \cdot p_1 \cdot q_2 \cdot \ldots \cdot q_s$$

dass

$$p_2 \cdot \ldots \cdot p_r = (w \cdot q_2) \cdot \ldots \cdot q_s$$

Induktion nach r gibt die Behauptung.

Umgekehrt müssen wir nur zeigen, dass jedes irreduzible Element prim ist:

Sei q irreduzibel und $q \mid a \cdot b$. Ist a eine Einheit, dann $q \mid b$, ist $a = 0$ dann $q \mid a$.

Sind $a, b \notin R^\times$ und $a, b \neq 0$, dann

$$a \cdot b = q \cdot w$$

Nach Voraussetzung haben a, b, w Zerlegungen in irreduzible Elemente. Setzen wir diese ein, dann liefert die Eindeutigkeit, dass q bis auf eine Einheit einer der irreduziblen Faktoren von a oder b sein muss, also $q \mid a$ oder $q \mid b$. Somit ist q prim. ■

Da für noethersche Ringe eine Zerlegung in irreduzible Elemente existiert (Satz 3.7.6), folgt sofort:

Corollar 3.7.11 *Ein noetherscher Integritätsring ist genau dann faktoriell, wenn jedes irreduzible Element auch prim ist.*

Beispiel 3.7.12 *Der Ring*

$$R = \mathbb{Z}\left[\sqrt{-3}\right] = \left\{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\right\} \subset \mathbb{C}$$

ist nicht faktoriell, denn

$$4 = 2 \cdot 2 = \left(1 - \sqrt{-3}\right)\left(1 + \sqrt{-3}\right)$$

sind Zerlegungen in irreduzible (nicht prime) Elemente und die Faktoren 2 und $1 \pm \sqrt{-3}$ unterscheiden sich nicht nur um Einheiten:

- *Wir bestimmen die Einheitengruppe: Ist*

$$1 = \left(a + b\sqrt{-3}\right) \cdot \left(c + d\sqrt{-3}\right)$$

dann folgt

$$1 = \left(a^2 + 3b^2\right) \cdot \left(c^2 + 3d^2\right)$$

also $a, c = \pm 1$ *und* $b = d = 0$, *d.h.*

$$R^\times = \mathbb{Z}^\times = \{-1, +1\}$$

- *Wir zeigen, dass* 2 *und* $1 \pm \sqrt{-3}$ *irreduzibel sind: Angenommen*

$$2 = \left(a + b\sqrt{-3}\right) \cdot \left(c + d\sqrt{-3}\right)$$

oder

$$1 \pm \sqrt{-3} = \left(a + b\sqrt{-3}\right) \cdot \left(c + d\sqrt{-3}\right)$$

ist ein Produkt von Nichteinheiten $a + b\sqrt{-3}$. *Nehmen wir das Betragsquadrat, erhalten wir in jedem Fall*

$$4 = \left|a + b\sqrt{-3}\right|^2 \cdot \left|c + d\sqrt{-3}\right|^2 = \left(a^2 + 3b^2\right) \cdot \left(c^2 + 3d^2\right)$$

also $a^2 + 3b^2 = c^2 + 3d^2 = 2$, *was offenbar für* $a, b, c, d \in \mathbb{Z}$ *nicht möglich ist.*

Siehe auch Übungsaufgabe 3.17.

Wir bemerken noch folgenden Satz (auf den wir in Abschnitt 8.3 zurückkommen werden):

Satz 3.7.13 (Satz von Gauß) *Sei* R *ein Integritätsring. Dann gilt*

$$R \text{ faktoriell} \iff R[x] \text{ faktoriell}$$

Induktiv ist also jeder Polynomring $R[x_1, ..., x_n]$ faktoriell, wenn R faktoriell ist (insbesondere wenn R ein Körper ist).

3.7.3 Größter gemeinsamer Teiler

Analog zum Konzept des größten gemeinsamen Teilers in $\mathbb{Z}$ aus Abschnitt 1.3 formulieren wir allgemeiner:

Definition 3.7.14 *Sei* R *ein Integritätsring. Dann heißt* $d \in R$ *ein* ***größter gemeinsamer Teiler*** *(kurz* ***ggT*** *oder* ***gcd*** *für greatest common divisor) von* $a_1, ..., a_r \in R$, *wenn gilt*

1) $d \mid a_j \ \forall j = 1, ..., r$, *d.h.* d *ist ein Teiler von allen* a_j, *und*

2) ist $\tilde{d} \in R$ *ein Teiler aller* a_j, *d.h.* $\tilde{d} \mid a_j \ \forall j = 1, ..., r$, *dann gilt* $\tilde{d} \mid d$.

Bezeichne mit $\mathrm{ggT}(a_1, ..., a_r)$ *die Menge aller ggT von* $a_1, ..., a_r$. *Ist* d *ein ggT von* $a_1, ..., a_r$, *dann gilt*

$$\mathrm{ggT}(a_1, ..., a_r) = \{u \cdot d \mid u \in R^\times\}$$

Wir schreiben kurz

$$\mathrm{ggT}(a_1, ..., a_r) = d$$

das heißt d *repräsentiert alle Elemente von* $\mathrm{ggT}(a_1, ..., a_r)$ *bis auf Assoziiertheit.*

Beweis. Sind $d_1, d_2 \in \mathrm{ggT}(a_1, ..., a_r)$, dann $d_1 \mid d_2$ und $d_2 \mid d_1$, nach Lemma 3.7.2 sind d_1 und d_2 also assoziiert. Ist umgekehrt $d_1 \in \mathrm{ggT}(a_1, ..., a_r)$ und $d_2 = u \cdot d_1$ mit $u \in R^\times$, dann gilt auch $d_2 \mid a_j \ \forall j$ und haben wir $\tilde{d} \mid a_j \ \forall j$, dann nach Voraussetzung $\tilde{d} \mid d_1$ also auch $\tilde{d} \mid d_2$. ■

Beispiel 3.7.15 *Für* $\mathbb{Z}$ *ist* $\mathbb{Z}^\times = \{+1, -1\}$ *also*

$$\mathrm{ggT}(6, 15) = \{-3, 3\} = 3$$

Durch die Zusatzbedingung $\mathrm{ggT} > 0$ *ist der ggT eindeutig bestimmt.*

Analog geht man für das kleinste gemeinsame Vielfache vor:

Definition 3.7.16 *Weiter heißt* $m \in R$ ***kleinstes gemeinsames Vielfaches*** *(kurz* ***kgV*** *oder* ***lcm*** *für least common multiple) von* $a_1, ..., a_r \in R$, *wenn gilt*

1) $a_j \mid m \ \forall j = 1, ..., r$, *d.h.* m *ist ein Vielfaches aller* a_j, *und*

2) ist $\tilde{m} \in R$ *ein Vielfaches aller* a_j, *d.h.* $a_j \mid \tilde{m} \ \forall j = 1, ..., r$, *dann gilt* $m \mid \tilde{m}$.

Bezeichne mit $\mathrm{kgV}(a_1, ..., a_r)$ *die Menge aller kgV von* $a_1, ..., a_r$. *Ist* m *ein kgV von* $a_1, ..., a_r$, *dann gilt*

$$\mathrm{kgV}(a_1, ..., a_r) = \{u \cdot m \mid u \in R^\times\}$$

Wir schreiben kurz

$$\mathrm{kgV}(a_1, ..., a_r) = m$$

Definition 3.7.17 $a_1, ..., a_r \in R$ *heißen* ***teilerfremd****, wenn*

$$\mathrm{ggT}(a_1, ..., a_r) = 1$$

Satz 3.7.18 *Sei* R *faktoriell. Dann gibt es einen ggT und kgV von* $a_1, ..., a_r \in R$*: Sind*

$$a_j = u_j \cdot \prod_{i=1}^{s} p_i^{r_{ji}}$$

mit paarweise nicht-assoziierten Primelementen $p_1, ..., p_s$ *und* $r_{ji} \geq 0$ *und* $u_j \in R^\times$, *dann ist*

$$\mathrm{ggT}(a_1, ..., a_r) = \prod_{i=1}^{s} p_i^{\min_j\{r_{ji}\}}$$
$$\mathrm{kgV}(a_1, ..., a_r) = \prod_{i=1}^{s} p_i^{\max_j\{r_{ji}\}}$$

Sind $a, b \in R$ und schreiben wir

$$\begin{aligned}\mathrm{ggT}(a,b) \cdot \mathrm{kgV}(a,b) &:= \{d \cdot m \mid d \in \mathrm{ggT}(a,b),\ m \in \mathrm{kgV}(a,b)\} \\ &= \{u \cdot a \cdot b \mid u \in R^\times\}\end{aligned}$$

dann gilt mit obiger Notation

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

Das heißt aber nur, ist $d \in \mathrm{ggT}(a,b)$ und $m \in \mathrm{kgV}(a,b)$, dann sind $d \cdot m$ und $a \cdot b$ assoziiert

$$d \cdot m \sim a \cdot b$$

äquivalent, es gibt $d \in \mathrm{ggT}(a,b)$ und $m \in \mathrm{kgV}(a,b)$ mit

$$d \cdot m = a \cdot b$$

3.8 Hauptidealringe

Definition 3.8.1 *Sei R ein kommutativer Ring mit 1. Ein Ideal $I \subset R$, das von einem einzigen Element $a \in R$ erzeugt wird, d.h. von der Gestalt*

$$I = (a)$$

*heißt **Hauptideal**. Ein Integritätsring R, in dem jedes Ideal ein Hauptideal ist, heißt **Hauptidealring**.*

Da ein Ideal, das von einem einzigen Element erzeugt wird, insbesondere endlich erzeugt ist, gilt:

Satz 3.8.2 *Jeder Hauptidealring ist noethersch.*

Primelemente sind stets irreduzibel. In Hauptidealringen ist auch die Umkehrung richtig:

Satz 3.8.3 *In einem Hauptidealring gilt*

$$p \text{ irreduzibel} \Longrightarrow p \text{ prim}$$

Mit Satz 3.8.2 und 3.7.11 folgt daraus sofort:

Corollar 3.8.4 *Hauptidealringe sind faktoriell.*

Beweis. Wir zeigen Satz 3.8.3: Sei p irreduzibel und $p \mid ab$. Es ist $(p) \subset (p,a)$ und $(p) \subset (p,b)$. Es können nicht (p,a) und (p,b) beide gleich (1) sein, denn sonst gäbe es r_i, s_i mit

$$r_1 a + s_1 p = 1 = r_2 b + s_2 p$$

also

$$1 = (r_1 a + s_1 p) \cdot (r_2 b + s_2 p) = r_1 r_2 ab + r_1 a s_2 p + s_1 r_2 bp + s_1 s_2 p^2 \in (p)$$

Somit ist ohne Einschränkung $(p,a) = (d) \subsetneq R$ mit $d \notin R^\times$, also $p = cd$ und $a = ed$. Da p irreduzibel ist, folgt $c \in R^\times$ und somit $a = ec^{-1}p \in (p)$, d.h. $p \mid a$. ∎

Satz 3.8.5 *Sei R ein Hauptidealring und $a_1, \ldots, a_r \in R$. Dann gilt:*

1) *Das von Elementen $a_1, ..., a_r$ erzeugte Ideal wird schon vom größten gemeinsamen Teiler erzeugt, d.h.*

$$(a_1, ..., a_r) = (\mathrm{ggT}\,(a_1, ..., a_r))$$

Insbesondere lässt sich der ggT darstellen als

$$\mathrm{ggT}\,(a_1, ..., a_r) = x_1a_1 + ... + x_ra_r$$

mit $x_i \in R$.

2) *Der Durchschnitt der von $a_1, ..., a_r$ erzeugten Hauptideale wird vom kleinsten gemeinsamen Vielfachen erzeugt, d.h.*

$$(a_1) \cap ... \cap (a_r) = (\mathrm{kgV}\,(a_1, ..., a_r))$$

Wir bemerken: Die Ideale $(\mathrm{ggT}\,(a_1, ..., a_r))$ und $(\mathrm{kgV}\,(a_1, ..., a_r))$ sind wohldefiniert, denn nach Lemma 3.7.2 gilt $a \sim b$ genau dann, wenn $(a) = (b)$.

Beweis. Wir zeigen Satz 3.8.5:

1) Da R ein Hauptidealring ist, gibt es ein $d \in R$ mit

$$(a_1, ..., a_r) = (d) = \{v \in R \mid d \text{ teilt } v\}$$

also $d \mid a_i$. Weiter gibt es $x_i \in R$ mit

$$d = x_1a_1 + ... + x_ra_r$$

Somit ist jeder Teiler von allen a_i schon ein Teiler von d, also

$$d = \mathrm{ggT}\,(a_1, ..., a_r)$$

2) Da R ein Hauptidealring ist, gibt es ein $m \in R$ mit

$$(a_1) \cap ... \cap (a_r) = (m)$$

Somit $m \in (a_i)$ d.h. $a_i \mid m \ \forall i$. Gilt $a_i \mid \tilde{m} \ \forall i$ d.h. $\tilde{m} \in (a_i)$ $\forall i$ also

$$\tilde{m} \in (a_1) \cap ... \cap (a_r) = (m)$$

dann $m \mid \tilde{m}$, also

$$m = \mathrm{kgV}\,(a_1, ..., a_r)$$

■

Beispiel 3.8.6 *1) Der Ring der ganzen Zahlen $\mathbb{Z}$ ist ein Hauptidealring, denn jedes Ideal hat die Form*

$$n\mathbb{Z} = (n)$$

Wir erinnern uns an Beispiel 2.3.19, wo wir schon für die abelschen Gruppen

$$(n, m) = m\mathbb{Z} + n\mathbb{Z} = (\mathrm{ggT}\,(n, m))$$

gezeigt hatten. Beispielsweise ist

$$(6, 10) = (\mathrm{ggT}\,(6, 10)) = (2)$$

Eine Darstellung

$$2 = 2 \cdot 6 + (-1) \cdot 10$$

wie in Satz 3.8.5 erhalten wir mit dem erweiterten euklidischen Algorithmus (siehe auch Beispiel 1.3.3).

Weiter ist

$$\begin{aligned}(6) \cap (10) &= \{\textit{gemeinsame Vielfache von } 6 \textit{ und } 10\} \\ &= (\mathrm{kgV}\,(6, 10)) = (30)\end{aligned}$$

(was wir schon in Beispiel 2.3.19 für die abelschen Gruppen gezeigt haben).

2) Sei K ein Körper. Der Polynomring in (mindestens) 2 Variablen $K[x, y]$ ist kein Hauptidealring, denn das Ideal (x, y) lässt sich nicht von einem einzigen Element erzeugen. Siehe auch Übung 3.19. Nach dem Satz von Gauß 3.7.13 ist $K[x, y]$ faktoriell, es existiert also der $\mathrm{ggT}\,(x, y)$, jedoch gilt

$$(x, y) \subsetneq (\mathrm{ggT}\,(x, y)) = (1) = K[x, y]$$

3) Dagegen ist der Polynomring $K[x]$ in einer Variablen über einem Körper K ein Hauptidealring, wie wir auch mit dem Euklidischen Algorithmus sehen werden.

In Hauptidealringen gilt auch die Umkehrung von Bemerkung 3.7.4:

Bemerkung 3.8.7 *Ist R ein Hauptidealring und $q \in R$, $q \notin R^\times$, $q \neq 0$, dann*

$$(q) \text{ ist maximales Ideal} \iff q \text{ ist irreduzibel}$$

Beweis. Sei q irreduzibel und $(q) \subset (a) \subset R$. Dann gibt es ein $b \in R$ mit $q = a \cdot b$. Somit ist $a \in R^\times$ oder $b \in R^\times$, also $(a) = R$ oder $(q) = (q)$, das heißt (q) maximal. ■

Der Nachweis, dass zum Beispiel $\mathbb{Z}$ und $K[x]$ Hauptidealringe sind, erfolgt nach dem selben Schema. Wir abstrahieren daher den wesentlichen Teil:

3.9 Euklidische Ringe

Definition 3.9.1 *Ein **euklidischer Ring** ist ein Paar (R, d) aus einem Integritätsring R und einer Abbildung*

$$d : R \setminus \{0\} \longrightarrow \mathbb{N}_0$$

sodass für je zwei Elemente $a, b \in R \setminus \{0\}$ Elemente $g, r \in R$ existieren mit

1) $a = g \cdot b + r$ und

2) $r = 0$ oder $d(r) < d(b)$.

*Wir bezeichnen dies als **Division** von a durch b **mit Rest** r. Die Abbildung d heißt **euklidische Norm**.*

Beispiel 3.9.2 *1) Der Ring der ganzen Zahlen $\mathbb{Z}$ ist euklidisch mit der Betragsabbildung*

$$d(n) = |n|$$

und der üblichen Division mit Rest zur Bestimmung von g und r, siehe auch Beispiel 1.3.3.

2) Sei K ein Körper. Der Polynomring $R = K[x]$ in einer Variablen ein euklidischer Ring mit der Gradabbildung

$$d(f) = \deg(f)$$

und der üblichen Division mit Rest zur Berechnung von g und r.

Konkrete Beispiele:

Teilen wir $a = x^2 + \frac{1}{2}x + \frac{1}{2}$ durch $b = 2x - 1$ erhalten wir

$$\begin{aligned} x^2 + \tfrac{1}{2}x + \tfrac{1}{2} &= (\tfrac{1}{2}x) \cdot (2x-1) + \left(x + \tfrac{1}{2}\right) \\ &= \underbrace{(\tfrac{1}{2}x + \tfrac{1}{2})}_{g} \cdot (2x-1) + \underbrace{1}_{r} \end{aligned}$$

also $d(r) = 0 < 1 = d(b)$.

Teilen wir $a = x^n - 1$, $n \geq 1$ durch $b = x - 1$ erhalten wir

$$\begin{aligned} x^n - 1 &= x^{n-1} \cdot (x-1) + (x^{n-1} - 1) \\ &= (x^{n-1} + x^{n-2}) \cdot (x-1) + (x^{n-2} - 1) \\ &\quad \vdots \qquad\qquad\qquad\quad \vdots \\ &= \underbrace{(x^{n-1} + x^{n-2} + \ldots + x + 1)}_{g} \cdot (x-1) + \underbrace{0}_{r} \end{aligned}$$

3) $\mathbb{Z}[x]$ ist kein euklidischer Ring. Siehe auch Übungsaufgabe 3.19.

4) Der Ring der Gaußschen Zahlen

$$R = \mathbb{Z}[i] = \{a_1 + i \cdot a_2 \mid a_1, a_2 \in \mathbb{Z}\} \subset \mathbb{C}$$

ist euklidisch mit

$$\begin{aligned} d : R \setminus \{0\} &\longrightarrow \mathbb{Z}_{\geq 0} \\ d(a_1 + i \cdot a_2) &= |a_1 + i \cdot a_2|^2 = a_1^2 + a_2^2 \end{aligned}$$

Die Abbildung d setzt sich zum Betragsquadrat

$$|-|^2 : \quad \mathbb{C} \quad \longrightarrow \quad \mathbb{R}_{\geq 0}$$

fort, und es gilt $|z \cdot w|^2 = |z|^2 \cdot |w|^2$.

Seien $a, b \in \mathbb{Z}[i]$, $a, b \neq 0$. Wir müssen die Existenz von $g, r \in \mathbb{Z}[i]$ mit $a = g \cdot b + r$ und $|r|^2 < |b|^2$ zeigen:

Wir können den Quotienten $\frac{a}{b} \in \mathbb{C}$ durch Runden von Real- und Imaginärteil mit einer Gaußschen Zahl $g = n + i \cdot m \in \mathbb{Z}[i]$ approximieren, sodass für die Differenz

$$w = \frac{a}{b} - g \in \mathbb{C}$$

gilt

$$|\mathrm{Re}\, w| \leq \tfrac{1}{2} \qquad |\mathrm{Im}\, w| \leq \tfrac{1}{2}$$

Somit

$$|w|^2 \leq \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 = \frac{1}{2}$$

also erfüllt der Rest

$$r = a - bg = b \cdot w$$

dass

$$|r|^2 \leq \frac{1}{2}|b|^2 < |b|^2$$

Konkretes Beispiel: Wir teilen $-1+12i$ durch $3+4i$ in $\mathbb{Z}[i]$:

$$\frac{-1+12i}{3+4i} = \frac{(-1+12i)(3-4i)}{25} = \frac{9}{5} + \frac{8}{5}i$$

Mit

$$g = 2 + 2i$$

gilt

$$-1 + 12i = \overbrace{g \cdot (3+4i)}^{-2+14i} + \overbrace{(1-2i)}^{r}$$

und der Rest hat kleinere Norm als der Divisor:

$$d(1-2i) = 5 < 25 = d(3+4i)$$

Satz 3.9.3 *Euklidische Ringe sind Hauptidealringe.*

Beweis. Sei (R, d) ein euklidischer Ring und $I \subset R$ ein Ideal. Das Ideal $I = (0)$ ist ein Hauptideal. Sonst betrachten wir $b \in I \setminus \{0\}$ mit $d(b)$ minimal.

Sei $a \in I$ beliebig und $a = g \cdot b + r$ mit $r = 0$ oder $d(r) < d(b)$. Da mit a und b auch $r \in I$ ist, muss $r = 0$ sein, denn sonst hätten wir ein Element kleinerer Norm gefunden. Also ist $a \in (b)$.

Damit folgt $I \subset (b) \subset I$. ■

Somit sind euklidische Ringe auch faktoriell und noethersch. Insbesondere gilt dies also für die ganzen Zahlen $\mathbb{Z}$ und den Polynomring in einer Variablen $K[x]$ und den Ring der Gaußschen Zahlen $\mathbb{Z}[i]$. Weitere Beispiele werden wir in Übungsaufgabe 3.24 sehen.

Bemerkung 3.9.4 *Der Ring* $\mathbb{Z}\left[\frac{1+\sqrt{-19}}{2}\right]$ *ist ein Hauptidealring, aber kein euklidischer Ring (ohne Beweis).*

In euklidischen Ringen kann man analog zu $\mathbb{Z}$ und $K[x]$ die Division mit Rest und den euklidischen Algorithmus zur Bestimmung des ggT durchführen. Somit hat man eine Methode, den ggT effizient zu berechnen, ohne wie in faktoriellen Ringen auf die (im Vergleich dazu ineffiziente) Faktorisierung in Primelemente zurückgreifen zu müssen.

Satz 3.9.5 (Euklidischer Algorithmus) *Sei* (R, d) *ein euklidischer Ring und* $a_1, a_2 \in R \setminus \{0\}$. *Dann terminiert die sukzessive Division mit Rest*

$$\begin{aligned}
a_1 &= q_1 a_2 + a_3 && d(a_3) < d(a_2) \\
&\vdots \\
a_j &= q_j a_{j+1} + a_{j+2} && d(a_{j+2}) < d(a_{j+1}) \\
&\vdots \\
a_{n-2} &= q_{n-2} a_{n-1} + a_n && d(a_n) < d(a_{n-1}) \\
a_{n-1} &= q_{n-1} a_n + 0 && a_{n+1} = 0
\end{aligned}$$

und

$$\mathrm{ggT}(a_1, a_2) = a_n$$

Rückwärtseinsetzen

$$\begin{aligned}
a_n &= a_{n-2} - q_{n-2} a_{n-1} \\
&\vdots \\
a_3 &= a_1 - q_1 a_2
\end{aligned}$$

liefert eine Darstellung

$$\mathrm{ggT}(a_1, a_2) = x \cdot a_1 + y \cdot a_2$$

mit $x, y \in R$.

Beweis. Der Beweis geht völlig analog zum Beweis für $\mathbb{Z}$. Alternativ kann man folgendermaßen vorgehen:

In jedem Schritt $j = 1, ..., n-1$ gilt

$$\begin{pmatrix} q_j & 1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} a_{j+1} \\ a_{j+2} \end{pmatrix} = \begin{pmatrix} a_j \\ a_{j+1} \end{pmatrix}$$

also mit

$$Q = \prod_{j=1}^{n-1} \begin{pmatrix} q_j & 1 \\ 1 & 0 \end{pmatrix}$$

und $a_{n+1} = 0$

$$Q \cdot \begin{pmatrix} a_n \\ 0 \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}$$

Somit

$$a_1, a_2 \in (a_n)$$

und, da Q wegen $\det Q = \pm 1$ in $R^{2\times 2}$ invertierbar ist, auch

$$a_n \in (a_1, a_2)$$

also

$$(a_n) = (a_1, a_2)$$

d.h. a_n ist ein größter gemeinsamer Teiler von a_1 und a_2. ■

Beispiel 3.9.6 *Wir bestimmen den größten gemeinsamen Teiler von*

$$f = x^4 + x^3 \quad \textit{und} \quad g = x^4 - 1$$

in $\mathbb{Q}[x]$ *mit dem euklidischen Algorithmus*

$$\begin{aligned} x^4 + x^3 &= 1 \cdot \left(x^4 - 1\right) + \left(x^3 + 1\right) \\ x^4 - 1 &= x \cdot \left(x^3 + 1\right) + (-x - 1) \\ x^3 + 1 &= \left(-x^2 + x - 1\right) \cdot (-x - 1) + 0 \end{aligned}$$

also

$$\mathrm{ggT}\,(f, g) = x + 1$$

und damit

$$\left(x^4 + x^3,\ x^4 - 1\right) = (x + 1)$$

Man beachte, dass im Polynomring $K[x]$ über einem Körper K der ggT nur eindeutig bis auf Einheiten

$$K[x]^\times = K^\times = K\setminus\{0\}$$

ist. Der ggT wird eindeutig, indem wir den Leitkoeffizienten festlegen als

$$\mathrm{LC}(\mathrm{ggT}(f,g)) = 1$$

Beispiel 3.9.7 *Wir bestimmen den ggT von $3+4i$ und $-1+12i$ in $\mathbb{Z}[i]$:*

In Beispiel 3.9.2 haben wir schon gesehen, dass die Divison mit Rest von $-1+12i$ durch $3+4i$

$$-1+12i = (2+2i)\cdot(3+4i)+(1-2i)$$

ergibt. Bei der nächsten Division im euklidischen Algorithmus

$$\frac{3+4i}{1-2i} = \frac{(3+4i)(1+2i)}{5} = \frac{-5+10i}{5} = -1+2i \in \mathbb{Z}[i]$$

bleibt kein Rest, und damit

$$\mathrm{ggT}(3+4i,\ -1+12i) = 1-2i$$

Der ggT ist nur eindeutig bis auf Einheiten $\mathbb{Z}[i]^\times = \{1,-1,i,-i\}$, also sind alle größten gemeinsamen Teiler

$$\mathrm{ggT}(3+4i,\ -1+12i) = \{1-2i,\ -1+2i,\ 2+i,\ -2-i\}$$

Siehe auch Übungsaufgabe 3.25.

3.10 Chinesischer Restsatz

Wir wollen nun das Lösen von simultanen Kongruenzen, das wir in Kapitel 1 in $\mathbb{Z}$ kennengelernt haben, allgemein für einen kommutativen Ring R mit 1 formulieren. Zunächst formulieren wir Teilerfremdheit für Ideale.

Definition 3.10.1 *Sind $I_1, I_2 \subset R$ Ideale, dann sind die* ***Summe***

$$I_1 + I_2 = \{a + b \mid a \in I_1, b \in I_2\}$$

der ***Durchschnitt***

$$I_1 \cap I_2 \subset R$$

und das ***Produkt***

$$I_1 \cdot I_2 = \{\textstyle\sum_{endlich} a_k b_k \mid a_k \in I_1, b_k \in I_2\}$$

wieder Ideale.

Zwei Ideale I_1 und I_2 heißen ***coprim****, wenn*

$$I_1 + I_2 = (1)$$

Beispiel 3.10.2 *Seien $n, m \in R$.*

1) Für die Summe von Hauptidealen gilt

$$(n) + (m) = (n, m)$$

insbesondere ist in einem noetherschen Ring jedes Ideal eine endliche Summe von Hauptidealen.

2) Für das Produkt von Hauptidealen gilt

$$(n) \cdot (m) = (n \cdot m)$$

3) In einem Hauptidealring R (zum Beispiel $R = \mathbb{Z}$ oder $R = K[x]$) gilt

$$\begin{aligned} (n) \text{ und } (m) \text{ coprim} &\iff \mathrm{ggT}(n, m) = 1 \\ &\iff \mathrm{kgV}(n, m) = n \cdot m \\ &\iff \underbrace{(n) \cdot (m)}_{(n \cdot m)} = \underbrace{(n) \cap (m)}_{(\mathrm{kgV}(n,m))} \end{aligned}$$

das heißt genau dann, wenn n und m teilerfremd sind.

Beweis.

1) klar.

2) Für Hauptideale $(n), (m) \subset R$ gilt

$$(n)\cdot(m) = \{\sum_{\text{endlich}} s_k \cdot n \cdot t_k \cdot m\} = \{(\sum_{\text{endlich}} s_k \cdot t_k) \cdot n \cdot m\} = (n \cdot m)$$

3) Nach Satz 3.8.5 ist

$$(n) + (m) = (n, m) = (\text{ggT}(n, m))$$
$$(n) \cap (m) = (\text{kgV}(n, m))$$

■

Satz 3.10.3 (Chinesischer Restsatz) *Sei R ein kommutativer Ring mit 1 und $I_1, ..., I_n$ paarweise coprime Ideale. Dann ist der Ringhomomorphismus*

$$\begin{array}{rccc} \varphi: & R & \longrightarrow & R/I_1 \times ... \times R/I_n \\ & r & \longmapsto & (r + I_1, ..., r + I_n) \end{array}$$

surjektiv und hat Kern

$$\ker \varphi = I_1 \cap ... \cap I_n = I_1 \cdot ... \cdot I_n$$

also mit dem Homomorphiesatz 3.3.4

$$R/(I_1 \cap ... \cap I_n) \cong R/I_1 \times ... \times R/I_n$$

Beweis.

1) Seien $r_i + I_i \in R/I_i$. Wir müssen ein $r \in R$ konstruieren, sodass

$$r + I_i = r_i + I_i$$

für $i = 1, ..., n$ gilt. Nach Voraussetzung existieren Elemente $a_{ij} \in I_i$ und $b_{ij} \in I_j$ mit

$$a_{ij} + b_{ij} = 1$$

Wir betrachten

$$s_j = \prod_{i \neq j} a_{ij} = \prod_{i \neq j} (1 - b_{ij})$$

Dann gilt $s_j \in I_i$ für $i \neq j$ und $s_j \in 1 + I_j$. Wir setzen nun

$$r = \sum_{j=1}^{n} r_j s_j$$

Es gilt dann

$$\begin{aligned} r + I_i &= r_i s_i + I_i = (r_i + I_i)(s_i + I_i) \\ &= (r_i + I_i)(1 + I_i) = r_i + I_i \ \forall i \end{aligned}$$

2) Klar ist

$$\ker \varphi = I_1 \cap \ldots \cap I_n$$

Bleibt

$$I_1 \cap \ldots \cap I_n = I_1 \cdot \ldots \cdot I_n$$

zu zeigen. Die Inklusion $\supset$ ist klar.

Wir zeigen die andere Inklusion mit Induktion nach n:

Sei $n = 2$ und $a_{12} \in I_1, b_{12} \in I_2$ mit

$$a_{12} + b_{12} = 1$$

Für $a \in I_1 \cap I_2$ gilt daher

$$a \cdot 1 = aa_{12} + ab_{12} \in I_1 \cdot I_2$$

Also

$$I_1 \cdot I_2 = I_1 \cap I_2$$

Sei nun $n \geqslant 2$ und sei

$$I_1 \cdot \ldots \cdot I_{n-1} = I_1 \cap \ldots \cap I_{n-1}$$

schon gezeigt. Nach Voraussetzung gibt es $a_{in} \in I_i$ und $b_{in} \in I_n$ mit

$$a_{in} + b_{in} = 1$$

also

$$1 = \prod_{i=1}^{n-1} (a_{in} + b_{in}) \in I_1 \cdot \ldots \cdot I_{n-1} + I_n$$

d.h. die Ideale $I_1 \cdot \ldots \cdot I_{n-1}$ und I_n sind coprim und der Fall $n = 2$ lässt sich anwenden. Somit folgt

$$I_1 \cdot \ldots \cdot I_{n-1} \cdot I_n = (I_1 \cdot \ldots \cdot I_{n-1}) \cap I_n = I_1 \cap \ldots \cap I_{n-1} \cap I_n$$

mit der Induktionsvoraussetzung.

■

Als Corollar für den Fall $R = \mathbb{Z}$ erhalten wir wieder Satz 1.4.1:

Corollar 3.10.4 (Chinesischer Restsatz über $\mathbb{Z}$) *Sind $n_1, ..., n_t \in \mathbb{Z}_{>0}$ teilerfremd, dann gilt*

$$\mathbb{Z}/(n_1 \cdot ... \cdot n_t) \cong \mathbb{Z}/(n_1) \times ... \times \mathbb{Z}/(n_t)$$

das heißt, für $a_1, ..., a_t \in \mathbb{Z}$ ist die simultane Kongruenz

$$\begin{aligned} x &\equiv a_1 \bmod n_1 \\ &\vdots \\ x &\equiv a_t \bmod n_t \end{aligned}$$

lösbar, und die Lösung ist eindeutig modulo $n_1 \cdot ... \cdot n_t$.

Beweis. Die Ideale $I_j = (n_j) \subset \mathbb{Z}$ sind nach Beispiel 3.10.2 coprim und

$$I_1 \cap ... \cap I_t = I_1 \cdot ... \cdot I_t = (n_1 \cdot ... \cdot n_t)$$

■

Bemerkung 3.10.5 *Der Rechenaufwand der Multiplikation in $\mathbb{Z}$ steigt stärker als linear mit der Größe der Zahlen. Deshalb zerlegt man mit dem Chinesischen Restsatz das Problem in kleinere: Zum Rechnen mit Zahlen $z \in \mathbb{Z}$ mit $|z| < C$ wählt man ein $n = n_1 \cdot ... \cdot n_r > 2C$ mit n_i paarweise teilerfremd und alle n_i etwa gleich groß und rechnet in*

$$\mathbb{Z}/(n_1) \times ... \times \mathbb{Z}/(n_r) \cong \mathbb{Z}/(n)$$

ersetzt also eine Operation der Bitlänge N durch r Operationen der Bitlänge $\frac{N}{r}$ (die außerdem parallel durchführbar sind).

Neben dem Fall $R = \mathbb{Z}$ kann man den Chinesischen Restsatz z.B. auch für den Polynomring $R = K[x]$ anwenden, zunächst ein Beispiel dazu:

Beispiel 3.10.6 *Wir bestimmen die Lösungsmenge $L \subset \mathbb{Q}[x]$ der simultanen Kongruenzen*

$$\begin{aligned} f &\equiv 3 \bmod (x+1) \\ f &\equiv 2 + x \bmod \left(x^2 + x + 1\right) \end{aligned}$$

das heißt wir suchen alle Polynome f, sodass $f-3$ ein Vielfaches von $x+1$ und $f-(2+x)$ ein Vielfaches von x^2+x+1 ist. Der Chinesische Restsatz gibt

$$\mathbb{Q}[x]/\left(x^3+2x^2+2x+1\right) \cong \mathbb{Q}[x]/(x+1) \times \mathbb{Q}[x]/\left(x^2+x+1\right)$$

denn $x+1$ und x^2+x+1 sind mit dem Euklidischen Algorithmus teilerfremd:

$$\mathrm{ggT}\,(x+1, x^2+x+1) = 1 = \qquad (-x)\cdot(x+1) \;+\; 1\cdot(x^2+x+1)$$

Weiter ist $$-x^3+x+3 = (2+x)\cdot(-x)\cdot(x+1) \;+\; 3\cdot 1\cdot(x^2+x+1)$$

nach dem Beweis des Chinesischen Restsatzes eine Lösung der simultanen Kongruenzen (überprüfen Sie dies nochmals analog zur Formel für $\mathbb{Z}$ aus Kapitel 1) und

$$\begin{aligned} L &= -x^3+x+3 \quad + \quad (x^3+2x^2+2x+1) \\ &= 2x^2+3x+4 \quad + \quad (x^3+2x^2+2x+1) \end{aligned}$$

mit der eindeutigen Lösung $2x^2+3x+4$ von Grad <3. Oder anders ausgedrückt

$$L = \overline{2x^2+3x+4} \in \mathbb{Q}[x]/\left(x^3+2x^2+2x+1\right)$$

ist unter obigem Isomorphismus das eindeutige Urbild von

$$\left(\overline{3},\ \overline{2+x}\right) \in \mathbb{Q}[x]/(x+1) \;\times\; \mathbb{Q}[x]/\left(x^2+x+1\right)$$

Siehe auch Übung 3.29. Eine zentrale Anwendung des Chinesischen Restsatzes ist die Interpolation durch Polynome:

Satz 3.10.7 (Lagrange-Interpolation) *Sei K ein Körper. Sind $t_1, \ldots, t_k \in K$ paarweise verschiedene Stützstellen und $c_1, \ldots, c_k \in K$, dann gibt es genau ein Polynom $f \in K[x]$ mit $\deg f < k$ und*

$$f(t_i) = c_i \;\; \forall i$$

Beweis. Es gilt

$$(x-t_i)+(x-t_j) = (t_i-t_j) = (1)$$

Somit liefert der Chinesische Restsatz

$$K[x]/\left(\textstyle\prod_{i=1}^{k}(x-t_i)\right) \cong K[x]/(x-t_1) \;\times\ldots\times\; K[x]/(x-t_k) \cong K^k$$

■

Bemerkung 3.10.8 *Mit*

$$f_i = \prod_{\substack{j=1 \\ j\neq i}}^{k} \frac{x - t_j}{t_i - t_j}$$

ist

$$f_i \equiv 1 \bmod (x - t_i)$$
$$f_i \equiv 0 \bmod (x - t_j)$$

also

$$f = \sum_{i=1}^{k} c_i f_i$$

Allgemeiner zeigen wir in Übungsaufgabe 3.30:

Corollar 3.10.9 (Hermite-Interpolation) *Seien $t_1, ..., t_r \in \mathbb{R}$ paarweise verschieden und $m_1, ..., m_r \in \mathbb{N}$ mit $\sum_{j=1}^{r} m_j = d + 1$. Dann gibt es für alle $b_{1,0}, ..., b_{1,m_1-1}, ..., b_{r,0}, ..., b_{r,m_r-1} \in \mathbb{R}$ genau ein $f \in \mathbb{R}[x]_{\leq d}$ mit*

$$f^{(j)}(a_i) = b_{i,j}$$

für alle $j = 0, ..., m_i - 1$, $i = 1, ..., r$.

3.11 Übungsaufgaben

Übung 3.1 *Sei R ein Ring. Zeigen Sie durch Verwendung der Ringaxiome, dass für alle $x, y \in R$ gilt*

$$0x = x0 = 0$$
$$(-x)\, y = x\, (-y) = -xy$$
$$(-x)\, (-y) = xy$$

Übung 3.2 *Stellen Sie die Verknüpfungstafeln der Multiplikation und Addition des Rings $\mathbb{Z}/10\mathbb{Z}$ auf. Welche Elemente von $\mathbb{Z}/10\mathbb{Z}$ sind Einheiten und welche Nullteiler? Geben Sie auch die Gruppentafel der Einheitengruppe $(\mathbb{Z}/10\mathbb{Z})^\times$ an.*

Können Sie ein Kriterium formulieren, wann ein Element von $\mathbb{Z}/n\mathbb{Z}$ eine Einheit oder ein Nullteiler ist?

Übung 3.3 *Geben Sie dem äußeren direkten Produkt*

$$\prod_{\alpha\in I} R_\alpha = \left\{ f \mid f : I \to \bigcup_{\alpha\in I} R_\alpha \text{ mit } f(\alpha) \in R_\alpha \ \forall \alpha \right\}$$

wobei $I \neq \varnothing$ eine Indexmenge und $(R_\alpha)_{\alpha\in I}$ eine Familie von Ringen ist, eine Ringstruktur.

Zeigen Sie, dass $\mathrm{Abb}(X, R)$ *ein Sonderfall ist (deshalb schreibt man auch* $\mathrm{Abb}(X, R) = R^X$*).*

Übung 3.4 *Sei R ein kommutativer Ring mit* 1 *und $I \subset R$ ein Ideal. Zeigen Sie: $I = R$ genau dann, wenn $I \cap R^\times \neq \varnothing$.*

Übung 3.5 *Zeigen Sie:*

1) *Jeder Integritätsring mit endlich vielen Elementen ist ein Körper.*

2) *In einem endlichen Ring ist jedes Element entweder eine Einheit oder ein Nullteiler.*

Übung 3.6 *Wir bestimmen die Einheitengruppe $R^\times$ von $R = \mathbb{Z}\left[\sqrt{2}\right]$. Zeigen Sie dazu:*

1) $\pm 1 \in R^\times$

2) $\pm\left(1 \pm \sqrt{2}\right) \in R^\times$

3) *Ist $a + b\sqrt{2} \in R^\times$, dann gilt $a^2 - 2b^2 = \pm 1$*

4) *Ist $a + b\sqrt{2} \in R^\times$, dann gibt es $n_1, n_2 \in \mathbb{Z}_{\geq 0}$ mit*

$$a + b\sqrt{2} = \pm\left(1 + \sqrt{2}\right)^{n_1}\left(1 - \sqrt{2}\right)^{n_2}$$

Hinweis: Vollständige Induktion nach $|a|$.

5) *Folgern Sie, dass*

$$R^\times = \left\{ \pm\left(1 + \sqrt{2}\right)^n \mid n \in \mathbb{Z} \right\}$$

Übung 3.7 *Sei $\varphi : R \to S$ ein Ringhomomorphismus. Zeigen Sie:*

1) *Ist $J \subset S$ ein Ideal, dann ist $\varphi^{-1}(J)$ ein Ideal. Insbesondere ist $\ker \varphi$ ein Ideal.*

2) *Ist φ surjektiv und $I \subset R$ ein Ideal, dann ist $\varphi(I)$ ein Ideal.*

Geben Sie ein Gegenbeispiel, dass dies ohne die Voraussetzung φ surjektiv im Allgemeinen nicht richtig ist.

Übung 3.8 *Sei R ein Ring. Ein Element $x \in R$ heißt nilpotent, wenn es ein $n \in \mathbb{N}$ gibt mit $x^n = 0$. Zeigen Sie: Ist x nilpotent und R ein Ring mit 1, dann ist $1 - x$ eine Einheit in R.*

Übung 3.9 *Sei R ein kommutativer Ring. Zeigen Sie, dass $I = \{a \in R \mid \exists n \in \mathbb{N} \text{ mit } a^n = 0\}$ ein Ideal in R ist. Bestimmen Sie dieses für $R = \mathbb{Z}/(12)$.*

Übung 3.10 *Sei R ein Integritätsring und $S = R \setminus \{0\}$. Wir konstruieren den Ring von Brüchen*

$$Q(R) = \left\{ \frac{r}{s} \mid r \in R,\ s \in S \right\}$$

als $Q(R) = (R \times S) / \sim$ mit der Äquivalenzrelation

$$(r, s) \sim (r', s') \Leftrightarrow rs' - sr' = 0$$

und schreiben $\frac{r}{s} := [(r, s)]$. Addition und Multiplikation sind gegeben durch

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}$$
$$\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2}$$

Zeigen Sie:

1) *Addition und Multiplikation sind wohldefiniert und $Q(R)$ ist ein Körper.*

2) *$j : R \to Q(R)$, $r \mapsto \frac{r}{1}$ ist ein Monomorphismus.*

3) *Universelle Eigenschaft: Ist K ein Körper und $\varphi : R \to K$ ein Monomorphismus, dann existiert genau ein Monomorphismus $\tilde{\varphi} : Q(R) \to K$, sodass $\varphi = \tilde{\varphi} \circ j$.*

Übung 3.11 *In Verallgemeinerung von Aufgabe 3.10 hat man folgende Konstruktion: Sei R ein kommutativer Ring mit 1.*

1) *Eine Menge $S \subset R$ heißt multiplikativ abgeschlossen, wenn $1 \in S$ und $s_1, s_2 \in S \Rightarrow s_1 s_2 \in S$. Zeigen Sie:*

   (a) *Ist $f \in R$, dann ist $S = \{1, f, f^2, \ldots\}$ multiplikativ abgeschlossen.*

   (b) *Ist $p \subset R$ ein Primideal, dann ist $S = R \backslash P$ multiplikativ abgeschlossen.*

2) *Wir konstruieren den Ring von Brüchen*

$$R\left[S^{-1}\right] = \left\{ \frac{r}{s} \mid r \in R,\ s \in S \right\}$$

als $R[S^{-1}] = (R \times S) / \sim$ mit

$$(r, s) \sim (r', s') \Leftrightarrow \exists t \in S : t(rs' - sr') = 0$$

und schreiben $\frac{r}{s} := [(r, s)]$. Addition und Multiplikation sind gegeben durch

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}$$
$$\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} = \frac{r_1 r_2}{s_1 s_2}$$

Zeigen Sie:

   (a) *$R[S^{-1}]$ ist ein kommutativer Ring mit 1.*

   (b) *$j : R \to R[S^{-1}]$, $r \mapsto \frac{r}{1}$ ist ein Ringhomomorphismus.*

   (c) *Universelle Eigenschaft von $R[S^{-1}]$:*
   Ist $\varphi : R \to T$ ein Ringhomomorphismus, sodass jedes Element $s \in S$ auf eine Einheit $\varphi(s) \in T$ abgebildet wird, dann existiert genau ein Ringhomomorphismus $\tilde{\varphi} : R[S^{-1}] \to T$, sodass $\varphi = \tilde{\varphi} \circ j$.

   (d) *Ist R ein Integritätsring und $S = R \backslash \{0\}$, dann ist $Q(R) = R[S^{-1}]$ ein Körper (der Quotientenkörper von R). Jede Inklusion von R in einen Körper K setzt sich durch die universelle Eigenschaft auf $Q(R)$ fort.*

Übung 3.12 *Sei K ein Körper. Der formale Potenzreihenring $K[[x]]$ ist die Menge der Reihen $\sum_{i=0}^{\infty} f_i x^i$ mit $f_i \in K$ (ohne irgendeine Konvergenzbedingung). Eine solche Reihe ist durch die Koeffizientenfolge*

$$\begin{array}{rccc} f: & \mathbb{N}_0 & \to & K \\ & j & \mapsto & f_j \end{array}$$

eindeutig bestimmt. Somit steht $K[[x]]$ in Bijektion mit der Menge aller Abbildungen von $\mathbb{N}_0$ nach K. Die Ringstruktur auf

$$K[[x]] = K^{\mathbb{N}_0} = \{f \mid f : \mathbb{N}_0 \to K \text{ Abbildung}\}$$

ist in Termen der Koeffizienten $f(j) = f_j$ folgendermaßen gegeben: Komponentenweise Addition

$$\begin{array}{rccl} +: & K[[x]] \times K[[x]] & \to & K[[x]] \\ & (f,g) & \mapsto & f+g : \mathbb{N}_0 \to K \\ & & & (f+g)(j) = f(j) + g(j) \end{array}$$

und Multiplikation

$$\begin{array}{rccl} \cdot: & K[[x]] \times K[[x]] & \to & K[[x]] \\ & (f,g) & \mapsto & f \cdot g : \mathbb{N}_0 \to K \\ & & & (f \cdot g)(k) = \sum\limits_{i=0}^{k} f(i) g(k-i) \end{array}$$

Zeigen Sie:

1) *$K[[x]]$ ist ein kommutativer Ring mit 1.*

2) *$K[[x]]$ ist ein Integritätsring.*

3) $K[[x]]^{\times} = \left\{ \sum\limits_{i=0}^{\infty} f_i x^i \mid f_0 \neq 0 \right\}$.

Übung 3.13 *Zeigen Sie: Es gibt keinen Körper mit genau 6 Elementen.*

Gibt es einen Körper mit genau 4 Elementen?

Übung 3.14 *Bestimmen Sie alle Elemente von*

$$K = \mathbb{F}_2[x] / \left(x^2 + x + 1\right)$$

und die Additions- und Multiplikationstabelle von K. Zeigen Sie, dass K ein Körper ist. Welche Charakteristik hat K?

Übung 3.15 *1) Bestimmen Sie*

$$I = \{f \in \mathbb{Q}[x] \mid f(0) = 0\}$$

und zeigen Sie, dass $I \subset \mathbb{Q}[x]$ ein maximales Ideal ist.

2) Zeigen Sie, dass $I = (xy-1) \subset \mathbb{C}[x,y]$ ein Primideal ist.

3) Ist $\mathbb{F}_3[x]/(x^2+x+1)$ ein Integritätsring?

Übung 3.16 *Sei R ein Integritätsring. Zeigen Sie:*

1) Für $a,b,c \in R$, $c \neq 0$ folgt aus $ac = bc$, dass schon $a = b$.

2) Für alle $a \in R$ gilt $a \mid 0$ und $a \mid a$ und $1 \mid a$.

3) Seien $a,b,c \in R$. Gilt $c \mid b$ und $b \mid a$, dann $c \mid a$.

4) Ist $a \in R$ und $u \in R^\times$ und $a \mid u$, dann ist $a \in R^\times$.

5) Seien $a,b,d \in R$ mit $d \mid a$ und $d \mid b$. Dann gilt $d \mid (xa+yb)$ für alle $x,y \in R$.

6) Seien $a,b \in R$. Dann ist $(a) \subset (b) \iff b \mid a$.

7) Seien $a,b \in R$. Dann gilt

$$a \mid b \text{ und } b \mid a \iff \exists u \in R^\times \text{ mit } a = ub \iff (a) = (b)$$

Man sagt dann, a und b sind assoziiert. Dies ist eine Äquivalenzrelation.

Übung 3.17 *Sei*

$$R = \mathbb{Z}\left[\sqrt{-5}\right] = \left\{a + b\sqrt{-5} \mid a,b \in \mathbb{Z}\right\} \subset \mathbb{C}$$

1) Bestimmen Sie die Einheitengruppe $R^\times$.

2) Zeigen Sie, dass R nicht faktoriell ist.

3) Zeigen Sie, dass R noethersch ist.

Übung 3.18 *Sei $\mathbb{F}_q$ ein endlicher Körper mit q Elementen.*

1) *Zeigen Sie, dass es unendlich viele irreduzible Polynome in* $\mathbb{F}_q[x]$ *gibt, indem Sie Euklids Beweis für* $\mathbb{Z}$ *(Satz 1.2.4) auf den Polynomring* $\mathbb{F}_q[x]$ *übertragen. Lässt sich auch Eulers Beweis aus Übungsaufgabe 1.3 übertragen?*

2) *Bestimmen Sie alle normierten irreduziblen Polynome vom Grad* ≤ 4 *in* $\mathbb{F}_2[x]$.

Übung 3.19 *Sei* K *ein Körper.*

1) *Zeigen Sie: Das Ideal* $(x, y) \subset K[x, y]$ *ist kein Hauptideal.*

2) *Ist* $\mathbb{Z}[x]$ *ein Hauptidealring?*

Übung 3.20 *Sei* K *ein Körper. Zeigen Sie, dass der formale Potenzreihenring* $K[[x]]$ *ein Hauptidealring ist.*

Übung 3.21 *Sei*

$$R = \{f \in \mathbb{Q}[x] \mid f(0) \in \mathbb{Z}\}$$

Zeigen Sie:

1) R *ist ein Ring.*

2) *Jedes von zwei Elementen erzeugte Ideal von* R *ist ein Hauptideal.*

3) *Das Ideal*
$$I = \left(\frac{x}{2^n} \mid n \in \mathbb{N}\right) \subset R$$
ist kein Hauptideal.

4) *Jedes endlich erzeugte Ideal von* R *ist ein Hauptideal.*

5) R *ist nicht noethersch.*

Übung 3.22 *Sei* K *ein Körper und* $(a_1, ..., a_n) \in K^n$. *Zeigen Sie:*

$$(x_1 - a_1, ..., x_n - a_n) \subset K[x_1, ..., x_n]$$

ist ein maximales Ideal.

Übung 3.23 *Bestimmen Sie alle maximalen Ideale von* $\mathbb{R}[x]$.

Übung 3.24 *Zeigen Sie für* $n = -1, -2, 2, 3$, *dass* $R = \mathbb{Z}\left[\sqrt{n}\right]$ *zusammen mit*

$$\begin{array}{rccl} d: & R\backslash\{0\} & \to & \mathbb{N}_0 \\ & a+b\sqrt{n} & \mapsto & \left|\left(a+b\sqrt{n}\right)\left(a-b\sqrt{n}\right)\right| \end{array}$$

ein euklidischer Ring ist. Geben Sie ein Verfahren an, um die Division mit Rest durchzuführen.

Übung 3.25 *1) Finden Sie alle größten gemeinsamen Teiler von* $1+5i$ *und* $-1+5i$ *in* $\mathbb{Z}[i]$.

2) Bestimmen Sie jeweils einen Erzeuger der Ideale

$$(2-i, 2+i) \subset \mathbb{Z}[i] \qquad \left(11+8\sqrt{3}, 7+2\sqrt{3}\right) \subset \mathbb{Z}\left[\sqrt{3}\right]$$

Übung 3.26 *Schreiben Sie ein Maple Programm, das in* $R = \mathbb{Z}\left[\sqrt{n}\right]$, $n = -1, -2, 2, 3$ *die Division mit Rest und den Euklidischen Algorithmus zur Bestimmung des ggT durchführt.*

Übung 3.27 *Sei* p *eine Primzahl und* $\mathbb{F}_p$ *der endliche Körper mit* p *Elementen. Bestimmen Sie das Verschwindungsideal* $I(M) \subset \mathbb{F}_p[x]$ *von*

$$M = \mathbb{F}_p$$

Übung 3.28 *Seien* $(a_1, b_1), ..., (a_r, b_r)$ *paarweise verschiedene Punkte im* $\mathbb{R}^2$ *und* $c_1, ..., c_r \in \mathbb{R}$. *Zeigen Sie: Es existiert ein Polynom* $f \in \mathbb{R}[x, y]$, *das in den vorgegebenen Punkten die vorgegebenen Werte annimmt:*

$$f(a_j, b_j) = c_j \text{ für } j = 1, ..., r$$

Übung 3.29 *Bestimmen Sie die Menge* $L \subset \mathbb{R}[x]$ *aller Lösungen* f *der simultanen Kongruenzen*

$$f \equiv 2 + 3(x-1) \bmod (x-1)^2$$
$$f \equiv 1 + 2(x+1) \bmod (x+1)^2$$

Übung 3.30 *Seien $a_1, ..., a_r \in \mathbb{R}$ paarweise verschieden und $m_1, ..., m_r \in \mathbb{N}$ mit $\sum_{j=1}^{r} m_j = d + 1$. Zeigen Sie mit Hilfe des Chinesischen Restsatzes, dass es für alle*

$$b_{1,0}, ..., b_{1,m_1-1}, ..., b_{r,0}, ..., b_{r,m_r-1} \in \mathbb{R}$$

ein eindeutiges Polynom $f \in \mathbb{R}[x]_{\leq d}$ gibt mit

$$f^{(j)}(a_i) = b_{i,j}$$

für alle $j = 0, ..., m_i - 1$ und $i = 1, ..., r$.

Übung 3.31 *Sei $R = \mathbb{Z}[i]$ der Ring der Gaußschen Zahlen.*

1) *Zeigen Sie: Der Chinesische Restsatz gibt einen Isomorphismus*

$$\varphi : R/(15 - 5i) \longrightarrow R/(3 + 4i) \times R/(1 - 3i)$$

2) *Bestimmen Sie das Urbild $x \in R/(15 - 5i)$ von*

$$\left(\overline{1 + i}, \overline{2 + i}\right) \in R/(3 + 4i) \times R/(1 - 3i)$$

unter φ.

4

Moduln und der Elementarteilersatz

4.1 Übersicht

In diesem Abschnitt verallgemeinern wir den Gauß-Algorithmus zur Normalformbestimmung über Körpern auf beliebige Hauptidealringe. Aus der linearen Algebra wissen wir: Ist K ein Körper und $A \in K^{n\times m}$, dann gibt es Basiswechsel $T \in \mathrm{GL}(m, K)$ und $S \in \mathrm{GL}(n, K)$, die A in die Normalform

$$S \cdot A \cdot T = \left(\begin{array}{ccc|c} 1 & & & \\ & \ddots & & 0 \\ & & 1 & \\ \hline & 0 & & 0 \end{array}\right)$$

bringen (mit $\operatorname{rang}(A)$ Einsen auf der Diagonalen). Ersetzen wir K durch einen Hauptidealring R, können wir dies nicht mehr erwarten. Mit der Adjungierten-Formel für die Inverse ist eine Matrix $T \in R^{n\times n}$ invertierbar genau dann, wenn $\det(T)$ eine Einheit ist. Somit ist zum Beispiel $A = (2) \in \mathbb{Z}^{1\times 1}$ schon in Normalform, denn $\mathbb{Z}^\times = \{\pm 1\}$. Im Allgemeinen können wir erreichen, dass

$$S \cdot A \cdot T = D = \left(\begin{array}{ccc|c} d_1 & & & \\ & \ddots & & 0 \\ & & d_r & \\ \hline & 0 & & 0 \end{array}\right) \in R^{n\times m}$$

wobei jedes d_i ein Teiler von d_{i+1} ist. Die sogenannten Elementarteiler d_i sind eindeutig durch A bestimmt.

Das Kapitel baut sich wie folgt auf: Wir zeigen zunächst im Elementarteilersatz diese Aussage. Der Beweis gibt gleichzeitig einen rekursiven Algorithmus zur Bestimmung von S, T und D. Mit Hilfe der Normalform D zeigen wir dann verschiedene Strukturaussagen: Als Verallgemeinerung von Vektorräumen über einem Körper führen wir Moduln über einem Ring ein und beschreiben endlich erzeugte Moduln über Hauptidealringen, insbesondere endlich erzeugte abelsche Gruppen ($\mathbb{Z}$-Moduln), und die Jordansche Normalform.

4.2 Der Elementarteileralgorithmus

Bemerkung 4.2.1 *Eine Matrix $A \in R^{n\times n}$ ist invertierbar (d.h. $A \in \mathrm{GL}(n,R)$) genau dann, wenn ihre Determinante eine Einheit ist, d.h.*

$$\det(A) \in R^\times$$

Beweis. Ist $A\cdot A^{-1} = E$, dann $\det(A)\cdot\det(A^{-1}) = 1$. Umgekehrt: Falls $\det(A) \in R^\times$, dann ist

$$A^{-1} = \frac{A^{adj}}{\det(A)} \in R^{n\times n}$$

mit der adjungierten Matrix $A^{adj} = \left((-1)^{i+j}\det(A_{ji})\right)_{i,j} \in R^{n\times n}$, wobei A_{ji} durch Streichen der j-ten Zeile und i-ten Spalte von A entsteht. ∎

Satz 4.2.2 (Elementarteilersatz) *Sei R ein Hauptidealring und $A \in R^{n\times m}$ eine Matrix. Dann gibt es Basiswechsel $S \in \mathrm{GL}(n,R)$ und $T \in \mathrm{GL}(m,R)$ und ein $r \le \min(n,m)$ mit*

$$S\cdot A\cdot T = D = \left(\begin{array}{ccc|c} d_1 & & & \\ & \ddots & & 0 \\ & & d_r & \\ \hline & 0 & & 0 \end{array}\right) \in R^{n\times m}$$

und

$$d_1 \mid d_2, \quad d_2 \mid d_3 \quad \ldots \quad d_{r-1} \mid d_r \neq 0$$

Die d_i sind bis auf Assoziiertheit $\sim$ durch A eindeutig bestimmt und heißen ***Elementarteiler*** *von A, und D heißt die* ***Smith-Normalform*** *von A.*

Bemerkung 4.2.3 *Der Spezialfall für $R = K$ ein Körper ist aus der linearen Algebra als Gauß-Algorithmus bekannt:*

Ist $A = (a_{i,j}) \in K^{n\times m}$, dann gibt es Basiswechsel $T \in \mathrm{GL}(m, K)$ und $S \in \mathrm{GL}(n, K)$ in Quelle und Ziel, die A in die Normalform

$$S \cdot A \cdot T = \left(\begin{array}{ccc|c} 1 & & & \\ & \ddots & & 0 \\ & & 1 & \\ \hline & 0 & & 0 \end{array}\right)$$

bringen mit $r = \mathrm{rang}(A)$ Einsen auf der Diagonalen.

Dabei erhalten wir S und T als Produkt von Zeilen- bzw. Spaltenoperationen: Durch Permutation von Zeilen und Spalten können wir $a_{11} \neq 0$ annehmen (falls $A \neq 0$). Subtraktion des $\frac{a_{1,j}}{a_{1,1}}$-fachen der ersten Spalte von der j-ten Spalte (und analog für die Zeilen) bringt A in die Form

$$\left(\begin{array}{c|ccc} a_{1,1} & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & * & \\ 0 & & & \end{array}\right)$$

Schließlich multiplizieren wir die erste Spalte mit $\frac{1}{a_{1,1}}$. Mit Induktion folgt die Behauptung.

In einem Ring R ist es dagegen im Allgemeinen nicht möglich, $\frac{a_{1,j}}{a_{1,1}}$ zu bilden, da $a_{1,1}$ keine Einheit sein muss. Wir zeigen nun zunächst Satz 4.2.2 für den Fall, dass R ein euklidischer Ring ist. Hier können wir die Division $\frac{a_{1,j}}{a_{1,1}}$ durch Division mit Rest ersetzen. Der Beweis gibt einen Algorithmus zur Berechnung der Smith-Normalform.

Beweis. Sei (R, d) ein euklidischer Ring und $A \neq 0$.

1) Durch Zeilen- und Spaltenvertauschungen können wir annehmen, dass $a_{1,1} \neq 0$ und

$$d(a_{1,1}) \leq d(a_{i,j}) \text{ oder } a_{i,j} = 0$$

für alle $(i, j) \neq (1, 1)$.

2) Ist ein Eintrag $a_{1,j}$ der ersten Zeile (analog für die erste Spalte) nicht durch $a_{1,1}$ teilbar, dann schreibe $a_{1,j}$ mit Division mit Rest

$$a_{1,j} = q \cdot a_{1,1} + r$$

mit $d(r) < d(a_{1,1})$. Der Fall $r = 0$ tritt nicht auf, da nach Voraussetzung $a_{1,1} \nmid a_{1,j}$.

Nach Subtraktion des q-fachen der 1-ten Spalte von der j-ten Spalte erreichen wir also

$$d(a_{1,1}) > d(a_{1,j})$$

Gehe nun zurück zu Schritt (1). Dieser Prozess terminiert, da $d(a_{1,1})$ in jedem Durchlauf echt kleiner wird.

3) Sind alle Einträge der ersten Zeile und Spalte durch $a_{1,1}$ teilbar, dann können wir durch Addition von Vielfachen der ersten Spalte A in die Form

$$\left(\begin{array}{c|ccc} a_{1,1} & 0 & \cdots & 0 \\ \hline * & & * & \end{array}\right)$$

und durch Addition von Vielfachen der ersten Zeile auf die Form

$$\left(\begin{array}{c|ccc} a_{1,1} & 0 & \cdots & 0 \\ \hline 0 & & & \\ \vdots & & A' & \\ 0 & & & \end{array}\right)$$

bringen. Hat A' einen Eintrag $a_{i,j}$, der nicht durch $a_{1,1}$ teilbar ist, dann addieren wir die i-te Zeile zu der ersten Zeile und gehen zurück zu (2). Danach wird $d(a_{1,1})$ wieder echt kleiner.

4) Sind alle Einträge von A durch $a_{1,1}$ teilbar, dann auch die Einträge von A', da sie R-Linearkombinationen von Einträgen von A sind.

Mit Induktion nach $\min(n, m)$ folgt die Behauptung.

Für den Induktionsanfang ($n = 1$ oder $m = 1$) sind die Schritte (1) – (3) der euklidische Algorithmus auf den Einträgen. ■

Bevor wir den Fall R Hauptidealring und die Eindeutigkeit behandeln, erproben wir diesen Algorithmus an einem Beispiel:

Beispiel 4.2.4 *Wir bestimmen die Smith-Normalform von*

$$A = \begin{pmatrix} 6 & 9 & 6 \\ 6 & 6 & 7 \end{pmatrix} \in \mathbb{Z}^{2\times 3}$$

und gleichzeitig $S \in \mathbb{Z}^{2\times 2}$ und $T \in \mathbb{Z}^{3\times 3}$ durch simultanes Ausführen der Zeilen- bzw. Spaltenoperation auf der 2×2 bzw. 3×3 Einheitsmatrix. Division mit Rest (Schritt 2) gibt

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 6 & 3 & 6 \\ 6 & 0 & 7 \end{pmatrix} \quad \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Vertauschen (Schritt 1)

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 3 & 6 & 6 \\ 0 & 6 & 7 \end{pmatrix} \quad \begin{pmatrix} -1 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Reduktion der ersten Zeile und Spalte (Schritt 3)

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 3 & 0 & 0 \\ 0 & 6 & 7 \end{pmatrix} \quad \begin{pmatrix} -1 & 3 & 2 \\ 1 & -2 & -2 \\ 0 & 0 & 1 \end{pmatrix}$$

Da 7 nicht durch 3 teilbar ist, addieren wir die zweite zur ersten Zeile

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 3 & 6 & 7 \\ 0 & 6 & 7 \end{pmatrix} \quad \begin{pmatrix} -1 & 3 & 2 \\ 1 & -2 & -2 \\ 0 & 0 & 1 \end{pmatrix}$$

Division mit Rest (Schritt 2)

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 3 & 6 & 1 \\ 0 & 6 & 7 \end{pmatrix} \quad \begin{pmatrix} -1 & 3 & 4 \\ 1 & -2 & -4 \\ 0 & 0 & 1 \end{pmatrix}$$

Vertauschen (Schritt 1)

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 6 & 3 \\ 7 & 6 & 0 \end{pmatrix} \quad \begin{pmatrix} 4 & 3 & -1 \\ -4 & -2 & 1 \\ 1 & 0 & 0 \end{pmatrix}$$

Reduktion der ersten Zeile und Spalte (Schritt 3 und 4)

$$\begin{pmatrix} 1 & 1 \\ -7 & -6 \end{pmatrix} \quad \begin{pmatrix} 1 & 0 & 0 \\ 0 & -36 & -21 \end{pmatrix} \quad \begin{pmatrix} 4 & -21 & -13 \\ -4 & 22 & 13 \\ 1 & -6 & -3 \end{pmatrix}$$

Rekursives Anwenden des Algorithmus auf die durch Streichen (bzw. Ignorieren) der ersten Zeile und Spalte erhaltene Untermatrix, gibt

$$\begin{pmatrix} -36 & -21 \end{pmatrix} \mapsto \begin{pmatrix} -15 & -21 \end{pmatrix} \mapsto \begin{pmatrix} -15 & -6 \end{pmatrix} \mapsto \begin{pmatrix} -3 & -6 \end{pmatrix} \mapsto \begin{pmatrix} -3 & 0 \end{pmatrix}$$

(in diesem Fall ist dies genau der euklidische Algorithmus) und wir erhalten die Smith-Normalform

$$D = S \cdot A \cdot T$$

mit

$$S = \begin{pmatrix} 1 & 1 \\ -7 & -6 \end{pmatrix} \qquad D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & -3 & 0 \end{pmatrix} \qquad T = \begin{pmatrix} 4 & 2 & -9 \\ -4 & 1 & 2 \\ 1 & -3 & 6 \end{pmatrix}$$

Die Elementarteiler von A sind also

$$d_1 = 1 \qquad d_2 = 3$$

bis auf Multiplikation mit Einheiten $\mathbb{Z}^\times = \{1, -1\}$.

Wir beobachten hier eine Eigenheit des Smith-Normalform Algorithmus: Die Größe der Zwischenergebnisse kann im Verhältnis zu Input und Output stark ansteigen. Eine Fragestellung in der Informatik ist die Vermeidung dieses Problems. Man kann z.B. die Berechnung modulo Primzahlen durchführen und die Resultate mit dem Chinesischen Restsatz zu einem ganzzahligen Ergebnis "liften".

Ist R allgemeiner ein Hauptidealring, können wir im Beweis von Satz 4.2.2 analog vorgehen, verwenden aber statt des Euklidischen Algorithmus die folgende Bemerkung:

Bemerkung 4.2.5 *Sei* $A = (a_{1,1},\ a_{1,2}) \in R^{1\times 2}$ *und*

$$\mathrm{ggT}\,(a_{1,1}, a_{1,2}) = d = x \cdot a_{1,1} + y \cdot a_{1,2}$$

(für R *euklidisch finden wir eine solche Darstellung mit dem erweiterten euklidischen Algorithmus). Schreibe*

$$a_{1,1} = u \cdot d \qquad a_{1,2} = v \cdot d$$

mit $u, v \in R$*. Dann gilt mit*

$$T = \begin{pmatrix} x & -v \\ y & u \end{pmatrix} \in \mathrm{GL}\,(2, R)$$

dass

$$A \cdot T = (d,\ 0)$$

Wir bemerken noch, dass sogar $\det(T) = 1$*, d.h.* $T \in \mathrm{SL}\,(2, R)$*.*

Mit diesem Verfahren kann man (wie in Schritt (1) – (3) *des Elementarteileralgorithmus für euklidische Ringe) abwechselnd alle Einträge außer* $a_{1,1} \neq 0$ *in der ersten Zeile oder Spalte zu* 0 *machen. Dieser Prozess terminiert, da die Einträge* $a_{1,1}$ *eine aufsteigende Kette von Idealen bilden. Diese muss stationär werden, da Hauptidealringe noethersch sind.*

Bemerkung 4.2.6 *Da die Basiswechsel in dem Elementarteileralgorithmus alle Determinante* 1 *haben und Permutationsmatrizen Determinante* ± 1*, können wir in Satz 4.2.2 erreichen, dass* $T \in \mathrm{SL}\,(m, R)$ *und* $S \in \mathrm{SL}\,(n, R)$*.*

Dass $r \leq n$ und die Elementarteiler d_i bis auf Einheiten eindeutig bestimmt sind, folgt aus:

Satz 4.2.7 *Für die Elementarteiler* $d_1, \ldots, d_r$ *von* $A \in R^{n\times m}$ *in Satz 4.2.2 gilt für* $i \leq r$ *(bis auf Einheiten)*

$$d_1 \cdot \ldots \cdot d_i = \mathrm{ggT}\,(\det(A_{I,J}) \mid |I| = |J| = i) =: D_i$$

Für $i > r$ *sind alle* $\det(A_{I,J}) = 0$*.*

Hier bezeichnet für $I \subset \{1, \ldots, n\}$ *und* $J \subset \{1, \ldots, m\}$

$$A_{I,J} \in R^{|I|\times|J|}$$

die Untermatrix von A mit den Zeilen aus I und Spalten aus J. Die $\det(A_{I,J})$ *mit* $|I| = |J| = i$ *heißen* $i \times i$-***Minoren*** *von A.*

Man nennt D_i auch als den i-ten ***Determinantenteiler*** *von A.*

Insbesondere ist $d_1 = D_1$ der größte gemeinsame Teiler aller Einträge von A.

Beweis. Wir skizzieren den Beweis unter Verwendung folgender Ergebnisse aus der (multi-)linearen Algebra: Die Einträge der darstellenden Matrix der i-ten äußeren Potenz $\bigwedge^i A$ von A (bezüglich einer geeigneten Basis) sind genau die $i \times i$-Minoren von A. Ist weiter $S \in R^{n\times n}$, dann gilt

$$\left(\bigwedge^i S\right) \cdot \left(\bigwedge^i A\right) = \bigwedge^i (S \cdot A)$$

Ist $S \in \mathrm{GL}(n, R)$ invertierbar, dann folgt damit für den ggT der Einträge

$$\mathrm{ggT}\left(\bigwedge^i (S \cdot A)\right) = \mathrm{ggT}\left(\bigwedge^i A\right)$$

(bis auf Einheiten), denn jeder Eintrag von $\bigwedge^i (S \cdot A)$ ist eine Linearkombination der Einträge von $\bigwedge^i A$ und somit wird $\mathrm{ggT}\left(\bigwedge^i (S \cdot A)\right)$ von $\mathrm{ggT}\left(\bigwedge^i A\right)$ geteilt. Die Umkehrung folgt, da $A = S^{-1} \cdot (S \cdot A)$.

Analog geht man für einen Basiswechsel T in der Quelle vor.

Haben wir nun gemäß dem Elementarteilersatz

$$S \cdot A \cdot T = D = \left(\begin{array}{ccc|c} d_1 & & & \\ & \ddots & & 0 \\ & & d_r & \\ \hline & 0 & & 0 \end{array}\right)$$

dann gilt

$$\begin{aligned} \mathrm{ggT}\left(\bigwedge^i A\right) &= \mathrm{ggT}\left(\bigwedge^i D\right) \\ &= \mathrm{ggT}\left(d_{j_1} \cdot \ldots \cdot d_{j_i} \mid 1 \le j_1 < \ldots < j_i \le r\right) \\ &= d_1 \cdot \ldots \cdot d_i \end{aligned}$$

denn $d_j \mid d_k$ für $j \le k$. ■

Beispiel 4.2.8 *Wir bestimmen für*

$$A = \begin{pmatrix} 1 & 1 & 1 \\ -3 & 1 & 1 \\ 1 & -3 & 1 \\ 1 & 1 & -3 \end{pmatrix}$$

die Smith-Normalform:

$$A \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 4 \\ 0 & -4 & 0 \\ 0 & 0 & -4 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 4 \\ 0 & -4 & 0 \\ 0 & 0 & -4 \end{pmatrix}$$
$$\mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \\ 0 & 0 & -4 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \\ 0 & 0 & 0 \end{pmatrix} = D$$

Andererseits ist offenbar

$$D_1 = 1 = d_1$$

die 2×2*-Minoren sind* 0, ± 4 *oder* 8*, also*

$$D_2 = 4 = d_1 \cdot d_2$$

und die 3×3 *Minoren sind* ± 16*, also*

$$D_3 = 16 = d_1 \cdot d_2 \cdot d_3$$

Der Elementarteilersatz 4.2.2 beschreibt die Struktur von endlich erzeugten Moduln über Hauptidealringen:

4.3 Moduln und Präsentationen

Sei im Folgenden R ein (nicht notwendigerweise kommutativer) Ring.

Definition 4.3.1 *Ein* R*-(Links)-**Modul*** $(M, +, \cdot)$ *ist eine Menge* M *mit Abbildungen*

$$+ : M \times M \longrightarrow M$$
$$\cdot : R \times M \longrightarrow M$$

sodass

1) $(M, +)$ *eine abelsche Gruppe ist,*

2) die Skalarmultiplikation $\cdot$ über der Addition $+$ distributiv ist, also

$$r \cdot (m_1 + m_2) = r \cdot m_1 + r \cdot m_2$$
$$(r_1 \overset{R}{+} r_2) \cdot m = r_1 \cdot m + r_2 \cdot m$$

für alle $r, r_1, r_2 \in R$ und $m, m_1, m_2 \in M$, und

3) für alle $r, s \in R$ und $m \in M$ gilt

$$(r \overset{R}{\cdot} s) \cdot m = r \cdot (s \cdot m)$$

Hat R ein 1-Element, so verlangen wir zusätzlich $1 \cdot m = m$.

Aus dem Kontext ist typischerweise klar, ob $+$ die Addition in R oder in M bezeichnet. Wenn wir präzisieren wollen, von welcher Verknüpfung wir sprechen, notieren wir R bzw. M darüber (ebenso für $\cdot$).

Beispiel 4.3.2 *1) Sei $R = K$ ein Körper. Dann ist ein K-Modul nichts anderes als ein K-Vektorraum.*

2) Ein $\mathbb{Z}$-Modul G ist nichts anderes als eine abelsche Gruppe $(G, +)$. Die Skalarmultiplikation ist

$$\mathbb{Z} \times G \longrightarrow G$$
$$(n, g) \longmapsto n \cdot g := \underbrace{g + \ldots + g}_{n\text{-mal}}$$

mit $(-1) \cdot g := -g$.

3) Sei $(R, +, \cdot)$ ein kommutativer Ring. Dann ist $I \subset R$ ein Ideal genau dann, wenn $(I, +, \cdot)$ ein R-Modul ist.

4) Sind M_1 und M_2 Moduln über R, dann ist auch das direkte Produkt $M_1 \times M_2$ ein R-Modul mit $r \cdot (m_1, m_2) = (r \cdot m_1, r \cdot m_2)$, insbesondere:

5) Ist R ein Ring, dann ist

$$R^n = \underbrace{R \times \ldots \times R}_{n}$$

ein R-Modul.

6) *Sei $(M,+,\cdot)$ ein R-Modul. Ein* ***Untermodul*** *$U \subset M$ ist eine Untergruppe von $(M,+)$, auf die sich die Skalarmultiplikation einschränkt, d.h. mit*

$$r \cdot m \in U$$

für alle $m \in U$ und $r \in R$. Ein Untermodul ist wieder ein R-Modul.

Eine Teilmenge $U \subset M$ ist ein Untermodul genau dann, wenn $U \neq \varnothing$ und

$$\begin{aligned} m_1 + m_2 &\in U \\ r \cdot m &\in U \end{aligned}$$

für alle $m_i, m \in U$ und $r \in R$.

7) *Sei M ein R-Modul und $U \subset M$ ein Untermodul. Dann ist die Quotientengruppe M/U wieder ein R-Modul (der* ***Quotientenmodul****) mit der Skalarmultiplikation*

$$r \cdot (m + U) = r \cdot m + U$$

für $r \in R$ und $m \in M$.

8) *Sei V ein K-Vektorraum und $A \in \operatorname{End}(V)$ ein Endomorphismus (z.B. $V = K^n$ und $A \in K^{n\times n}$). Dann wird V durch den Substitutionshomomorphismus*

$$\begin{array}{ccc} K[x] & \longrightarrow & \operatorname{End}(V) \\ x & \longmapsto & A \end{array}$$

zu einem $K[x]$-Modul mit der Skalarmultiplikation

$$\begin{aligned} K[x] \times V &\longrightarrow V \\ (f, v) &\longmapsto f \cdot v := f(A)(v) \end{aligned}$$

9) *Eine R-Algebra S war ein Ring $(S,+,\cdot)$ mit einem injektiven Ringhomomorphismus $\varphi : R \to S$ und $\varphi(r)\cdot s = s \cdot \varphi(r)$ für alle $r \in R$ und $s \in S$. Mit der Skalarmultiplikation*

$$\begin{array}{rcl} * : R \times S & \longrightarrow & S \\ (r, s) & \longmapsto & r * s := \varphi(r) \cdot s \end{array}$$

wird S zu einem R-Modul.

Eine R-Algebra ist also nichts anderes als eine Menge S mit Verknüpfungen

$$\begin{aligned} + &: S \times S \to S \quad \textit{(Addition)} \\ \cdot &: S \times S \to S \quad \textit{(Multiplikation)} \\ * &: R \times S \to S \quad \textit{(Skalarmultiplikation)} \end{aligned}$$

sodass

(a) $(S, +, *)$ *ein R-Modul ist,*

(b) $(S, +, \cdot)$ *ein Ring ist und*

(c) für alle $r \in R$ und $s_1, s_2 \in S$ gilt

$$r * (s_1 \cdot s_2) = (r * s_1) \cdot s_2 = s_1 \cdot (r * s_2)$$

Definition 4.3.3 *Ein R-**Modulhomomorphismus** ist ein R-linearer Gruppenhomomorphismus $f : M \to N$ zwischen R-Moduln, das heißt*

1) $f(m_1 + m_2) = f(m_1) + f(m_2)$ *für alle $m_1, m_2 \in M$*

2) $f(r \cdot m) = r \cdot f(m)$ *für alle $m \in M$ und $r \in R$.*

Kern und Bild sind Untermoduln, und es gilt der Homomorphiesatz für Moduln

$$M/\ker(f) \cong \text{Bild}(f)$$

Definition 4.3.4 *Sei M ein R-Modul.*

*1) M heißt **endlich erzeugt**, wenn es einen surjektiven R-Modulhomomorphismus*

$$\varphi : R^r \to M$$

*gibt. Die Bilder $m_i = \varphi(e_i) \in M$ der Standardbasisvektoren e_i nennt man **Erzeuger**. Die Abbildung φ ist surjektiv genau dann, wenn sich jedes Element von M als R-Linearkombination von $m_1, ..., m_r$ schreiben lässt, d.h.*

$$\forall m \in M \ \exists a_1, ..., a_r \in R \text{ mit } m = a_1 m_1 + ... + a_r m_r$$

Wir schreiben dann wie für Gruppen

$$M = \langle m_1, ..., m_r \rangle$$

2) *M heißt **frei** vom Rang r, wenn es einen Isomorphismus $\varphi : R^r \to M$ gibt, d.h.*

$$M \cong R^r$$

*Obige Darstellung $m = a_1 m_1 + ... + a_r m_r$ ist dann eindeutig, und wir bezeichnen $m_1, ..., m_r$ als eine **Basis** von M.*

3) *Ein R-Modul M heißt **endlich präsentiert**, wenn M endlich erzeugt ist und $\ker \varphi$ ebenfalls endlich erzeugt ist.*

Beispiel 4.3.5 *Die rationalen Zahlen $\mathbb{Q}$ sind als $\mathbb{Z}$-Modul nicht endlich erzeugt: Angenommen $\mathbb{Q}$ wird von $r_1, ..., r_n$ erzeugt. Dann gibt es ein $d \in \mathbb{Z}$ teilerfremd zu den Nennern der r_i und $\frac{1}{d}$ liegt nicht in dem von $r_1, ..., r_n$ erzeugten $\mathbb{Z}$-Modul (d.h abelschen Gruppe) $\langle r_1, ..., r_n \rangle$.*

Ein K-Vektorraum der Dimension r ist als K-Modul frei vom Rang r (denn er hat eine Basis).

Der Ring $R = K[x_1, x_2, ...]$ der Polynome in abzählbar vielen Variablen ist als R-Modul endlich erzeugt (von 1), der Untermodul

$$M = \{f \in R \mid f(0) = 0\}$$

jedoch nicht, da jede endliche Menge von Polynomen nur endlich viele Variablen involviert.

Wir führen folgende Kurzschreibweise ein:

Definition 4.3.6 *Eine Sequenz von R-Modulhomomorphismen*

$$... \to M_i \overset{\varphi_i}{\to} M_{i+1} \overset{\varphi_{i+1}}{\to} M_{i+2} \to ...$$

*heißt **exakt**, wenn*

$$\text{Bild}(\varphi_i) = \ker(\varphi_{i+1}) \quad \forall i$$

Bemerkung 4.3.7 *Ein Homomorphismus $\varphi : N \to M$ ist also surjektiv, wenn die Sequenz*

$$N \overset{\varphi}{\to} M \to 0$$

exakt ist, bzw. injektiv, wenn

$$0 \to N \overset{\varphi}{\to} M$$

exakt ist.

Definition 4.3.8 *Ein endlich erzeugter Modul M ist also eine exakte Sequenz*

$$R^n \xrightarrow{\pi} M \to 0$$

Mit der Inklusion des Kerns erhalten wir auch eine exakte Sequenz

$$0 \to \ker(\varphi) \to R^n \xrightarrow{\pi} M \to 0$$

Somit ist ein endlich präsentierter Modul M eine exakte Sequenz

$$R^m \xrightarrow{A} R^n \xrightarrow{\pi} M \to 0$$

mit $A \in R^{n\times m}$. Diese Matrix A heißt ***Präsentationsmatrix*** *von M und beschreibt M vollständig, denn mit dem Homomorphiesatz gilt*

$$M \cong R^n/\ker(\pi) = R^n/\operatorname{Bild}(A)$$

Das heißt, das Bild von A sind alle Relationen, die zwischen den Erzeugern $\pi(e_i)$ von M gelten (mit e_i die Standardbasis von R^n). Oder anders ausgedrückt: Wir erhalten M aus dem freien Modul R^n, indem wir die Rechenregeln

$$r_1e_1 + \ldots + r_ne_n = 0$$

fordern für alle

$$\begin{pmatrix} r_1 \\ \vdots \\ r_n \end{pmatrix} \in \operatorname{Bild}(A)$$

d.h. aus dem Spaltenraum von A.

Jeden endlich erzeugten Modul über einem noetherschen Ring können wir so darstellen: Analog zum Resultat für Ideale kann man folgende Äquivalenz zeigen (Übung 4.6):

Definition und Satz 4.3.9 *Sei R ein kommutativer Ring mit 1. Ein R-Modul M heißt* ***noethersch****, wenn er folgende äquivalente Bedingungen erfüllt:*

1) Jede aufsteigende Kette von Untermoduln wird stationär.

2) Jeder Untermodul von M ist endlich erzeugt.

3) Jede Teilmenge von Untermoduln enthält ein maximales Element.

Mit der Kettenbedingung zeigt man die folgenden Aussagen (Übung 4.7 und 4.8):

Lemma 4.3.10 *Sei*

$$0 \to U \to F \to M \to 0$$

eine exakte Sequenz von R-Moduln. Dann ist F noethersch genau dann, wenn U und M noethersch sind.

Lemma 4.3.11 *Ist R ein noetherscher Ring, dann ist R^n ein noetherscher Modul.*

Da jeder endlich erzeugte Modul M von der Form $M \cong R^n/U$ mit einem Untermodul $U \subset R^n$ ist, folgt:

Satz 4.3.12 *Endlich erzeugte Moduln über noetherschen Ringen sind schon endlich präsentiert.*

Oder allgemeiner: Endlich erzeugte Moduln über noetherschen Ringen sind noethersch.

Insbesondere können wir mit Satz 4.3.12 endlich erzeugte $\mathbb{Z}$-Moduln (d.h. endlich erzeugte abelsche Gruppen) und endlich erzeugte $K[x]$-Moduln mittels einer Präsentationsmatrix beschreiben.

Beispiel 4.3.13 *Wir betrachten die abelsche Gruppe G mit der Präsentation als $\mathbb{Z}$-Modul*

$$0 \to \mathbb{Z}^3 \xrightarrow{A} \mathbb{Z}^4 \to G \to 0$$

gegeben durch die Matrix

$$A = \begin{pmatrix} 1 & 1 & 1 \\ -3 & 1 & 1 \\ 1 & -3 & 1 \\ 1 & 1 & -3 \end{pmatrix}$$

(also $G \cong \mathbb{Z}^4/\operatorname{Bild}(A)$). Bestimme zunächst die Smith-Normalform $D = S \cdot A \cdot T$ von A mit

$$D = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 4 & 0 \\ 0 & 0 & 4 \\ 0 & 0 & 0 \end{pmatrix} \qquad S = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 3 & 1 & 0 & 0 \\ 2 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} \qquad T = \begin{pmatrix} 1 & -1 & 0 \\ 0 & 1 & -1 \\ 0 & 0 & 1 \end{pmatrix}$$

Wir haben also ein Diagramm

$$\begin{array}{ccccccccc} 0 & \to & \mathbb{Z}^3 & \stackrel{A}{\to} & \mathbb{Z}^4 & \stackrel{\pi}{\to} & G & \to & 0 \\ & & \uparrow T & & \downarrow S & & \cong & & \\ 0 & \to & \mathbb{Z}^3 & \stackrel{D}{\to} & \mathbb{Z}^4 & \to & G' & \to & 0 \end{array}$$

Die Spalten $v_i = S^{-1}(e_i)$, $i = 1, ..., 4$ von

$$S^{-1} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ -3 & 1 & 0 & 0 \\ 1 & -1 & 1 & 0 \\ 1 & 0 & -1 & 1 \end{pmatrix}$$

(genauer deren Bilder unter π) sind Erzeuger von G mit den Relationen

$$1 \cdot v_1 = 0 \qquad 4 \cdot v_2 = 0 \qquad 4 \cdot v_3 = 0$$

Der Erzeuger v_1 ist also irrelevant und

$$G \cong G' \cong \mathbb{Z}/4 \times \mathbb{Z}/4 \times \mathbb{Z}$$

wobei die Faktoren den Erzeugern v_2, v_3, v_4 entsprechen.

Wir formulieren im nächsten Abschnitt das allgemeine Resultat.

4.4 Endlich erzeugte Moduln über Hauptidealringen

Mit Hilfe des Elementarteilersatzes können wir endlich erzeugte Moduln über Hauptidealringen beschreiben:

Sei R ein Hauptidealring und M ein endlich erzeugter R-Modul. Nach Satz 4.3.12 ist M endlich präsentiert

$$R^m \xrightarrow{A} R^n \xrightarrow{\pi} M \to 0$$

und $A \in R^{n\times m}$. Der Elementarteilersatz 4.2.2 gibt $S \in \mathrm{GL}(n,R)$ und $T \in \mathrm{GL}(m,R)$ mit

$$\begin{array}{ccccccc} R^m & \xrightarrow{A} & R^n & \xrightarrow{\pi} & M & \to & 0 \\ \uparrow T & & \downarrow S & & \cong & & \\ R^m & \xrightarrow{D} & R^n & \to & M' & \to & 0 \end{array}$$

und

$$D = \left(\begin{array}{ccc|c} d_1 & & & \\ & \ddots & & 0 \\ & & d_r & \\ \hline & 0 & & 0 \end{array}\right)$$

Somit sind mit der Standardbasis e_i von R^n

$$v_i = \pi\left(S^{-1}(e_i)\right)$$

Erzeuger von M mit den Relationen

$$d_1 v_1 = 0 \quad \ldots \quad d_r v_r = 0$$

Ist d_i eine Einheit, dann folgt aus $d_i v_i = 0$ schon $v_i = 0$, also können wir den Erzeuger v_i (und damit die i-te Zeile von D) streichen. Die letzten $m-r$ Spalten kann man streichen, da sich dadurch $\mathrm{Bild}(A) = \ker(\pi)$ nicht ändert.

Um dies als Satz zu formulieren, verwenden wir noch folgende Notation:

Definition 4.4.1 *Man sagt, ein R-Modul M ist die* ***direkte Summe***

$$M = U_1 \oplus \ldots \oplus U_n$$

von Untermoduln $U_1, \ldots, U_n \subset M$, wenn M von den Elementen der U_i erzeugt wird und für alle $u_i \in U_i$ gilt

$$u_1 + \ldots + u_n = 0 \quad \Longrightarrow \quad u_1 = \ldots = u_n = 0$$

Definition 4.4.2 *Ein Modul heißt* ***zyklisch****, wenn er von einem einzigen Element erzeugt wird.*

Satz 4.4.3 *Sei R ein Hauptidealring und M ein endlich erzeugter R-Modul. Dann gilt:*

1) *Es gibt Erzeuger $v_1, ..., v_n$ von M und $d_1, ..., d_r \in R$, $r \leq n$ mit $d_i \notin R^\times$ und $d_i \mid d_{i+1}$ für $i = 1, ..., r-1$, sodass M durch die Relationen*

$$d_1 v_1 = 0 \quad \dots \quad d_r v_r = 0$$

beschrieben wird.

2) *M ist eine direkte Summe*

$$M = U_1 \oplus ... \oplus U_n$$

von zyklischen Untermoduln, und

$$U_i \cong \begin{cases} R/(d_i) & \text{für } i \leq r \\ R & \text{für } i > r \end{cases}$$

3) *das heißt*

$$M \cong R/(d_1) \times \dots \times R/(d_r) \times R^{n-r}$$

Der ***Rang*** *$n - r$ von M ist durch M eindeutig bestimmt, ebenso die* ***Elementarteiler*** *d_i von M (bis auf Einheiten).*

Corollar 4.4.4 *Sei R ein Hauptidealring und M ein endlich erzeugter R-Modul. Sei*

$$T = \{m \in M \mid \exists r \in R \text{ mit } r \cdot m = 0\} \subset M$$

der ***Torsionsuntermodul*** *von M.*

Dann gibt es einen freien Untermodul $F \subset M$ mit

$$M = T \oplus F$$

Der freie Anteil F ist im Gegensatz zu T als Untermodul nicht kanonisch (vielmehr ist der Quotient $M/T \cong F$ kanonisch).

Bemerkung 4.4.5 *Ein Modul M heißt **torsionsfrei**, wenn $T = \{0\}$, bzw. ein **Torsionsmodul**, wenn $M = T$.*

Corollar 4.4.4 gibt: Ein endlich erzeugter Modul über einem Hauptidealring ist frei genau dann, wenn er torsionsfrei ist.

Damit folgt:

Bemerkung 4.4.6 *Sei R ein Hauptidealring. Dann ist jeder Untermodul eines freien R-Moduls wieder frei.*

Beispiel 4.4.7 *In Übung 3.19 haben wir gezeigt, dass das Ideal $M = (x, y) \subset R = K[x, y]$ kein Hauptideal ist. Als R-Untermodul von R ist M torsionsfrei, jedoch nicht frei (siehe Übung 4.9).*

Beispiel 4.4.8 *In Beispiel 4.3.13 hatten wir gesehen, dass die abelsche Gruppe G mit Präsentation*

$$0 \to \mathbb{Z}^3 \to \mathbb{Z}^4 \to G \to 0$$

$$A = \begin{pmatrix} 1 & 1 & 1 \\ -3 & 1 & 1 \\ 1 & -3 & 1 \\ 1 & 1 & -3 \end{pmatrix}$$

erzeugt wird von

$$v_2 = \begin{pmatrix} 0 \\ 1 \\ -1 \\ 0 \end{pmatrix} \qquad v_3 = \begin{pmatrix} 0 \\ 0 \\ 1 \\ -1 \end{pmatrix} \qquad v_4 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \quad \in \quad \mathbb{Z}^4 / \operatorname{Bild}(A)$$

mit den Relationen

$$4 \cdot v_2 = 0 \qquad 4 \cdot v_3 = 0$$

Also

$$M = \underbrace{\langle v_2 \rangle \oplus \langle v_3 \rangle}_{T} \oplus \underbrace{\langle v_4 \rangle}_{F}$$

mit dem (eindeutigen) Torsionsuntermodul

$$T = \langle v_2, v_3 \rangle \cong \mathbb{Z}/4 \times \mathbb{Z}/4$$

und dem (nicht eindeutigen) freien Anteil

$$F = \langle v_4 \rangle \cong \mathbb{Z}$$

Beispielsweise könnten wir für v_4 statt e_4 auch e_3 oder e_2 nehmen.

In Abschnitt 4.6 und z.B. in Übung 4.12 werden wir noch weitere Beispiele über dem Polynomring $K[x]$ sehen.

Die Zerlegung in Satz 4.4.3 kann noch verfeinert werden: Ist $d \in R$ und $d = p_1^{e_1}, ..., p_k^{e_k}$ eine Primfaktorisierung (mit allen $e_i > 0$), dann folgt mit dem Chinesischen Restsatz

$$R/(d) \cong R/(p_1^{e_1}) \times ... \times R/\left(p_k^{e_k}\right)$$

denn die Ideale $(p_i^{e_i})$ sind paarweise coprim. Somit gilt:

Satz 4.4.9 *Sei R ein Hauptidealring und M ein endlich erzeugter R-Modul. Dann gibt es ein $t \in \mathbb{N}_0$ und Primelemente $p_1, ..., p_s \in R$ und $e_1, ..., e_s \in \mathbb{N}$ mit*

$$G \cong R/(p_1^{e_1}) \times \ldots \times R/(p_s^{e_s}) \times R^t$$

und diese Darstellung ist eindeutig bis auf die Reihenfolge der Faktoren.

4.5 Der Hauptsatz über endlich erzeugte abelsche Gruppen

Als Spezialfall können wir endlich erzeugte $\mathbb{Z}$-Moduln, d.h. endlich erzeugte abelsche Gruppen, betrachten. Wir fassen die Ergebnisse aus dem letzten Abschnitt nochmals für diesen zentralen Fall zusammen:

Satz 4.5.1 *Sei G eine endlich erzeugte abelsche Gruppe. Dann gilt:*

1) G ist die direkte Summe von zyklischen Untergruppen.

2) Es gibt $0 \leq r \leq n$ *und* $d_1, ..., d_r \geq 2$ *mit* $d_i \mid d_{i+1}$ *für* $i = 1, ..., r-1$, *sodass*

$$G \cong \mathbb{Z}/(d_1) \times \ldots \times \mathbb{Z}/(d_r) \times \mathbb{Z}^{n-r}$$

3) Ebenso gibt es Primzahlen $p_1, ..., p_s$ *(nicht notwendig paarweise verschieden) und* $e_1, ..., e_s \in \mathbb{N}$ *mit*

$$G \cong \mathbb{Z}/(p_1^{e_1}) \times \ldots \times \mathbb{Z}/(p_s^{e_s}) \times \mathbb{Z}^{n-r}$$

Dabei sind r, n *und* d_i *eindeutig bestimmt, ebenso die* $p_i^{e_i}$ *(bis auf Reihenfolge).*

Im folgenden Beispiel verwenden wir zur Abkürzung des Elementarteileralgorithmus eine Bemerkung, die sich sofort aus dem Determinantenteilersatz 4.2.7 ergibt: Ist $A \in \mathbb{Z}^{2\times 2}$, dann sind die Elementarteiler von A

$$d_1 = \mathrm{ggT}(A) \qquad d_2 = \frac{\det(A)}{\mathrm{ggT}(A)}$$

Insbesondere für eine Diagonalmatrix ist d_2 das kleinste gemeinsame Vielfache der Einträge.

Beispiel 4.5.2 *Sei* G *gegeben durch die Präsentationsmatrix*

$$A = \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 3 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 18 \end{pmatrix} \in \mathbb{Z}^{5\times 5}$$

Mit dem Elementarteiler-Algorithmus erhalten wir die Smith Normalform D *von* A *als*

$$A \mapsto \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 6 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 18 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 12 & 0 \\ 0 & 0 & 0 & 18 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 6 & 0 \\ 0 & 0 & 0 & 36 \end{pmatrix} = D$$

Die Elementarteilerdarstellung in Satz 4.5.1 ist also

$$G \cong \mathbb{Z}/2 \times \mathbb{Z}/6 \times \mathbb{Z}/36$$

und die Primpotenzdarstellung mit $6 = 2 \cdot 3$ *und* $36 = 2^2 \cdot 3^2$

$$G \cong \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/3 \times \mathbb{Z}/2^2 \times \mathbb{Z}/3^2$$

Aus dieser erhalten wir wieder die Elementarteilerdarstellung als

$$\begin{array}{rcccccc} G & \cong & \mathbb{Z}/2 & \times & \mathbb{Z}/2 & \times & \mathbb{Z}/2^2 \\ & & & \times & \mathbb{Z}/3 & \times & \mathbb{Z}/3^2 \\ & \cong & \mathbb{Z}/2 & \times & \mathbb{Z}/6 & \times & \mathbb{Z}/36 \end{array}$$

denn wegen der Teilbarkeitsbedingung gilt: Schreiben wir alle Elementarteiler

$$d_i = p_1^{e_{i,1}} \cdot \ldots \cdot p_t^{e_{i,t}}$$

mit Primzahlen $p_1, \ldots, p_t$ *und* $e_{i,j} \geq 0$*, dann muss* $e_{i,j} \leq e_{i+1,j}$ *sein. Desweiteren dürfen wir jeden Primpotenzfaktor nur einmal verwenden. Siehe dazu auch Übungsaufgabe 4.10.*

4.6 Die Jordansche Normalform

Neben der $\mathbb{Z}$-Modul-Struktur von abelschen Gruppen ist auch die durch einen Endomorphismus $A = (a_{i,j}) \in K^{n \times n}$ (K ein Körper) spezifizierte $K[x]$-Modul-Struktur von K^n von besonderem Interesse.

Bemerkung 4.6.1 *In Beispiel 4.3.2(4) haben wir gesehen, dass* K^n *vermöge Substitution von* x *durch* A *ein* $K[x]$*-Modul ist mit der Skalarmultiplikation*

$$\begin{aligned} K[x] \times K^n &\longrightarrow K^n \\ (f, v) &\longmapsto f(A) \cdot v \end{aligned}$$

Aus der $K[x]$*-Modul-Struktur erhalten wir* A *zurück als die* K*-lineare Abbildung*

$$\begin{array}{ccc} K^n & \to & K^n \\ v & \mapsto & x \cdot v \end{array}$$

Eine $K[x]$*-Modul-Struktur auf* K^n *ist somit das gleiche wie ein Vektorraumendomorphismus* $A \in K^{n \times n}$*.*

Bemerkung 4.6.2 *Ein Untervektorraum* $U \subset K^n$ *ist ein* $K[x]$*-Untermodul genau dann, wenn* $A(U) \subset U$*.*

Beweis. Sei $u \in U$. Dann ist $f \cdot u \in U \ \forall f \in K[x]$ genau dann, wenn $x \cdot u \in U$, genau dann, wenn $A \cdot u \in U$. ■

Bemerkung 4.6.3 *Die Standardbasisvektoren $e_1, ..., e_n$ von K^n sind offenbar auch Erzeuger von K^n als $K[x]$-Modul, d.h. es gibt eine exakte Sequenz*

$$K[x]^n \xrightarrow{\pi} K^n \longrightarrow 0$$

Zwischen den e_i haben wir die offensichtlichen Relationen

$$x \cdot e_j = A \cdot e_j = \begin{pmatrix} a_{1,j} \\ \vdots \\ a_{n,j} \end{pmatrix} = \sum_{i=1}^{n} a_{i,j} \cdot e_i \in K^n$$

Da sich vermöge dieser Relationen jedes Element $\sum_{i=1}^{n} f_i \cdot e_i \in K[x]^n$ mit $f_i \in K[x]$ zu einem Vektor von Konstanten (d.h. einem Element von K^n) reduzieren lässt, erzeugen diese Relationen schon $\ker(\pi)$ als $K[x]$-Modul.

Somit hat K^n als $K[x]$-Modul die Präsentation

$$K[x]^n \xrightarrow{xE-A} K[x]^n \longrightarrow K^n \longrightarrow 0$$

mit der Präsentationsmatrix

$$xE - A = \begin{pmatrix} x - a_{1,1} & -a_{2,1} & \cdots & -a_{1,1} \\ -a_{1,2} & x - a_{2,2} & & \vdots \\ \vdots & & \ddots & \vdots \\ -a_{1,1} & \cdots & \cdots & x - a_{n,n} \end{pmatrix}$$

*Diese Matrix bezeichnet man in der linearen Algebra auch als **charakteristische Matrix** von A.*

Bemerkung 4.6.4 *Der Kern des Substitutionshomomorphismus (siehe auch Beispiel 3.2.10)*

$$\begin{array}{rccc} \varphi_A : & K[x] & \to & K^{n \times n} \\ & x & \mapsto & A \end{array}$$

*ist ein Hauptideal im Hauptidealring $K[x]$. Das **Minimalpolynom** p_A von A wird in der linearen Algebra definiert als der normierte Erzeuger des Kerns, also*

$$\ker(\varphi_A) = (p_A)$$

Somit ist jedes $v \in K^n$ *die Skalarmultiplikation* $p_A \cdot v = 0$, *das heißt* K^n *ist ein (endlich erzeugter) Torsionsmodul.*

Gemäß dem Satz von Cayley-Hamilton ist das ***charakteristische Polynom***

$$\chi_A = \det(xE - A) \in \ker(\varphi_A)$$

also $p_A \mid \chi_A$. *Siehe dazu auch Übungsaufgabe 4.4.*

Lemma 4.6.5 *Angenommen das charakteristische Polynom* χ_A *zerfällt in Linearfaktoren. Dann ist* K^n *als* $K[x]$*-Modul eine direkte Summe*

$$K^n = U_1 \oplus \ldots \oplus U_s$$

von zyklischen Untermoduln

$$U_i \cong K[x]/((x - \lambda_i)^{e_i})$$

und

$$\prod_{i=1}^{s} (x - \lambda_i)^{e_i} = \chi_A$$

Beweis. Wir bestimmen für $xE - A$ die Smith-Normalform

$$D = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_r \end{pmatrix}$$

mit $d_i \neq 0$ (beachte K^n ist ein Torsionsmodul), und zerlegen weiter mit dem Chinesischen Restsatz (d.h. wir wenden Satz 4.4.9 an). Damit erhalten wir eine Zerlegung

$$K^n = U_1 \oplus \ldots \oplus U_s$$

in eine direkte Summe von Untermoduln U_i und Isomorphismen

$$\alpha_i : U_i \xrightarrow{\cong} K[x]/(p_i^{e_i})$$

mit irreduziblen Polynomen $p_i \in K[x]$. Es gilt dann

$$\prod_{i=1}^{s} p_i^{e_i} = d_1 \cdot \ldots \cdot d_r = \det(D) = \det(xE - A) = \chi_A$$

Da χ_A in Linearfaktoren zerfällt, müssen die p_i schon von der Form $p_i = x - \lambda_i$ mit $\lambda_i \in K$ gewesen sein. ∎

Wir beschreiben nun eine K-Vektorraumbasis von U_i, bezüglich der $A|_{U_i}$ zu einem Jordanblock wird: Als K-Vektorraum hat

$$K[x]/((x-\lambda_i)^{e_i})$$

die Basis

$$1,\ x-\lambda_i,\ (x-\lambda_i)^2,\ \ldots,\ (x-\lambda_i)^{e_i-1}$$

Die Urbilder

$$v_{i,j} = \alpha_i^{-1}\left((x-\lambda_i)^j\right)$$

unter dem Isomorphismus $\alpha_i : U_i \longrightarrow K[x]/(p_i^{e_i})$ bilden also eine Basis $\mathcal{B}_i = (v_{i,j})_{j=1,\ldots,e_i-1}$ von U_i.

Es gilt dann

$$(A-\lambda_i E)\cdot v_{i,j} = (x-\lambda_i)\cdot\alpha_i^{-1}\left((x-\lambda_i)^j\right) = \alpha_i^{-1}\left((x-\lambda_i)^{j+1}\right) = v_{i,j+1}$$

für $j = 0, \ldots, e_i-2$ und

$$(A-\lambda_i E)\cdot v_{i,e_i-1} = (x-\lambda_i)\cdot v_{i,e_i-1} = 0$$

Das heißt, bezüglich $\mathcal{B}_i$ hat A als darstellende Matrix einen $e_i \times e_i$-**Jordanblock** zum Eigenwert λ_i

$$M_{\mathcal{B}_i}^{\mathcal{B}_i}(A|_{U_i}) = J(\lambda_i, e_i) = \begin{pmatrix} \lambda_i & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & \lambda_i \end{pmatrix} \in K^{e_i \times e_i}$$

Wir haben damit gezeigt:

Satz 4.6.6 (Jordansche Normalform) *Sei $A \in K^{n\times n}$ und $\chi_A(t)$ zerfalle über K in Linearfaktoren (z.B. für $K = \mathbb{C}$). Dann existiert ein $S \in \mathrm{GL}(n, K)$, sodass*

$$SAS^{-1} = J = \begin{pmatrix} \boxed{J(\lambda_1, e_1)} & & & 0 \\ & \boxed{J(\lambda_2, e_2)} & & \\ & & \ddots & \\ 0 & & & \boxed{J(\lambda_s, e_s)} \end{pmatrix}$$

Blockdiagonalgestalt hat mit Jordankästchen $J(\lambda_i, r_i)$ zu den (nicht notwendigerweise verschiedenen) Eigenwerten $\lambda_1, \ldots, \lambda_s$ auf der Diagonalen. Bis auf Reihenfolge der Blöcke ist J eindeutig durch A bestimmt.

Wir bemerken noch: Die Primpotenzfaktoren des letzten Elementarteilers entsprechen den maximalen Jordanblöcken, also ist $d_r = p_A$ das Minimalpolynom.

Beispiel 4.6.7 *Wir erproben den Algorithmus an der Matrix*

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

(der Einfachheit halber schon in Jordanscher Normalform). Zunächst bestimmen wir die Smith-Normalform von $xE - A$:

$$\begin{pmatrix} x & -1 & 0 & 0 & 0 \\ 0 & x & -1 & 0 & 0 \\ 0 & 0 & x & 0 & 0 \\ 0 & 0 & 0 & x & 0 \\ 0 & 0 & 0 & 0 & x-1 \end{pmatrix} \mapsto \begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & x^2 & -1 & 0 & 0 \\ 0 & 0 & x & 0 & 0 \\ 0 & 0 & 0 & x & 0 \\ 0 & 0 & 0 & 0 & x-1 \end{pmatrix}$$

$$\mapsto \begin{pmatrix} -1 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & x^3 & 0 & 0 \\ 0 & 0 & 0 & x & 0 \\ 0 & 0 & 0 & 0 & x-1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & x & 0 \\ 0 & 0 & 0 & 0 & x^3(x-1) \end{pmatrix} = D$$

Aus den Elementarteilern sehen wir, dass die Jordansche Normalform von A jeweils einen Jordanblock hat der Dimension

$$\begin{array}{c} 1 \times 1 \text{ zum Eigenwert } 0 \\ 3 \times 3 \text{ zum Eigenwert } 0 \\ 1 \times 1 \text{ zum Eigenwert } 1 \end{array}$$

Die Primpotenzfaktoren des letzten Elementarteilers entsprechen den maximalen Jordanblöcken, die des vorletzten den nächstkleineren Blöcken und so weiter.

Beispiel 4.6.8 *Hätte A dagegen zwei 1×1 Blöcke und einen 3×3 Block, alle zum Eigenwert 0, dann würden wir als Smith-*

Normalform von $xE - A$ erhalten

$$D = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & x & 0 & 0 \\ 0 & 0 & 0 & x & 0 \\ 0 & 0 & 0 & 0 & x^3 \end{pmatrix}$$

Für ein weiteres Beispiel siehe Übungsaufgabe 4.12.

4.7 Übungsaufgaben

Übung 4.1 *1) Bestimmen Sie für*

$$A = \begin{pmatrix} 4 & 6 & 2 \\ 2 & 3 & 2 \\ 2 & -2 & -2 \end{pmatrix} \in \mathbb{Z}^{3\times 3}$$

die Smith-Normalform D und $S, T \in \mathrm{GL}(3, \mathbb{Z})$ mit

$$S \cdot A \cdot T = D$$

2) Seien

$$a_1 = \begin{pmatrix} 4 \\ 2 \\ 2 \end{pmatrix},\ a_2 = \begin{pmatrix} 6 \\ 3 \\ -2 \end{pmatrix},\ a_3 = \begin{pmatrix} 2 \\ 2 \\ -2 \end{pmatrix} \in \mathbb{Z}^3$$

Bestimmen Sie eine Basis der von $a_1, ..., a_3$ erzeugten Untergruppe U von $\mathbb{Z}^3$.

3) Beschreiben Sie $\mathbb{Z}^3/U$.

Übung 4.2 *Seien*

$$g_1 = \begin{pmatrix} 1 \\ 0 \\ 2 \end{pmatrix},\ g_2 = \begin{pmatrix} 1 \\ 2 \\ 0 \end{pmatrix},\ g_3 = \begin{pmatrix} -3 \\ -3 \\ -3 \end{pmatrix},\ g_4 = \begin{pmatrix} 1 \\ 2 \\ 2 \end{pmatrix} \in \mathbb{Z}^3$$

Bestimmen Sie eine Basis der von $g_1, ..., g_4$ erzeugten Untergruppe von $\mathbb{Z}^3$.

Übung 4.3 *Sei G eine endliche abelsche Gruppe und*

$$\mathbb{Z}^n \xrightarrow{A} \mathbb{Z}^n \to G \to 0$$

mit $A = (a_{i,j}) \in \mathbb{Z}^{n\times n}$ eine Präsentation. Zeigen Sie, dass für die Gruppenordnung von G gilt

$$|G| = |\det A|$$

Übung 4.4 *Sei R ein kommutativer Ring mit 1 und M ein R-Modul mit Präsentation*

$$R^n \xrightarrow{A} R^n \to M \to 0$$

Der Annihilator von M ist

$$\mathrm{Ann}(M) = \{r \in R \mid r \cdot m = 0 \quad \forall m \in M\}$$

Zeigen Sie:

1) $\mathrm{Ann}(M)$ *ist ein Ideal.*

2) $\det(A) \in \mathrm{Ann}(M)$.

Übung 4.5 *Implementieren Sie in Maple oder GAP den Algorithmus zur Bestimmung der Smith-Normalform D einer ganzzahligen Matrix $A \in \mathbb{Z}^{n\times m}$:*

1) Schreiben Sie eine Funktion die die Elementarteiler $d_1, ..., d_r$ von A berechnet.

2) Implementieren Sie auch die Bestimmung von $T \in \mathrm{GL}(m, \mathbb{Z})$ und $S \in \mathrm{GL}(n, \mathbb{Z})$ mit

$$S \cdot A \cdot T = D = \left(\begin{array}{ccc|c} d_1 & & & \\ & \ddots & & 0 \\ & & d_r & \\ \hline & 0 & & 0 \end{array}\right)$$

3) Erproben Sie Ihre Implementation an dem Beispiel aus Aufgabe 4.1 und vergleichen Sie mit den integrierten Funktionen von Maple bzw. GAP.

Übung 4.6 *Ein R-Modul M heißt noethersch, wenn er folgende äquivalente Bedingungen erfüllt:*

1) *Jede aufsteigende Kette von Untermoduln wird stationär.*
2) *Jeder Untermodul von M ist endlich erzeugt.*
3) *Jede Teilmenge von Untermoduln enthält ein maximales Element.*

Zeigen Sie die Äquivalenz.

Übung 4.7 *Sei*

$$0 \to M' \xrightarrow{i} M \xrightarrow{p} M'' \to 0$$

eine exakte Sequenz von R-Moduln. Zeigen Sie M ist noethersch genau dann, wenn M' und M'' noethersch sind.

Übung 4.8 *Sei R ein noetherscher Ring. Zeigen Sie:*

1) *Für $n \in \mathbb{N}$ ist R^n ein noetherscher Modul.*
2) *Jeder endlich erzeugte R-Modul ist schon endlich präsentiert.*

Übung 4.9 *Sei K ein Körper und $R = K[x, y]$. Zeigen Sie, dass $M = (x, y) \subset R$ als R-Modul torsionsfrei, aber nicht frei ist.*

Übung 4.10 *Bestimmen Sie die Elementarteiler d_i von*

$$G = \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/2 \times \mathbb{Z}/3^2 \times \mathbb{Z}/3^2 \times \mathbb{Z}/3^5 \times \mathbb{Z}/5 \times \mathbb{Z}/5 \times \mathbb{Z}/7$$

das heißt die Darstellung $G \cong \mathbb{Z}/d_1 \times \ldots \times \mathbb{Z}/d_r$ mit $d_i \geq 2$ und $d_i \mid d_{i+1}$ für $i = 1, \ldots, r-1$.

Übung 4.11 *Sei $R = \mathbb{C}[x]$. Bestimmen Sie die Smith-Normalform D von*

$$A = \begin{pmatrix} x-1 & 1 & -2 \\ 1 & x & -3 \\ 0 & 1 & x-3 \end{pmatrix} \in R^{3\times 3}$$

und $S, T \in \mathrm{GL}(3, R)$ mit $D = S \cdot A \cdot T$.

Übung 4.12 *Sei*

$$B = \begin{pmatrix} 1 & -1 & 2 \\ -1 & 0 & 3 \\ 0 & -1 & 3 \end{pmatrix} \in \mathrm{End}\left(\mathbb{C}^3\right)$$

1) Zeigen Sie: Vermöge der Operation von x durch B auf $V = \mathbb{C}^3$ hat V als $\mathbb{C}[x]$-Modul die Präsentationsmatrix

$$A = xE - B = \begin{pmatrix} x-1 & 1 & -2 \\ 1 & x & -3 \\ 0 & 1 & x-3 \end{pmatrix}$$

2) Bestimmen Sie die Jordansche Normalform von B mit Hilfe des Elementarteileralgorithmus.

5

Die prime Restklassengruppe

5.1 Übersicht

Die Restklassen modulo $n \in \mathbb{Z}$

$$\overline{a} = a + n\mathbb{Z} = \{a + nk \mid k \in \mathbb{Z}\}$$

bilden einen Ring

$$\mathbb{Z}/n = \left\{\overline{0}, \overline{1}, ..., \overline{n-1}\right\}$$

mit repräsentantenweiser Addition und Multiplikation

$$\overline{a} + \overline{b} = \overline{a+b} \qquad \overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

wie wir in Abschnitt 3.3 gesehen haben. Die Menge der Restklassen ungleich 0 ist aber im Allgemeinen keine Gruppe bezüglich der Multiplikation: Beipielsweise gilt in $\mathbb{Z}/8$, dass

$$\overline{2} \cdot \overline{4} = \overline{0}$$

und damit auch

$$\overline{6} \cdot \overline{4} = \overline{0}$$

Dagegen sind $\overline{1}, \overline{3}, \overline{5}, \overline{7}$ Einheiten (das heißt bezüglich $\cdot$ invertierbar), denn

$$\overline{1} \cdot \overline{1} = \overline{1} \qquad \overline{3} \cdot \overline{3} = \overline{1} \qquad \overline{5} \cdot \overline{5} = \overline{1} \qquad \overline{7} \cdot \overline{7} = \overline{1}$$

(siehe auch Übungsaufgabe 3.2). Tatsächlich ist jedes Element von $\mathbb{Z}/n$ entweder ein Nullteiler oder eine Einheit, wie wir in Übungsaufgabe 3.5 gezeigt haben.

Die Menge der Einheiten bildet offenbar eine Gruppe (siehe auch Abschnitt 3.4), die Einheitengruppe $(\mathbb{Z}/n)^\times$, deren Struktur wir in diesem Kapitel untersuchen wollen.

Dabei werden wir verschiedene praktische Anwendungen sehen, zum Beispiel in der Kryptographie, bei Tests ob eine Zahl (wahrscheinlich) eine Primzahl ist und bei der Primfaktorisierung.

5.2 Die Einheitengruppe von $\mathbb{Z}/n$

Ein Element $\overline{a} \in \mathbb{Z}/n$ ist invertierbar genau dann, wenn es ein $b \in \mathbb{Z}$ gibt mit $\overline{a} \cdot \overline{b} = \overline{1}$, das heißt, wenn es $b, k \in \mathbb{Z}$ gibt mit

$$a \cdot b + k \cdot n = 1$$

Solche b und k erhalten wir mit dem erweiterten Euklidischen Algorithmus, falls

$$\mathrm{ggT}\,(a, n) = 1$$

Haben wir umgekehrt eine solche Darstellung der 1, dann müssen natürlich a und n teilerfremd sein (denn jeder gemeinsame Teiler teilt auch 1). Somit können wir die Elemente der Einheitengruppe beschreiben:

Satz 5.2.1 *Für $n \in \mathbb{N}$ ist*

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

*Die Elemente heißen **prime Restklassen**. Die Gruppe $(\mathbb{Z}/n)^\times$ bezeichnen wir auch als die **prime Restklassengruppe**.*

Als direkte Folgerung sehen wir nochmals:

Corollar 5.2.2 *Der Ring $\mathbb{Z}/n$ ist ein Körper genau dann, wenn n eine Primzahl ist.*

Beispiel 5.2.3 *Die Restklasse* $\overline{8} \in \mathbb{Z}/15$ *hat ein Inverses, d.h.* $\overline{8} \in (\mathbb{Z}/15)^\times$*, denn*

$$\mathrm{ggT}\,(8, 3 \cdot 5) = 1$$

Mit dem erweiterten Euklidischen Algorithmus erhalten wir eine Darstellung des größten gemeinsamen Teilers

$$1 = (2) \cdot 8 + (-1) \cdot 15$$

also ist

$$\overline{8}^{-1} = \overline{2}$$

Tatsächlich können wir uns bei der Beschreibung von $(\mathbb{Z}/n)^\times$ darauf beschränken, dass n eine Primpotenz ist, denn der Isomorphismus im Chinesischen Restsatz 3.10.3 liefert:

Corollar 5.2.4 *Sei* R *ein kommutativer Ring mit* 1 *und* $I_1, ..., I_k \subset R$ *coprime Ideale und sei* $I := I_1 \cap ... \cap I_k$*. Dann ist*

$$(R/I)^\times \cong (R/I_1)^\times \times ... \times (R/I_k)^\times$$

Beweis. Mit dem Chinesischen Restsatz ist $a + I \in (R/I)^\times$ genau dann, wenn

$$(a + I_1, ..., a + I_r) \in (R/I_1 \times ... \times R/I_k)^\times$$

also genau dann, wenn $a + I_j \in (R/I_j)^\times \ \forall j$, da die Multiplikation komponentenweise definiert ist. ■

Damit können wir die Einheitengruppe als kartesisches Produkt beschreiben:

Corollar 5.2.5 *Ist*

$$n = p_1^{e_1} \cdot ... \cdot p_k^{e_k} \in \mathbb{Z}$$

eine Primfaktorzerlegung, dann ist

$$(\mathbb{Z}/n)^\times \cong (\mathbb{Z}/p_1^{e_1})^\times \times ... \times \left(\mathbb{Z}/p_k^{e_k}\right)^\times$$

5.3 Die Eulersche Phi-Funktion und der kleine Satz von Fermat

Definition 5.3.1 *Die* ***Eulersche φ-Funktion*** $\varphi : \mathbb{N} \to \mathbb{Z}$ *ist definiert durch*

$$\varphi(n) := \left|\{r \in \mathbb{Z} \mid 1 \leq r \leq n,\ \mathrm{ggT}(r,n) = 1\}\right| = \left|(\mathbb{Z}/n)^\times\right|$$

gibt also für n die Ordnung $\varphi(n)$ der Einheitengruppe $(\mathbb{Z}/n)^\times$ an.

Satz 5.3.2 (Satz von Fermat-Euler) *Für alle $a, n \in \mathbb{Z}$, $n \geq 1$ mit $\mathrm{ggT}(a,n) = 1$ gilt*

$$a^{\varphi(n)} \equiv 1 \bmod n$$

Beweis. Nach Corollar 2.2.38 teilt die Ordnung jedes Elements $g \in G$ die Gruppenordnung, also ist

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

Angewendet auf $\overline{a} \in (\mathbb{Z}/n)^\times$ erhalten wir

$$\overline{a}^{\varphi(n)} = \overline{1}$$

■

Für Primzahlen p ist

$$\varphi(p) = p - 1$$

also

$$a^{p-1} \equiv 1 \bmod p$$

falls $p \nmid a$, und somit:

Corollar 5.3.3 (Kleiner Satz von Fermat) *Ist p eine Primzahl und $a \in \mathbb{Z}$, dann gilt*

$$a^p \equiv a \bmod p$$

Mit dem Corollar 5.2.4 zum Chinesischen Restsatz sehen wir, dass φ multiplikativ ist:

Lemma 5.3.4 *Sind $m_1, m_2 \in \mathbb{N}$ teilerfremd, dann ist*

$$\varphi(m_1 m_2) = \varphi(m_1)\,\varphi(m_2)$$

Beweis. Es gilt

$$\left|(\mathbb{Z}/m_1 m_2)^\times\right| = \left|(\mathbb{Z}/m_1)^\times\right| \cdot \left|(\mathbb{Z}/m_2)^\times\right|$$

■

Damit können wir die Berechnung von φ auf den Fall von Primpotenzen reduzieren, für die sich das Ergebnis explizit angeben lässt:

Satz 5.3.5 *Ist*

$$n = p_1^{e_1} \cdot \ldots \cdot p_k^{e_k}$$

eine Primfaktorzerlegung, dann gilt

$$\varphi(n) = \prod_{i=1}^{k} \varphi(p_i^{e_i}) = \prod_{i=1}^{k} p_i^{e_i - 1}(p_i - 1)$$

Beweis. Für p prim ist

$$\begin{aligned}\varphi(p^e) &= \left|\{a \in \mathbb{Z} \mid 1 \le a \le p^e,\ \operatorname{ggT}(a, p^e) = 1\}\right| \\ &= p^e - \frac{p^e}{p}\end{aligned}$$

Die Behauptung folgt dann mit Lemma 5.3.4 oder Corollar 5.2.5.

■

5.4 Die Struktur von zyklischen Gruppen

Für zyklische Gruppen, das heißt Gruppen, die von einem einzigen Element erzeugt werden, kann man die Untergruppen explizit beschreiben. Daraus folgt eine interessante Aussage über die Eulersche Funktion.

In Beispiel 2.3.17 haben wir gesehen, dass jede zyklische Gruppe isomorph zu der additiven Gruppe $\mathbb{Z}/n$ mit $n \ge 0$ ist (d.h. falls unendlich, isomorph zu $\mathbb{Z}$, d.h. $n = 0$). Man beachte, dass die Gruppe der Einheiten $(\mathbb{Z}/n)^\times$ bezüglich der Multiplikation nicht zyklisch sein muss. Allerdings wird uns später hauptsächlich dieser Fall interessieren.

Beispiel 5.4.1 *Die Gruppe der n-ten Einheitswurzeln*

$$\mu_n = \{\zeta \in \mathbb{C} \mid \zeta^n = 1\} \subset \mathbb{C}^\times$$

(mit der Multiplikation als Verknüpfung) ist nach Beispiel 2.2.12(7) vermöge

$$\begin{array}{ccc} (\mathbb{Z}/n, +) & \cong & \mu_n \\ j & \mapsto & e^{\frac{2\pi i}{n} j} \end{array}$$

isomorph zu $\mathbb{Z}/n$, also zyklisch.

Satz 5.4.2 *Sei $G = \langle g \rangle$ eine zyklische Gruppe. Dann ist auch jede Untergruppe von G zyklisch.*

Beweis. Sei $U \subset G$ eine Untergruppe und

$$d := \min \left\{ j \in \mathbb{N} \mid g^j \in U \right\}$$

Dann ist $U \supset \langle g^d \rangle$. Für die andere Inklusion sei $g^m \in U$ ein beliebiges Element von U. Division mit Rest in $\mathbb{Z}$ liefert eine Darstellung der Exponenten

$$m = q \cdot d + r$$

mit $0 \leq r < d$. Somit gilt

$$g^m = \left(g^d\right)^q \cdot g^r$$

Da mit $g^d, g^m \in U$ auch $g^r \in U$, folgt $r = 0$, also

$$g^m = \left(g^d\right)^q \in \left\langle g^d \right\rangle$$

■

Satz 5.4.3 *Sei $G = \langle g \rangle$ eine zyklische Gruppe der Ordnung $n = |G| < \infty$. Dann gilt:*

1) *Für $j \in \mathbb{N}$ ist*

$$\operatorname{ord}\left(g^j\right) = \frac{n}{\operatorname{ggT}(n, j)}$$

2) *Ist $d \in \mathbb{N}$ ein Teiler von n, dann gibt es genau $\varphi(d)$ Elemente der Ordnung d in G, nämlich*

$$\left\{ g^{r\frac{n}{d}} \mid 1 \leq r \leq d,\ \operatorname{ggT}(r, d) = 1 \right\}$$

3) Insbesondere hat G genau $\varphi(n)$ zyklische Erzeuger.

Beweis. Teil (1) zeigen wir in Übung 5.1. Zur Aussage (2): Es gilt mit (1)

$$\operatorname{ord}\left(g^j\right) = \frac{n}{\operatorname{ggT}(n,j)}$$

Ist also $\operatorname{ord}(g^j) = d$, d.h. $\frac{n}{d} = \operatorname{ggT}(n,j)$, und schreiben wir $j = \operatorname{ggT}(n,j) \cdot r$ mit $r \in \mathbb{Z}$, dann gilt

$$j = r \cdot \frac{n}{d}$$

und somit $\frac{n}{d} = \operatorname{ggT}\left(d \cdot \frac{n}{d}, r \cdot \frac{n}{d}\right)$, also

$$\operatorname{ggT}(r,d) = 1$$

■

Beispiel 5.4.4 *Wir betrachten die zyklische Gruppe*

$$G = \langle (1,2,3,4,5,6) \rangle \subset S_6$$

der Ordnung 6 und geben die Ordnung der Elemente an

j	0	1	2	3	4	5
$\operatorname{ord}(g^j)$	1	6	3	2	3	6

Dementsprechend ist

$$\varphi(1) = 1 \qquad \varphi(2) = 1 \qquad \varphi(3) = 2 \qquad \varphi(6) = \varphi(2)\,\varphi(3) = 2$$

Ebenso hätten wir natürlich auch $(\mu_6, \cdot) \cong (\mathbb{Z}/6, +) \cong G$ betrachten können.

Definition 5.4.5 *Erzeuger von μ_n bezeichnet man auch als **primitive n-te Einheitswurzeln**. Abbildung 5.1 gibt für die Elemente von μ_6 jeweils ihre Ordnung an, ebenso Abbildung 5.2 für die Elemente von μ_8.*

Mit Satz 5.4.3 sehen wir, dass es in einer endlichen zyklischen Gruppe zu jedem Teiler der Gruppenordnung genau eine Untergruppe dieser Ordnung gibt (und diese ist wieder zyklisch nach Satz 5.4.2):

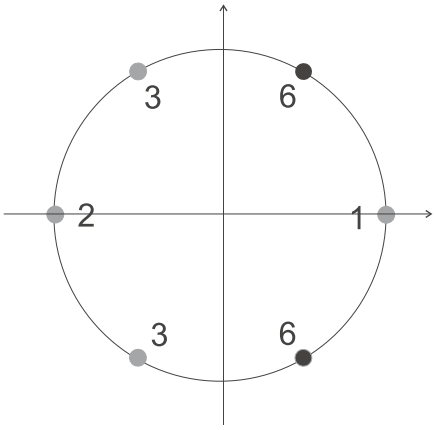


Abbildung 5.1: Sechste Einheitswurzeln und deren Ordnungen

Satz 5.4.6 *Sei $G = \langle g \rangle$ eine zyklische Gruppe der Ordnung $n = |G| < \infty$. Zu jedem Teiler d von n hat G eine eindeutige Untergruppe der Ordnung d, und diese ist*

$$\left\langle g^{\frac{n}{d}} \right\rangle \subset G$$

Beweis. Die Ordnung von $U := \left\langle g^{\frac{n}{d}} \right\rangle$ ist die Ordnung des Elements $g^{\frac{n}{d}}$, also gleich d. Weiter enthält U alle Elemente $g^{r\frac{n}{d}}$ der Ordnung d, es kann also keine weitere Untergruppe der Ordnung d geben (beachte, dass jede Untergruppe zyklisch ist mit Satz 5.4.2). ■

Bemerkung 5.4.7 *Ist G zyklisch und $U \subset G$ eine Untergruppe, dann ist auch G/U zyklisch. Beispielsweise ist*

$$\frac{\mathbb{Z}/6\mathbb{Z}}{2\mathbb{Z}/6\mathbb{Z}} \cong \mathbb{Z}/2\mathbb{Z}$$

mit dem zweiten Isomorphiesatz 2.3.20, explizit

$$\begin{array}{ccccccccc}
0 & \to & 2\mathbb{Z}/6\mathbb{Z} & \to & \mathbb{Z}/6\mathbb{Z} & \to & \mathbb{Z}/2\mathbb{Z} & \to & 0 \\
 & & \overline{0} & \mapsto & \overline{0} & \mapsto & \overline{0} & & \\
 & & & & \overline{1} & \mapsto & \overline{1} & & \\
 & & \overline{2} & \mapsto & \overline{2} & \mapsto & \overline{0} & & \\
 & & & & \overline{3} & \mapsto & \overline{1} & & \\
 & & \overline{4} & \mapsto & \overline{4} & \mapsto & \overline{0} & & \\
 & & & & \overline{5} & \mapsto & \overline{1} & &
\end{array}$$

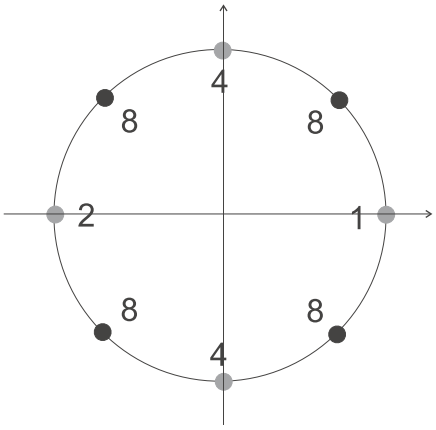


Abbildung 5.2: Achte Einheitswurzeln und deren Ordnungen

wobei die Untergruppe $2\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/3\mathbb{Z}$ *zyklisch erzeugt wird von* $\overline{2}$.

Beispiel 5.4.8 *Sei* $G = \langle g \rangle$ *eine zyklische Gruppe der Ordnung* 36. *Abbildung 5.3 zeigt die Ordnung* d *aller Untergruppen und deren Inklusionsrelationen. Dabei ist die Untergruppe der Ordnung* d *erzeugt von* $g^{\frac{36}{d}}$.

Aus Satz 5.4.3 erhalten wir auch das folgende grundlegende Resultat zur Euler-Funktion:

Corollar 5.4.9 *Für* $n \in \mathbb{N}$ *gilt*

$$\sum_{d|n} \varphi(d) = n$$

Beweis. Sei G die zyklische Gruppe der Ordnung n. Da die Ordnung d jedes Elements ein Teiler von n ist und es genau $\varphi(d)$ Elemente der Ordnung d gibt, folgt die Behauptung. ■

Es gibt eine Vielzahl von Anwendungen, die im Wesentlichen auf der Struktur der Einheitengruppe $(\mathbb{Z}/n)^\times$ beruhen. Im Folgenden wollen wir einige behandeln.

5.5 Der Fermatsche Primzahltest

Angenommen wir wollen testen, ob n eine Primzahl ist.

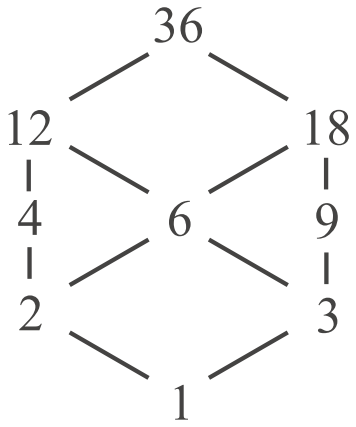


Abbildung 5.3: Untergruppenverband der zyklischen Gruppe der Ordnung 36

1) Zunächst wählen wir ein $a \in \mathbb{Z}$ und bestimmen $\mathrm{ggT}(a, n)$ mit dem Euklidischen Algorithmus. Falls $\mathrm{ggT}(a, n) \neq 1$, war n nicht prim.

2) Ist $\mathrm{ggT}(a, n) = 1$, dann testen wir, ob

$$a^{n-1} \equiv 1 \bmod n$$

Gilt dies nicht, dann kann nach dem kleinen Satz von Fermat n auch nicht prim gewesen sein. Anderenfalls können wir keine Aussage machen und gehen zurück zu (1).

Falls n prim war, bricht der Algorithmus nicht ab, man kann also nur durch mehrfaches Durchlaufen die Wahrscheinlichkeit erhöhen, dass n prim war.

Es gibt auch Zahlen, bei denen der Test in (2) für kein a mit $\mathrm{ggT}(a, n) = 1$ erkennt, dass sie nicht prim sind, die sogenannten Carmichael-Zahlen. Diese erkennt Schritt (1) für geeignetes a.

Definition 5.5.1 *Eine Zahl n heißt **Fermatsche Pseudoprimzahl** zur Basis a, wenn n nicht prim ist, aber dennoch $a^{n-1} \equiv 1 \bmod n$ gilt.*

Beispiel 5.5.2 *Die Rechnung*

$$2^5 \equiv 2 \bmod 6$$

zeigt, dass 6 *nicht prim ist.*

Dagegen gilt

$$2^{340} \equiv 1 \bmod 341$$

aber unglücklicherweise ist

$$341 = 11 \cdot 31$$

nicht prim, also 341 *eine Fermatsche Pseudoprimzahl zur Basis* $a = 2$. *Testen wir nochmals zur Basis* $a = 3$ *erhalten wir*

$$3^{340} \equiv 56 \bmod 341$$

und haben damit gezeigt, dass 341 *keine Primzahl ist.*
Man beachte:
Dies konnten wir erkennen, ohne einen Teiler zu finden.

Siehe dazu auch Übung 5.2 und 5.4.

5.6 Primfaktorisierung und das Verfahren von Pollard

Zunächst behandeln wir folgendes offensichtliche Primfaktorisierungsverfahren:

Algorithmus 5.6.1 (Probedivision) *Sei* $n \in \mathbb{Z}$ *zusammengesetzt. Für den kleinsten Primteiler* p *von* n *gilt*

$$p \leq m := \lfloor \sqrt{n} \rfloor$$

(zeigen Sie dies). Kennen wir alle Primzahlen $p \leq m$, *dann testen wir diese mit Division mit Rest. Damit können wir eine gegebene Zahl faktorisieren (und beliebig große Primzahlen finden).*

Praktisch zählt man die notwendigen Primzahlen mit dem Sieb des Eratosthenes auf:

Algorithmus 5.6.2 (Sieb des Eratosthenes) *Wir erhalten eine Liste aller Primzahlen kleiner gleich* $N \in \mathbb{N}$ *wie folgt:*

1) *Erstelle eine boolsche Liste* L *zu allen Zahlen* $2, ..., N$. *Markiere alle Zahlen als prim (true). Setze* $p = 2$.

2) Markiere alle $j \cdot p$ mit $j \geq p$ als nicht prim ($false$).

3) Finde das kleinste $q > p$ das als prim ($true$) markiert ist.
Falls $q > \sqrt{N}$ gebe L zurück.
Setze $p := q$, gehe zu Schritt (2).

Wir bemerken noch, dass in Schritt (2) alle $j \cdot p$ mit $2 \leq j < p$ schon aus vorherigen Schritten markiert sind, da sie einen Primteiler $< p$ besitzen.

Beispiel 5.6.3 *Wir bestimmen alle Primzahlen ≤ 15 und geben in jedem Durchlauf die Liste aller j mit $L_j = true$ an*

2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	3		5		7		9		11		13		15
2	3		5		7				11		13		

Im ersten Schritt streichen wir alle Vielfachen von 2, im zweiten Schritt alle Vielfachen von 3.

Es gibt wesentlich effizientere Methoden als Probedivision, um einen Primteiler zu finden, als Beispiel behandeln wir ein Verfahren von John Pollard, das unter folgender Voraussetzung gut funktioniert:

Algorithmus 5.6.4 (Pollard Faktorisierung) *Angenommen ein Primfaktor p von n hat die Eigenschaft, dass $p-1$ nur kleine Primpotenzfaktoren $\leq B$ hat. Dann lässt sich ein Vielfaches k von $p-1 = \varphi(p)$ bestimmen, ohne p zu kennen:*

$$k := \prod_{\substack{q \text{ Primzahl} \\ l \text{ maximal mit } q^l \leq B}} q^l$$

Sei nun $1 < a < n$ beliebig gewählt. Teste zunächst $\mathrm{ggT}(a,n) = 1$ (wenn nicht haben wir einen echten Teiler gefunden). Anderenfalls ist

$$\mathrm{ggT}\left(a^k - 1, n\right) > 1$$

denn k ist nach Voraussetzung ein Vielfaches von $\varphi(p)$, also $k = k' \cdot \varphi(p)$. Damit gibt der kleine Fermatsche Satz

$$a^k = \left(a^{\varphi(p)}\right)^{k'} \equiv 1 \bmod p$$

also $p \mid \mathrm{ggT}\,(a^k - 1, n)$.

Falls wir aufgrund der Wahl von a *und* B *keinen echten Teiler finden, ändern wir unsere Wahl.*

Beispiel 5.6.5 *Sei* $n = 21733$ *und* $B = 10$, *also* $k = 8 \cdot 9 \cdot 5 \cdot 7$. *Sei weiter* $a = 2$. *Dann ist*

$$\mathrm{ggT}\left(2^k - 1, n\right) = 211$$

Sowohl 211 *also auch* $\frac{n}{211} = 103$ *sind prim, was man z.B. mit Probedivision sieht. Damit haben wir* n *vollständig faktorisiert. Man beachte, dass die gefundenen Teiler im Allgemeinen nicht prim sein müssen.*

Siehe dazu auch Übungsaufgabe 5.6.

5.7 Der Primzahlsatz von Dirichlet

Dirichlets Primzahlsatz (den wir hier nicht beweisen können) besagt, dass es in jeder primen Restklasse

$$\overline{a} = \{a + k \cdot n \mid k \in \mathbb{Z}\} \in (\mathbb{Z}/n)^\times$$

unendlich viele Primzahlen gibt, und deren Anteil wird im Verhältnis zu allen Primzahlen durch die Eulersche Funktion beschrieben:

Satz 5.7.1 (Dirichlets Primzahlsatz) *Sind* $a, n \in \mathbb{Z}$ *mit*

$$\mathrm{ggT}\,(a, n) = 1$$

dann gibt es unendlich viele Primzahlen mit

$$p \equiv a \bmod n$$

Quantitativ gilt

$$\lim_{x \mapsto \infty} \frac{|\{p \leq x \mid p \text{ Primzahl}\}|}{|\{p \leq x \mid p \equiv a \bmod n,\ p \text{ Primzahl}\}|} = \varphi(n)$$

Siehe dazu auch Übungsaufgabe 5.3.

5.8 RSA

Beim RSA-Kryptosystem verwendet der Sender den öffentlichen Schlüssel des Empfängers zum Chiffrieren einer Nachricht und dieser seinen privaten Schlüssel zu Dechiffrieren, d.h. es ist ein sogenanntes Public-Key Kryptosystem. Das Verfahren wurde von James Ellis, Clifford Cocks und Malcolm Williamson im britischen Nachrichtendienst entwickelt (und geheim gehalten) und ist nach Ronald Rivest, Adi Shamir und Leonard Adleman benannt, die es später erneut entdeckt haben. Es basiert auf einer Trapdoor (Geheimtür) - Einwegfunktion

$$\{\text{Klartextnachrichten}\} \to \{\text{verschlüsselte Nachrichten}\}$$

die man leicht berechnen kann, das Urbild aber nur unter hohem Rechenaufwand, sofern man nicht die Geheimtür-Information (d.h. den privaten Schlüssel) besitzt.

Im Fall von RSA beruht dies darauf, dass die Primfaktorzerlegung (und damit die Geheimtür) heute nur schwer zu berechnen ist. Allerdings ist nicht klar, ob nicht in Zukunft schnellere Verfahren zur Verfügung stehen. Auch muss man bei der Verwendung von RSA abschätzen, wie lange die Verschlüsselung unter dem typischen exponentiellen Anstieg der Rechenleistung von Computern (Moores Gesetz) sicher ist.

Typischerweise wird aus Gründen der Geschwindigkeits RSA nur zum Austausch eines Schlüssels für ein konventionelles symmetrisches Kryptosystem (z.B. 3DES, AES, Twofish, Serpent) verwendet.

5.8.1 Setup

Man wählt eine große Zahl $N \in \mathbb{N}$ und codiert Nachrichteneinheiten in eine Zahl $0 \leq m < N$ (zum Beispiel $N = 26^k$ und repräsentiert Buchstaben durch Ziffern). In der Praxis verwendet man ein N mit etwa 200 bis 600 Dezimalziffern.

Jeder Benutzer führt nun die folgenden Schritte aus:

1) Wähle 2 Primzahlen p, q mit $p \cdot q > N$.

2) Berechne

$$n := p \cdot q$$

und den Wert der Eulerfunktion

$$\varphi(n) = (p-1)(q-1)$$

Die Zahlen p und q können nun gelöscht werden.

3) Wähle eine Zahl $e \in \mathbb{N}$ mit

$$\mathrm{ggT}(e, \varphi(n)) = 1$$

4) Berechne das Inverse $0 < d < \varphi(n)$ von e modulo $\varphi(n)$, also mit

$$ed \equiv 1 \bmod \varphi(n)$$

Nun kann $\varphi(n)$ gelöscht werden.

Der öffentliche Schlüssel ist das Tupel (n, e) und der private Schlüssel d.

5.8.2 Nachrichtenübertragung

Betrachten wir nun zwei Personen Alice und Bob mit Schlüsseln

	privat	öffentlich
Alice	d_A	(n_A, e_A)
Bob	d_B	(n_B, e_B)

Will Bob an Alice eine Nachricht m senden, berechnet er

$$c := m^{e_A} \bmod n_A$$

und überträgt c an Alice.

Diese berechnet nun zum Entschlüsseln

$$\tilde{m} := c^{d_A} \bmod n_A$$

Dann gilt modulo n_A, dass

$$\tilde{m} \equiv c^{d_A} \equiv \left(m^{e_A}\right)^{d_A} = m^{e_A d_A} = m^{1+k\cdot\varphi(n_A)} = m\cdot\left(m^{\varphi(n_A)}\right)^k \equiv m \bmod n_A$$

mit dem Satz von Fermat-Euler 5.3.2.

Beispiel 5.8.1 *Alice wählt*

$$n_A = 7 \cdot 11 = 77$$

also

$$\varphi(n_A) = 6 \cdot 10 = 60$$

und

$$e_A = 13$$

Der öffentliche Schlüssel von Alice ist dann

$$(n_A, e_A) = (77, 13)$$

Mit dem erweiterten Euklidischen Algorithmus erhalten wir

$$1 = \mathrm{ggT}(e_A, \varphi(n)) = (-23) \cdot 13 + (5) \cdot 60$$

und somit das Inverse d_A von e_A modulo $\varphi(n_A)$

$$d_A = 37$$

den privaten Schlüssel von Alice.

Bob möchte die Nachricht $m = 31$ verschlüsselt an Alice senden, berechnet also

$$m^{e_A} \bmod n_A = 31^{13} \bmod 77 = 3 \bmod 77$$

und überträgt

$$c = 3$$

Zum Entschlüsseln berechnet Alice dann

$$c^{d_A} \bmod n_A = 3^{37} = 31 \bmod 77$$

Siehe auch Übungsaufgabe 5.5.

5.9 Übungen

Übung 5.1 *1) Stellen Sie die Gruppentafel der Einheitengruppe $G = (\mathbb{Z}/14)^\times$ des Rings $\mathbb{Z}/14$ auf. Zeigen Sie, dass G zyklisch ist und bestimmen Sie alle zyklischen Erzeuger. Geben Sie auch für jedes $g \in G$ seine Ordnung $\mathrm{ord}(g)$ an.*

2) Sei $G = \langle g \rangle$ eine zyklische Gruppe der Ordnung $n = |G| < \infty$. Zeigen Sie: Die Ordnung von g^j, $j \in \mathbb{N}$ ist

$$\operatorname{ord}\left(g^j\right) = \frac{n}{\operatorname{ggT}(n,j)}$$

Welche Ordnung hat die Einheitengruppe von $\mathbb{Z}/(n)$.

Übung 5.2 *Der Fermatsche Primzahltest: n heißt Fermatsche Pseudoprimzahl zur Basis a, wenn n nicht prim ist, aber dennoch $a^{n-1} \equiv 1 \bmod n$ gilt.*

Bestimmen Sie mit Computerhilfe jeweils alle Pseudoprimzahlen $n \leq 1000$ zur Basis a mit $a = 2, 3, 5$ und vergleichen Sie deren Anzahl mit der Anzahl der Primzahlen.

Haben Sie eine Vermutung für eine Carmichael-Zahl?

Hinweis: Maple-Funktionen `nextprime` *und* `mod`*.*

Übung 5.3 *Überprüfen Sie experimentell den Primzahlsatz von Dirichlet, indem Sie den Grenzwert*

$$\lim_{x \mapsto \infty} \frac{|\{p \leq x \mid p \text{ Primzahl}\}|}{|\{p \leq x \mid p \equiv a \bmod n,\ p \text{ Primzahl}\}|}$$

für $n = 1000$ und alle $0 \leq a < n$ mit $\operatorname{ggT}(a,n) = 1$ approximativ berechnen und mit $\varphi(n)$ vergleichen. Bestimmen Sie auch den Mittelwert (über a) und die Standardabweichung.

Übung 5.4 *Sei $m \in \mathbb{Z}_{\geq 2}$. Für ein $a \in \mathbb{Z}$ gelte $a^{m-1} \equiv 1 \bmod m$ und $a^{\frac{m-1}{p}} \not\equiv 1 \bmod m$ für jeden Primteiler p von $m-1$. Zeigen Sie, dass dann m prim ist.*

Übung 5.5 *Der öffentliche RSA-Schlüssel von Alice ist*

$n_A = 161935822840646707547491477555701045096697214757652936 19$

$e_A = 2^{16} + 1$

Bob hat eine verschlüsselte Nachricht

$c = 133198771180672258316829571431051577577308271129346428 28$

an Alice geschickt. Was war der Inhalt der Nachricht?

Hinweise: Alice hat ungeschickterweise einen Primfaktor p von $n_A = p \cdot q$ gewählt, sodass $\varphi(p)$ nur Primpotenzfaktoren ≤ 200000 hat.

Um für $a, b, n \in \mathbb{N}$ effizient $a^b \bmod n$ zu berechnen, gibt es in Maple das Kommando

```
a&^b mod n
```

(das im Wesentlichen sukzessive modulo n mit a multipliziert).

Testen Sie, ob auch die Maple-Funktion `ifactor` *zum Ziel führt.*

Übung 5.6 *Implementieren Sie*

1) *das Sieb des Eratosthenes,*
2) *die Faktorisierung von ganzen Zahlen mittels Probedivision und*
3) *das Faktorisierungsverfahren von Pollard.*

Testen Sie Ihre Implementierung jeweils an Beispielen, siehe insbesondere auch Aufgabe 5.5.

6

Körper

6.1 Übersicht

In diesem Kapitel behandeln wir die Grundlagen der Körpertheorie. Wir erinnern uns, dass ein Körper ein kommutativer Ring K mit 1 war, sodass für die Einheitengruppe gilt

$$K^\times = K \setminus \{0\}$$

(das heißt jedes Element $\neq 0$ hat ein multiplikativ Inverses). Als Beispiele von Körpern kennen wir bisher neben den rationalen, reellen und komplexen Zahlen

$$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

auch die endlichen Körper

$$\mathbb{F}_p = \mathbb{Z}/p$$

für p eine Primzahl.

In erster Linie werden wir uns mit der Frage beschäftigen, wie man einen Körper K vergrößern muss, um alle Nullstellen eines Polynoms $f \in K[x]$ darstellen zu können.

Beispielsweise benötigen wir im Satz 4.6.6 über die Jordansche Normalform, dass das charakteristische Polynom in Linearfaktoren zerfällt.

Beispiel 6.1.1 *Das Polynom*

$$f = x^2 + 2x - 1 \in \mathbb{Q}[x]$$

hat die Nullstellen

$$x = -1 \pm \sqrt{2}$$

Über dem Ring

$$\mathbb{Q}\big[\sqrt{2}\big] = \Big\{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\Big\}$$

zerfällt f in Linearfaktoren

$$f = \Big(x - \big(-1 + \sqrt{2}\big)\Big)\Big(x - \big(-1 - \sqrt{2}\big)\Big)$$

Tatsächlich ist $\mathbb{Q}\big[\sqrt{2}\big]$ schon ein Körper, denn für $a+b\sqrt{2} \neq 0$ ist das Inverse

$$\frac{1}{a + b\sqrt{2}} = \frac{a - b\sqrt{2}}{a^2 - 2b^2} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \in \mathbb{Q}\big[\sqrt{2}\big]$$

Euklids Beweis der Irrationalität von $\sqrt{2}$ zeigt, dass der Nenner $a^2-2b^2 \neq 0$ ist: Gibt es $a, b \in \mathbb{Q}$ mit $a^2 = 2b^2$, dann auch teilerfremde $a, b \in \mathbb{Z}$. Somit wäre a durch 2 teilbar und damit wiederum auch b, ein Widerspruch. Geometrisch ist die Verschwindungsmenge $\{a^2 - 2b^2 = 0\} \subset \mathbb{Q}^2$ die Vereinigung von zwei Geraden mit irrationaler Steigung $\pm\sqrt{2}$.

Wie rechnet man praktisch in Körpern der Form $\mathbb{Q}\big[\sqrt{2}\big]$?

Bemerkung 6.1.2 *Der Substitutionshomomorphismus*

$$\mathbb{Q}[x] \to \mathbb{Q}\big[\sqrt{2}\big],\ x \mapsto \sqrt{2}$$

hat als Kern das Ideal $(x^2 - 2) \subset \mathbb{Q}[x]$ (warum?), also gibt der Homomorphiesatz

$$\mathbb{Q}[x] \,/\, \big(x^2 - 2\big) \cong \mathbb{Q}\big[\sqrt{2}\big],\ \overline{x} \mapsto \sqrt{2}$$

Das heißt: Man rechnet in $\mathbb{Q}\big[\sqrt{2}\big]$ wie mit Polynomen in einer Unbestimmten x mit der zusätzlichen Rechenregel

$$x^2 = 2$$

Somit hat jedes Element von $\mathbb{Q}[x] \,/\, (x^2 - 2)$ einen Repräsentanten vom Grad < 2, d.h. ist von der Form $\overline{a + bx} = a + b\overline{x}$ mit $a, b \in \mathbb{Q}$.

Wollen wir das Inverse von $\overline{a+bx} \neq 0$ *bestimmen, verwenden wir analog zum Invertieren von primen Restklassen in* $\mathbb{Z}/n$ *den erweiterten Euklidischen Algorithmus zur Bestimmung des größten gemeinsamen Teilers: Dieser berechnet Polynome* $v, w \in \mathbb{Q}[x]$ *mit*

$$v \cdot (a+bx) + w \cdot \left(x^2 - 2\right) = 1$$

denn $x^2 - 2 \in \mathbb{Q}[x]$ *ist irreduzibel. Also gilt*

$$v \cdot (a+bx) \equiv 1 \bmod \left(x^2 - 2\right)$$

oder anders ausgedrückt

$$\left(\overline{a+bx}\right)^{-1} = \overline{v} \in \mathbb{Q}[x] / \left(x^2 - 2\right)$$

Eine explizite Lösung wäre (analog zur Formel oben)

$$v = \tfrac{a}{a^2-2b^2} - \tfrac{b}{a^2-2b^2}x \qquad w = \tfrac{b^2}{a^2-2b^2}$$

Beispielsweise ist das Inverse von $\overline{x}+1$ *gegeben durch* $\overline{x}-1$*, denn Division mit Rest gibt*

$$x^2 - 2 = (x-1)(x+1) - 1$$

In $\mathbb{Q}\left[\sqrt{2}\right]$ *heißt das*

$$\left(\sqrt{2}+1\right)^{-1} = \sqrt{2} - 1$$

Die hier demonstrierten Rechnungen werden wir im Konzept der algebraischen Körpererweiterungen formalisieren.

Im zweiten Teil des Kapitels betrachten wir dann insbesondere endliche Körper. Auf der Basis der in diesem Kapitel geschaffenen Grundlagen untersuchen wir im nächsten Kapitel weiter die prime Restklassengruppe, insbesondere die Lösbarkeit von Gleichungen der Form

$$x^2 \equiv a \bmod m$$

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

Auf mehr Details über Körperautomorphismen kommen wir dann später nochmals genauer im Kapitel zur Galoistheorie zurück.

6.2 Körpererweiterungen

Die Inklusion

$$\mathbb{Q} \subset \mathbb{Q}[x]/\left(x^2-2\right)$$

(oder auch $\mathbb{Q} \subset \mathbb{Q}\left[\sqrt{2}\right]$) ist ein Beispiel einer Körpererweiterung:

Definition 6.2.1 *Ist L ein Körper und $K \subset L$ bezüglich den Verknüpfungen von L ein Körper, dann heißt K ein* ***Unterkörper*** *von L und das Tupel*

$$K \subset L$$

eine ***Körpererweiterung****. Man nennt L dann einen* ***Oberkörper*** *von K.*

Dann ist L insbesondere ein K-Vektorraum mit der Skalarmultiplikation

$$K \times L \to L,\ (k,l) \mapsto k \cdot l$$

und die Dimension von L als K-Vektorraum

$$[L:K] \coloneqq \dim_K(L)$$

heißt ***Grad der Körpererweiterung****.*

Andere gebräuchliche Schreibweisen für eine Körpererweiterung $K \subset L$ sind L/K oder $L \supset K$.

Ist $[L:K] = 1$, dann ist $1 \in L$ eine K-Vektorraumbasis von L, also:

Bemerkung 6.2.2 $[L:K] = 1$ *genau dann, wenn $L = K$.*

Beispiel 6.2.3 *Im Beispiel aus der Einleitung ist*

$$\left[\mathbb{Q}[x]/\left(x^2-2\right):\mathbb{Q}\right] = 2$$

denn jedes Element des Oberkörpers hat einen eindeutigen Repräsentanten der Form $a+bx$ mit $a,b \in \mathbb{Q}$, d.h. 1 und $\overline{x}$ bilden eine $\mathbb{Q}$-Vektorraumbasis von $\mathbb{Q}[x]/(x^2-2)$.

Für die Körpererweiterungen

$$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

gilt

$$[\mathbb{R}:\mathbb{Q}] = \infty \qquad [\mathbb{C}:\mathbb{R}] = 2$$

Jede komplexe Zahl z hat eine eindeutige Darstellung $z = a + i \cdot b$ mit Realteil $a = \mathrm{Re}(z) \in \mathbb{R}$ und Imaginärteil $b = \mathrm{Im}(z) \in \mathbb{R}$.

Satz 6.2.4 (Gradsatz) *Seien $K \subset L \subset M$ Körpererweiterungen (man nennt L auch einen **Zwischenkörper** von $K \subset M$). Dann gilt*

$$[M : K] = [M : L] \cdot [L : K]$$

Beweis. Wir müssen dies nur für $[M : L], [L : K] < \infty$ zeigen. Sei $v_1, ..., v_s$ eine L-Vektorraumbasis von M und $w_1, ..., w_r$ eine K-Vektorraumbasis von L. Jedes $m \in M$ lässt sich mit $l_i \in L$ schreiben

$$m = \sum_{i=1}^{s} l_i v_i$$

und jedes l_i mit $k_{ij} \in K$ als

$$l_i = \sum_{j=1}^{r} k_{ij} w_j$$

also

$$m = \sum_{i,j} k_{ij} w_j v_i$$

Ist $m = 0$, dann $l_i = 0 \ \forall i$ und somit $k_{ij} = 0 \ \forall i, j$.

Also bilden die $s \cdot r$ Vektoren $v_i \cdot w_j$ eine K-Vektorraumbasis von M, d.h. $s \cdot r = [M : K]$. ■

Ist also zum Beispiel $[L : K]$ eine Primzahl, dann gibt es keine echten Zwischenkörper von $K \subset L$.

6.3 Charakteristik und Primkörper

Wir beschreiben zunächst den kleinstmöglichen Unterkörper eines gegebenen Körpers K.

In Abschnitt 3.4 hatten wir die charakteristische Abbildung

$$\begin{array}{rccc} \chi : & \mathbb{Z} & \longrightarrow & K \\ & n & \longmapsto & n \cdot 1_K \end{array}$$

untersucht. Der Kern ist ein Ideal

$$\ker \chi = (p)$$

mit $p = 0$ oder prim, und man nennt $\operatorname{char}(K) = p$ die Charakteristik von K. Ist $\operatorname{char}(K) = 0$, dann setzt sich χ zu einem Monomorphismus $\mathbb{Q} \hookrightarrow K$ fort, anderenfalls liefert der Homomorphiesatz einen Monomorphismus $\mathbb{F}_p \hookrightarrow K$.

Bemerkung 6.3.1 *Ist $K \subset L$ eine Körpererweiterung, dann gilt*

$$\operatorname{char}(K) = \operatorname{char}(L)$$

denn $1_K = 1_L$.

Beispiel 6.3.2 *Es gilt also*

$$\operatorname{char}(\mathbb{Q}) = \operatorname{char}(\mathbb{R}) = \operatorname{char}(\mathbb{C}) = 0$$

$$\operatorname{char}(\mathbb{F}_p) = p$$

Ist $|K| < \infty$ endlich, dann kann χ nicht injektiv sein, d.h.

$$\begin{array}{lcl} \operatorname{char}(K) = 0 & \Rightarrow & |K| = \infty \\ \operatorname{char}(K) \text{ prim} & \Leftarrow & |K| < \infty \end{array}$$

Nicht jeder unendliche Körper hat Charakteristik 0, zum Beispiel enthält der Quotientenkörper von $\mathbb{F}_p[x]$ unendlich viele Elemente.

Definition 6.3.3 *Ein Körper heißt **Primkörper**, wenn er keinen echten Unterkörper besitzt. Ist K ein Körper, dann ist*

$$P(K) = \bigcap_{U \subset K \text{ Unterkörper}} U$$

ein Primkörper, der Primkörper von K.

Da das Bild des Monomorphismus $\mathbb{Q} \hookrightarrow K$ bzw. $\mathbb{F}_p \hookrightarrow K$ ein Unterkörper ist (und insbesondere dieselbe Charakteristik hat), können wir die möglichen Primkörper klassifizieren:

Satz 6.3.4 *Es gilt*

$$\begin{aligned} \operatorname{char}(K) = 0 &\iff P(K) \cong \mathbb{Q} \\ \operatorname{char}(K) = p &\iff P(K) \cong \mathbb{F}_p \end{aligned}$$

(mit p prim).

6.4 Maximale Ideale in Hauptidealringen

Im Beispiel in der Übersicht hatten wir gesehen, dass die Aussagen $x^2 - 2 \in \mathbb{Q}[x]$ irreduzibel und $\mathbb{Q}[x]/(x^2-2)$ ein Körper äquivalent sind.

Tatsächlich gilt in jedem Hauptidealring (siehe Bemerkungen 3.7.4 und 3.8.7, Satz 3.8.3, Satz 3.4.11):

Bemerkung 6.4.1 *Ist R ein Hauptidealring und $q \in R$, $q \neq 0$, $q \notin R^\times$, dann gilt*

$$\begin{array}{ccccc} q \text{ irreduzibel} & \iff & (q) \text{ maximal} & \iff & R/(q) \text{ Körper} \\ \Updownarrow & & & & \\ q \text{ prim} & \iff & (q) \text{ Primideal} & \iff & R/(q) \text{ Integritätsring} \end{array}$$

Beweis. Die Äquivalenz von irreduzibel und prim gilt, da Hauptidealringe faktoriell sind. Wir wiederholen nochmals den Beweis: q irreduzibel $\Leftrightarrow$ (q) maximal:

$\Leftarrow$: Sei (q) maximal und $q = a \cdot b$ mit $a, b \notin R^\times$, dann $(q) \subsetneq (a)$, denn sonst $\exists b'$ mit $a = q \cdot b'$, also $1 = b \cdot b'$, ein Widerspruch. Diese Implikation gilt in jedem Integritätsring.

$\Rightarrow$: Sei q irreduzibel und $(q) \subset (a) \subset R$ (hier verwenden wir, dass jedes Ideal ein Hauptideal ist). Dann gibt es ein $b \in R$ mit $q = a \cdot b$. Somit ist $a \in R^\times$ oder $b \in R^\times$, also $(a) = R$ oder $(a) = (q)$, das heißt (q) war maximal. ∎

6.5 Algebraische Körpererweiterungen

Sei $K \subset L$ eine Körpererweiterung und $\alpha \in L$. In Abschnitt 3.2 hatten wir

$$K[\alpha] = \text{Bild}(\varphi_\alpha)$$

als das Bild des Substitutionshomomorphismus

$$\varphi_\alpha : K[x] \to L,\ x \mapsto \alpha$$

definiert, d.h.

$$K[\alpha] = \{f(s) \mid f \in K[x]\}$$

Ebenso definiert man

$$K[\alpha_1, ..., \alpha_n] = \{f(\alpha_1, ..., \alpha_n) \mid f \in K[x_1, ..., x_n]\}$$

für $\alpha_1, ..., \alpha_n \in L$.

Lemma 6.5.1 *$K[\alpha_1, ..., \alpha_n]$ ist der Durchschnitt aller Unterringe von L, die K und $\alpha_1, ..., \alpha_n$ enthalten.*

Beweis. Jeder Ring, der K und $\alpha_1, ..., \alpha_n$ enthält muss schon $K[\alpha_1, ..., \alpha_n]$ enthalten, und $K[\alpha_1, ..., \alpha_n]$ ist ein Unterring. ■

Definition 6.5.2 *Sei $K \subset L$ eine Körpererweiterung und $\alpha_1, ..., \alpha_n \in L$. Dann definieren wir $K(\alpha_1, ..., \alpha_n)$ (genannt K adjungiert $\alpha_1, ..., \alpha_n$) als den Durchschnitt aller Unterkörper von L, die K und $\alpha_1, ..., \alpha_n$ enthalten.*

Lemma 6.5.3 *$K(\alpha_1, ..., \alpha_n)$ ist der Quotientenkörper von $K[\alpha_1, ..., \alpha_n]$.*

Beweis. Zunächst ist der Unterring $K[\alpha_1, ..., \alpha_n] \subset L$ ein Integritätsring. Mit der universellen Eigenschaft des Quotientenkörpers (siehe Übung 3.10) setzt sich die Inklusion

$$K[\alpha_1, ..., \alpha_n] \to K(\alpha_1, ..., \alpha_n)$$

zu einer Inklusion

$$Q(K[\alpha_1, ..., \alpha_n]) \to K(\alpha_1, ..., \alpha_n)$$

fort. ■

Zum Beispiel für $\alpha \in L$ ist

$$K(\alpha) = \left\{ \frac{f(\alpha)}{h(\alpha)} \mid f, h \in K[x],\ h(\alpha) \neq 0 \right\}$$

Bemerkung 6.5.4 *Sei $K \subset L$ eine Körpererweiterung. Man kann auch für eine beliebige (nicht notwendig endliche) Teilmenge $M \subset L$ die Körperadjunktion $K(M)$ definieren als den Durchschnitt aller Unterkörper von L, die K und M enthalten.*

Ebenso ist die Ringadjuktion $K[M]$ der Durchschnitt aller Unterringe von L, die K und M enthalten. Dies stimmt für $M = \{\alpha_1, ..., \alpha_n\}$ mit unserer obigen Definition überein, denn $K[\alpha_1, ..., \alpha_n]$ ist ein Unterring und jeder Ring, der K und $\alpha_1, ..., \alpha_n$ enthält, muss schon alle $f(\alpha_1, ..., \alpha_n)$, $f \in K[x_1, ..., x_n]$ enthalten.

Definition und Satz 6.5.5 *Sei $K \subset L$ eine Körpererweiterung. Ein Element $\alpha \in L$ heißt* ***algebraisch über*** *K, wenn die folgenden äquivalenten Bedingungen erfüllt sind:*

1) Es gibt ein Polynom $g \in K[x] \setminus \{0\}$ mit

$$g(\alpha) = 0$$

d.h. es gibt n und $c_1, ..., c_{n-1} \in K$ mit

$$\alpha^n + c_{n-1}\alpha^{n-1} + ... + c_1 x + c_0 = 0$$

2) $\ker(\varphi_\alpha) \neq 0$,

3) $K[\alpha] = K(\alpha)$, d.h. $K[\alpha]$ ist ein Körper.

Dann ist der normierte Erzeuger m_α des Hauptideals

$$(m_\alpha) = \ker(\varphi_\alpha) \subset K[x]$$

irreduzibel und heißt ***Minimalpolynom*** *von α. Es gilt*

$$[K[\alpha] : K] = \deg(m_\alpha)$$

und die Potenzen

$$1, \alpha, ..., \alpha^{\deg(m_\alpha)-1}$$

bilden eine K-Vektorraumbasis von $K[\alpha]$.

Der ***Grad*** *von α ist* $\deg(\alpha) := \deg(m_\alpha)$.

Ist α nicht algebraisch über K, dann heißt α ***transzendent*** *über K.*

Das Minimalpolynom von α ist das normierte Polynom kleinsten Grades, das durch φ_α auf 0 abgebildet wird.

Beweis. Wir zeigen die Äquivalenz in 6.5.5:

(1) $\Leftrightarrow$ (2) ist klar.

(2) $\Rightarrow$ (3): Mit dem Homomorphiesatz gilt

$$K[\alpha] = \text{Bild}(\varphi_\alpha) \cong K[x] / \ker(\varphi_\alpha)$$

Nach Bemerkung 6.4.1 müssen wir zeigen, dass der normierte Erzeuger $m_\alpha \neq 0$ von $\ker(\varphi_\alpha)$ irreduzibel ist: Angenommen $m_\alpha = g_1 \cdot g_2$, dann

$$\begin{array}{rccc} & 0 = m_\alpha(\alpha) = g_1(\alpha) \cdot g_2(\alpha) \in L & & \\ \Rightarrow & g_1(\alpha) = 0 & \text{oder} & g_2(\alpha) = 0 \\ \Rightarrow & m_\alpha \mid g_1 & \text{oder} & m_\alpha \mid g_2 \\ \Rightarrow & \deg(g_2) = 0 & \text{oder} & \deg(g_1) = 0 \end{array}$$

Ein konstantes Polynom $\neq 0$ ist aber eine Einheit, d.h. in $K^\times = K[x]^\times$.

(3) $\Rightarrow$ (2): Ist $\ker(\varphi_\alpha) = 0$, dann gilt mit dem Homomorphiesatz

$$K[\alpha] \cong K[x]$$

und dies ist kein Körper.

Für die restlichen Aussagen bemerken wir noch: Jedes Element von $K[x]/(m_\alpha)$ lässt sich nach Division mit Rest nach m_α durch ein eindeutiges Polynom vom Grad $< \deg(m_\alpha)$ repräsentieren. Somit bilden $1, \overline{x}, ..., \overline{x}^{\deg(m_\alpha)-1}$ eine Basis von $K[x]/(m_\alpha)$ als K-Vektorraum, d.h. $1, \alpha, ..., \alpha^{\deg(m_\alpha)-1}$ eine K-Vektorraumbasis von $K[\alpha] \cong K[x]/(m_\alpha)$. ■

Zum Rechnen in

$$\begin{array}{ccccc} K[x]/(g) & \cong & K[\alpha] & = & K(\alpha) \\ \overline{f} & \mapsto & f(\alpha) & & \end{array}$$

können wir jedes Element darstellen als ein Polynom $f \in K[x]$ mit $\deg(f) < \deg(m_\alpha)$. Für die Berechnung des multiplikativ Inversen eines Elements in $K[\alpha]$ siehe auch nochmals Übung 6.2.

Definition 6.5.6 *Eine Körpererweiterung $K \subset L$, für die es ein $\alpha \in L$ gibt mit $L = K(\alpha)$, heißt **einfach** und α nennt man ein **primitives Element** von $K \subset L$.*

Beispiel 6.5.7 *1) Die Quadratwurzel $\sqrt{2} \in \mathbb{R}$ ist algebraisch über $\mathbb{Q}$ mit Minimalpolynom $x^2 - 2$ und*

$$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}] \cong \mathbb{Q}[x]/(x^2 - 2)$$

also

$$\deg(\sqrt{2}) = [\mathbb{Q}[\sqrt{2}] : \mathbb{Q}] = 2$$

2) Die komplexen Zahlen sind

$$\begin{array}{ccc} \mathbb{C} & \cong & \mathbb{R}[x]/(x^2+1) \\ a+b\cdot i & \mapsto & \overline{a+b\cdot x} \end{array}$$

3) Es gibt transzendente Zahlen: Die Menge der Polynome vom Grad n über $\mathbb{Q}$ ist abzählbar, also die Menge der Nullstellen auch, aber $\mathbb{C}$ ist überabzählbar.

4) Die Kreiszahl π ist transzendent (Beweis von Ferdinand von Lindemann 1882, Unmöglichkeit der Quadratur des Kreises).

Bemerkung 6.5.8 *Im Beweis von Satz 6.5.5 haben wir gesehen: Für α transzendent über K ist*

$$K[\alpha] \cong K[x]$$

ein Polynomring, also kein Körper, und somit echt enthalten in

$$K(\alpha) \cong K(x)$$

(dem Körper der rationalen Funktionen in einer Variablen).

Definition 6.5.9 *Eine Körpererweiterung $K \subset L$ heißt **algebraisch**, wenn jedes $\alpha \in L$ algebraisch ist, anderenfalls heißt sie **transzendent**.*

Beispiel 6.5.10 *Der Körper der rationalen Funktionen $K(x)$ in einer Unbestimmten x über einem Körper K ist eine transzendente Körpererweiterung und $[K(x) : K] = \infty$.*

Für α algebraisch über K ist dagegen $K \subset K(\alpha)$ eine algebraische Körpererweiterung, und wir hatten gesehen, dass

$$[K(\alpha) : K] < \infty$$

beispielsweise $\left[\mathbb{Q}\left(\sqrt{2}\right) : \mathbb{Q}\right] = 2$. Zur Umkehrung:

Satz 6.5.11 *Für eine Körpererweiterung $K \subset L$ sind äquivalent:*

1) $[L : K] < \infty$

2) $K \subset L$ *ist eine algebraische Körpererweiterung und es gibt* $\alpha_1, ..., \alpha_n \in L$ *mit* $L = K(\alpha_1, ..., \alpha_n)$

3) Es gibt über K *algebraische Elemente* $\alpha_1, ..., \alpha_n \in L$ *mit* $L = K(\alpha_1, ..., \alpha_n)$

Wir bezeichnen $K \subset L$ *dann auch als* ***endlich****.*

Beweis. (1) $\Rightarrow$ (2) : Bezeichne $n := [L : K] < \infty$ die Dimension von L als K-Vektorraum. Dann sind für jedes $\alpha \in L$ die Elemente $1, \alpha, ..., \alpha^n$ linear abhängig über K, d.h. es gibt $\lambda_i \in K$ nicht alle 0 mit

$$\sum_{i=0}^{m} \lambda_i \alpha^i = 0$$

also $g(\alpha) = 0$ mit $g = \sum_{i=0}^{m} \lambda_i x^i \in K[x]$. Ist $\alpha_1, ..., \alpha_n$ eine K-Vektorraumbasis von L, dann gilt $L = K(\alpha_1, ..., \alpha_n)$.

(2) $\Rightarrow$ (3) : klar.

(3) $\Rightarrow$ (1) : Mit Satz 6.2.4 gilt

$$\begin{aligned} [L : K] \quad = \quad & [K(\alpha_1, ..., \alpha_n) : K(\alpha_1, ..., \alpha_{n-1})] \\ & \cdot [K(\alpha_1, ..., \alpha_{n-1}) : K(\alpha_1, ..., \alpha_{n-2})] \\ & \quad \vdots \\ & \cdot [K(\alpha_1, \alpha_2) : K(\alpha_1)] \\ & \cdot [K(\alpha_1) : K] \end{aligned}$$

und für jeden Faktor

$$[K(\alpha_1, ..., \alpha_i)(\alpha_{i+1}) : K(\alpha_1, ..., \alpha_i)] \leq [K(\alpha_{i+1}) : K] < \infty$$

■

Bemerkung 6.5.12 *Ist* $K \subset L$ *eine Körpererweiterung und sind* $\alpha_1, ..., \alpha_n \in L$ *algebraisch über* K*, dann*

$$K(\alpha_1, ..., \alpha_n) = K[\alpha_1, ..., \alpha_n]$$

(mit Induktion nach n*).*

Eine leichte Folgerung daraus ist (siehe Übung 6.4):

Satz 6.5.13 *Für Körpererweiterungen* $K \subset L \subset M$ *gilt:*

$$K \subset M \text{ algebraisch} \iff K \subset L \text{ und } L \subset M \text{ algebraisch}$$

Bemerkung 6.5.14 *Ist $K \subset L$ eine Körpererweiterung, dann bilden die über K algebraischen Elemente von L einen Körper A, und $K \subset A$ ist eine algebraische Körpererweiterung. Mit Satz 6.5.13 folgt, dass jedes über A algebraische Element schon über K algebraisch ist.*

Siehe auch Übung 6.5.

Beispiel 6.5.15 *Die über $\mathbb{Q}$ algebraischen Elemente von $\mathbb{C}$ (das heißt die Menge aller Nullstellen von Polynomen $f \in \mathbb{Q}[x]$, z.B. $\sqrt{2}$, $i = \sqrt{-1}$) heißen* ***algebraische Zahlen****. Sie bilden eine algebraische, nicht-endliche Körpererweiterung $\mathbb{Q} \subset \overline{\mathbb{Q}}$.*

Zu den algebraischen Zahlen siehe auch Übung 6.6.

6.6 Der Zerfällungskörper

In Bemerkung 6.4.1 haben wir gesehen, dass für $g \in K[x]$ gilt

$$K[x]/(g) \text{ ist ein Körper } \Leftrightarrow g \text{ ist irreduzibel}$$

Satz 6.6.1 (Satz von Kronecker) *Sei K ein Körper, $f \in K[x]$ ein Polynom und g ein irreduzibler Faktor von f. Dann hat f in dem Oberkörper*

$$L = K[x]/(g)$$

von K eine Nullstelle, nämlich

$$\alpha = \bar{x} = x + (g) \in L$$

und

$$L \cong K[\alpha]$$

Beweis. Schreibe $f = g \cdot h$ mit $h \in K[x]$. Dann

$$f(\alpha) = \overline{f} = \overline{g} \cdot \overline{h} = \overline{0} \in L$$

Das Minimalpolynom von α teilt g, ist also (bis auf Normieren) gleich g, denn g war irreduzibel. ■

Corollar 6.6.2 *Sei K ein Körper und $f \in K[x]$ ein Polynom vom Grad $d = \deg(f) > 0$. Dann gilt:*

- *Es existiert ein Oberkörper L von K, in dem f vollständig in Linearfaktoren zerfällt.*
- *Sind $\alpha_1, ..., \alpha_d \in L$ die Nullstellen, dann ist $K[\alpha_1, ..., \alpha_d]$ der kleinste solche Körper in L.*
- *Dieser ist bis auf Isomorphie eindeutig bestimmt und heißt* ***Zerfällungskörper*** *von f.*

Beweis. Sei g ein irreduzibler Faktor von f. In $L_1 = K[x]/(g) \cong K[\alpha]$ hat f nach dem Satz von Kronecker eine Nullstelle α, also

$$f = (x - \alpha) \cdot f_1$$

mit $f_1 \in L_1[x]$. Mit Induktion nach d existiert ein Oberkörper L von L_1, sodass f_1 in $L[x]$ in Linearfaktoren zerfällt. Also zerfällt f über L. Für den Induktionsanfang $d = 1$ nehmen wir $L = K$.

Sind $\alpha_1, ..., \alpha_d \in L$ die Nullstellen, dann ist

$$f = c \cdot (x - \alpha_1) \cdot ... \cdot (x - \alpha_d) \in K[\alpha_1, ..., \alpha_d]$$

und nach Definition ist dies der kleinste Körper der K und $\alpha_1, ..., \alpha_d$ enthält.

Zur Eindeutigkeit:

Sei L' ein weiterer Oberkörper von K, in dem f in Linearfaktoren zerfällt mit Nullstellen α_i', also

$$K[\alpha_1, ..., \alpha_d] \subset L \qquad K[\alpha_1', ..., \alpha_d'] \subset L'$$

Zu zeigen ist

$$K[\alpha_1, ..., \alpha_d] \cong K[\alpha_1', ..., \alpha_d']$$

Sei g der im ersten Schritt der Konstruktion betrachtete irreduzible (normierte) Faktor von f und $\alpha_1 = x + (g)$. Das Polynom g zerfällt über L' in Linearfaktoren. Sei ohne Einschränkung α_1' eine Nullstelle von g in L'. Dann ist das Minimalpolynom von α_1' über K ein Faktor von g und damit gleich g. Also

$$L \supset K[\alpha_1] \cong K[x]/(g) \cong K[\alpha_1'] \subset L'$$

Nach Konstruktion hat f in $K[\alpha_1][x]$ bzw. $K[\alpha_1'][x]$ Linearfaktoren $(x - \alpha_1)$ bzw. $(x - \alpha_1')$. Der Isomorphismus $K[\alpha_1] \cong K[\alpha_1']$ induziert einen Isomorphismus

$$K[\alpha_1][x] \to K[\alpha_1'][x]$$

der wegen

$$(x-\alpha_1)\cdot f_1 = f = (x-\alpha_1')\cdot f_1'$$

f_1 auf f_1' abbildet. Mit Induktion hat $f_1 \in K[\alpha_1][x]$ einen eindeutigen Zerfällungskörper. ■

Falls $[K[\alpha_1,...,\alpha_d]:K] > 1$ gilt, ist der Isomorphismus in obigem Beweis nicht eindeutig bestimmt. Statt α_1' hätten wir auch jede andere Nullstelle von g in L' wählen können. Die Galoistheorie studiert die Symmetrien, die aus dieser Nichteindeutigkeit resultieren:

Definition 6.6.3 *Seien $K \subset L_1, L_2$ Körper. Ein Isomorphismus $\varphi : L_1 \to L_2$ heißt K-**Isomorphismus**, wenn $\varphi|_K = \mathrm{id}_K$.*

*Man definiert die **Galoisgruppe** von $f \in K[x]$ bzw. der Körpererweiterung $K \subset K[\alpha_1,...,\alpha_d]$ als*

$$\begin{aligned}&\mathrm{Gal}(f) = \mathrm{Gal}(K \subset K[\alpha_1,...,\alpha_d])\\ &= \{\varphi : K[\alpha_1,...,\alpha_d] \to K[\alpha_1,...,\alpha_d] \mid \varphi \text{ ein } K\text{-Isomorphismus}\}\end{aligned}$$

Jedes solche φ ist durch seine Wirkung auf den Nullstellen $\alpha_1,...,\alpha_d$ bestimmt und bildet Nullstellen wieder auf Nullstellen ab

$$\varphi(\alpha_i) = \alpha_j$$

denn schreiben wir $f = c_n x^n + ... + c_1 x + c_0 \in K[x]$, dann

$$\begin{aligned}0 &= \varphi(f(\alpha_i))\\ &= \varphi(c_n\alpha_i^n + ... + c_1\alpha_i + c_0) = c_n\varphi(\alpha_i)^n + ... + c_1\varphi(\alpha_i) + c_0\\ &= f(\varphi(\alpha_i))\end{aligned}$$

für alle i. Somit ist φ eine bijektive Abbildung auf der Menge der Nullstellen, also

$$\mathrm{Gal}(f) \subset S_d = S(\{\alpha_1,...,\alpha_d\})$$

Einige Beispiele von Zerfällungskörpern:

Beispiel 6.6.4 *Die Nullstellen von $f = x^d - 1 \in \mathbb{Q}[x]$ in $\mathbb{C}$ bilden die zyklische Gruppe*

$$\mu_d = \left\{\alpha_j = e^{\frac{2\pi i}{d}j} \mid j = 0,...d-1\right\} \subset \mathbb{C}^\times$$

der d-ten Einheitswurzeln. Der Zerfällungskörper ist

$$\mathbb{Q}[\alpha_1, ..., \alpha_d] = \mathbb{Q}[\alpha_j]$$

für jeden zyklischen Erzeuger α_j von μ_d, d.h. (nach Abschnitt 5.4) für alle j mit $\mathrm{ggT}(d, j) = 1$, d.h. $\overline{j} \in (\mathbb{Z}/d)^\times$. Siehe auch Abbildungen 5.1 und 5.2. Können Sie $\mathrm{Gal}(f)$ bestimmen?

Beispiel 6.6.5 *Das Polynom $f = x^3 - 2 \in \mathbb{Q}[x]$ ist irreduzibel, hat in $\mathbb{C}$ die Nullstellen*

$$\alpha_n = \sqrt[3]{2} e^{\frac{2\pi i}{3} n} \text{ mit } n = 0, 1, 2$$

und $\mathbb{Q}[\alpha_1, \alpha_2, \alpha_3]$ ist der Zerfällungskörper, jedoch $\mathbb{Q}[\alpha_1, \alpha_2, \alpha_3] \neq \mathbb{Q}[\alpha_i]$ $\forall i$. Können Sie ein primitives Element der Erweiterung $\mathbb{Q} \subset \mathbb{Q}[\alpha_1, \alpha_2, \alpha_3]$ angeben?

Beispiel 6.6.6 *Wir bestimmen den Zerfällungskörper von*

$$f = x^8 + x \in \mathbb{F}_2[x]$$

Zunächst faktorisieren wir f in $\mathbb{F}_2[x]$:

Ein normiertes Polynom in $\mathbb{F}_2[x]$ vom Grad d hat d Koeffizienten, also gibt es 2^d solche Polynome. In jedem Grad erhalten wir die reduziblen Polynome als Produkt von irreduziblen von kleinerem Grad:

d	2^d	*reduzibel*	*irreduzibel*
1	2		$x,\ x+1$
2	4	$x^2,\ x^2+x,\ x^2+1$	x^2+x+1
3	8	$x^3,\ x^3+x^2,\ x^3+x,\ x^3+x^2+x$ $x^3+1,\ x^3+x^2+x+1$	$x^3+x+1,\ x^3+x^2+1$

Man beachte: Für Grad $d = 2, 3$ können wir auch einfacher entscheiden, ob ein Polynom irreduzibel ist, siehe Übungsaufgabe 6.7.

Man beachte auch: In allen Rechnungen spielen Vorzeichen keine Rolle, da in $\mathbb{F}_2 = \mathbb{Z}/2$ gilt $2 = 0$ also $-1 = 1$.

Faktorisiere

$$\begin{aligned} f &= x \cdot (x+1) \cdot \frac{x^7+1}{x+1} \\ &= x \cdot (x+1) \cdot \left(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1\right) \\ &= x \cdot (x+1) \cdot \left(x^3 + x + 1\right) \cdot \left(x^3 + x^2 + 1\right) \end{aligned}$$

Zur Konstruktion des Zerfällungskörpers betrachten wir z.B. den irreduziblen Faktor x^3+x+1, der in dem Körper

$$\begin{aligned} K &= \mathbb{F}_2[x]/\left(x^3+x+1\right) \\ &= \left\{\overline{0},\overline{1},\overline{x},\overline{x+1},\overline{x^2},\overline{x^2+x},\overline{x^2+1},\overline{x^2+x+1}\right\} \end{aligned}$$

die Nullstelle $\alpha=\overline{x}$ besitzt. Division mit Rest nach $x-\alpha=x+\alpha$ liefert

$$\begin{aligned} x^3+x+1 &= x^2\cdot(x+\alpha)+\left(\alpha x^2+x+1\right) \\ &= \left(x^2+\alpha x\right)\cdot(x+\alpha)+\left(\left(1+\alpha^2\right)x+1\right) \\ &= \left(x^2+\alpha x+\left(1+\alpha^2\right)\right)\cdot(x+\alpha)+\left(\alpha^3+\alpha+1\right) \\ &= \left(x^2+\alpha x+\left(1+\alpha^2\right)\right)\cdot(x+\alpha) \end{aligned}$$

Tatsächlich zerfällt dies weiter:

$$x^3+x+1=\left(x+\alpha^2+\alpha\right)\cdot\left(x+\alpha^2\right)\cdot(x+\alpha)$$

Da auch

$$x^3+x^2+1=(x+\alpha+1)\cdot\left(x+\alpha^2+1\right)\cdot\left(x+\alpha^2+\alpha+1\right)$$

ist K schon der Zerfällungskörper von f.

Siehe auch Übung 6.9.

Den Grund hierfür werden wir im übernächsten Abschnitt über endliche Körper in allgemeinerer Form sehen, zunächst wollen wir aber noch die Beobachtungen aus Bemerkung 6.5.14 zum algebraischen Abschluss etwas ergänzen.

6.7 Algebraisch abgeschlossene Körper

Definition und Satz 6.7.1 *Sei K ein Körper. Es sind äquivalent:*

1) *Jedes $f\in K[x]$ mit $\deg(f)\geq 1$ hat eine Nullstelle in K.*
2) *$f\in K[x]$ ist irreduzibel $\Longleftrightarrow \deg(f)=1$.*
3) *K lässt sich nicht algebraisch erweitern (d.h. ist $K\subset L$ eine algebraische Körpererweiterung, gilt schon $K=L$).*

Dann heißt K ***algebraisch abgeschlossen****.*

Beweis. (1) $\Rightarrow$ (2) : Nach Voraussetzung hat f eine Nullstelle a, mit Division mit Rest also

$$f = g\,(x - a) + r$$

und $\deg(r) = 0$. Da $0 = f(a) = r(a)$ ist $r = 0$. Induktiv ist f ein Produkt von Linearfaktoren.

(2) $\Rightarrow$ (3) : Das Minimalpolynom jedes über K algebraischen Elements a ist irreduzibel, also vom Grad 1, mit Bemerkung 6.2.2 also $a \in K$.

(3) $\Rightarrow$ (1) : Mit Satz 6.6.1 besitzt f eine Nullstelle a in einer algebraischen Erweiterung und nach Voraussetzung gilt $K(a) = K$, also $a \in K$. ■

Nicht zeigen können wir hier:

Satz 6.7.2 *Zu jedem Körper K existiert eine algebraische Körpererweiterung $K \subset \overline{K}$ mit $\overline{K}$ algebraisch abgeschlossen.*

Der Körper $\overline{K}$ ist bis auf Isomorphie eindeutig und enthält jede algebraische Erweiterung von K. Er heißt ***algebraischer Abschluss*** *von K.*

Beispiel 6.7.3 *Sei $K \subset L$ eine Körpererweiterung und L algebraisch abgeschlossen. Dann ist die Menge A der über K algebraischen Elemente von L der algebraische Abschluss von K (siehe Übung 6.5).*

Beispielsweise ist die Menge aller Nullstellen in $\mathbb{C}$ von allen Polynomen in $\mathbb{Q}[x]$ (z.B. $\sqrt{2}$ oder $i = \sqrt{-1}$, nicht jedoch π) der algebraische Abschluss $\overline{\mathbb{Q}}$ von $\mathbb{Q}$, denn es gilt der Fundamentalsatz der Algebra (ohne Beweis):

Satz 6.7.4 (Fundamentalsatz der Algebra) *Der Körper der komplexen Zahlen $\mathbb{C}$ ist algebraisch abgeschlossen.*

6.8 Endliche Körper

6.8.1 Konstruktion und Klassifikation

Ist $\mathbb{F}$ ein endlicher Körper, dann kann die charakteristische Abbildung $\chi : \mathbb{Z} \to \mathbb{F}$ nicht injektiv sein. Somit folgt mit Abschnitt 6.3:

Satz 6.8.1 *Sei $\mathbb{F}$ ein Körper mit endlich vielen Elementen. Dann ist $\operatorname{char}(\mathbb{F}) = p$ eine Primzahl, also $\mathbb{F}_p$ der Primkörper von $\mathbb{F}$ und die Anzahl der Elemente von $\mathbb{F}$ ist eine p-Potenz*

$$|\mathbb{F}| = p^r$$

mit

$$r = [\mathbb{F} : \mathbb{F}_p] < \infty$$

Beweis. $\mathbb{F}$ ist ein endlicher $\mathbb{F}_p$-Vektorraum, also muss $r = [\mathbb{F} : \mathbb{F}_p] = \dim_{\mathbb{F}_p}(\mathbb{F}) < \infty$ sein, d.h.

$$\mathbb{F} \cong \mathbb{F}_p^r$$

als $\mathbb{F}_p$-Vektorraum. ■

Die Einheitengruppe $\mathbb{F}^\times = \mathbb{F} \setminus \{0\}$ eines Körpers $\mathbb{F}$ mit p^r Elementen hat Ordnung

$$|\mathbb{F}^\times| = p^r - 1$$

also gilt mit Satz 2.2.38, dass $a^{p^r-1} = 1$ für alle $a \in \mathbb{F}^\times$ oder, wenn wir die 0 mit einschliessen wollen,

$$a^{p^r} = a \text{ für alle } a \in \mathbb{F}$$

Wir werden zeigen, dass $\mathbb{F}$ tatsächlich isomorph zu dem Zerfällungskörper von

$$x^{p^r} - x \in \mathbb{F}_p[x]$$

ist. Die Nullstellen dieses Polynoms können wir mit Hilfe des Frobeniushomomorphismus charakterisieren:

Definition und Satz 6.8.2 *Sei L ein Körper mit $\operatorname{char}(L) = p$. Die Abbildung*

$$F : L \to L$$
$$F(a) = a^p$$

ist ein Körpermonomorphismus, der ***Frobenius-Homomorphismus****.*

Für einen endlichen Körper L ist also F ein Automorphismus.

Beweis. Offenbar gilt $F(1) = 1$, $F(0) = 0$ und

$$F(a) \cdot F(b) = F(a \cdot b)$$

für alle $a, b \in L$. Erstaunlicher ist

$$F(a+b) = (a+b)^p = \sum_{j=0}^{p} \binom{p}{j} a^j b^{p-j} = a^p + b^p = F(a) + F(b)$$

Dies gilt, da p für $0 < j < p$ den Zähler von

$$\binom{p}{j} = \frac{p!}{j! \cdot (p-j)!} \in \mathbb{Z}$$

teilt, nicht jedoch den Nenner, und $p \cdot 1 = 0$.

Aus $a^p = 0$ folgt $a = 0$, also F injektiv (und somit $F : L \to L$ für L endlich schon bijektiv). ■

Bemerkung 6.8.3 *Sei L der Zerfällungskörper von $x^{p^r} - x \in \mathbb{F}_p[x]$ und $a \in L$. Dann ist a eine Nullstelle von $x^{p^r} - x$, genau dann, wenn*

$$F^r(a) = a$$

d.h. wenn a ein Fixpunkt von F^r ist.

Im Folgenden werden wir ein Kriterium benötigen, um festzustellen, ob ein Polynom $f \in K[x]$ mehrfache Nullstellen hat: Sei L der Zerfällungskörper von f. Dann heißt $a \in L$ eine ***m*-fache Nullstelle** von f, wenn

$$(x-a)^m \mid f \quad \text{und} \quad (x-a)^{m+1} \nmid f$$

Die Ableitung eines Polynoms über einem endlichen Körper kann nicht mittels einer analytischen Grenzwertbildung definiert werden. Stattdessen verwendet man allgemein die **formale Ableitung**, die für einen kommutativen Ring R mit 1 und

$$f = c_n \cdot x^n + \ldots + c_2 \cdot x^2 + c_1 \cdot x + c_0 \in R[x]$$

definiert ist als

$$f' = n \cdot c_n \cdot x^{n-1} + \ldots + 2 \cdot c_2 \cdot x + c_1$$

Es gelten die übliche Produkt- und Kettenregel (Übung).

Lemma 6.8.4 *Mit der Notation wie oben ist $a \in L$ eine mehrfache Nullstelle (d.h. $m \geq 2$) von f genau dann, wenn $f(a) = 0$ und $f'(a) = 0$.*

Beweis. Sei $f = (x-a)^m \cdot g$ mit $g(a) \neq 0$. Dann

$$f' = (x-a)^{m-1} \cdot (m \cdot g + (x-a) \cdot g')$$

Ist $m \geq 2$, dann $f(a) = 0$ und $f'(a) = 0$. Ist $m = 0$, dann $f(a) \neq 0$. Ist $m = 1$, dann $f'(a) = g(a) \neq 0$. ■

Ein Polynom, das nur einfache Nullstellen hat, (bzw. oft auch, sodass jeder irreduzible Faktor nur einfache Nullstellen hat) bezeichnet man als **separabel**.

Satz 6.8.5 *Zu jeder Primzahlpotenz p^r gibt es bis auf Isomorphie genau einen Körper $\mathbb{F}_{p^r}$ mit p^r Elementen, nämlich den Zerfällungskörper von*

$$x^{p^r} - x \in \mathbb{F}_p[x]$$

Beweis. Das Polynom $f = x^{p^r} - x$ hat keine mehrfachen Nullstellen, denn

$$f' = q \cdot x^{p^r-1} - 1 = -1 \in \mathbb{F}_p[x]$$

hat keine Nullstellen. Der Zerfällungskörper L von f enthält also die p^r Nullstellen von f. Wir zeigen, dass die Nullstellen von f einen Körper bilden. Dann ist die Menge der Nullstellen von f schon gleich L, also $|L| = p^r$.

Mit der r-ten Potenz $F^r : L \to L$, $a \mapsto a^{p^r}$ des Frobenius gilt

$$a \text{ ist eine Nullstelle von } x^{p^r} - x \Leftrightarrow F^r(a) = a$$

Seien α, β Nullstellen von f. Dann ist

$$F^r(\alpha + \beta) = F^{r-1}(F(\alpha) + F(\beta)) = \ldots = F^r(\alpha) + F^r(\beta) = \alpha + \beta$$

also auch $\alpha + \beta$ eine Nullstelle von f, ebenso

$$F^r(\alpha \cdot \beta) = F^r(\alpha) \cdot F^r(\beta) = \alpha \cdot \beta$$

d.h. $\alpha \cdot \beta$ eine Nullstelle von f.

Mit der Eindeutigkeit des Zerfällungskörpers ist jeder Körper mit p^r Elementen isomorph zu L. ■

Bemerkung 6.8.6 *Für p prim und $g \in \mathbb{F}_p[x]$ ein irreduzibles Polynom vom Grad r ist $\mathbb{F}_p[x]/(g)$ ein Körper mit p^r Elementen, also können wir $\mathbb{F}_{p^r}$ explizit konstruieren als*

$$\mathbb{F}_{p^r} \cong \mathbb{F}_p[x]/(g)$$

sofern die Existenz eines solchen g gesichert ist. Dies werden wir gleich in Corollar 6.8.10 sehen.

Wie man alle irreduziblen Polynome in einem gegebenen Grad rekursiv aufzählt, haben wir bereits gesehen, siehe Beispiel 6.6.6, oder auch nochmal das einfachst mögliche Beispiel:

Beispiel 6.8.7 *Da $[\mathbb{F}_4 : \mathbb{F}_2] = 2$, benötigen wir, um $\mathbb{F}_4$ explizit zu konstruieren, ein irreduzibles Polynom in $\mathbb{F}_2[x]$ vom Grad 2. Ein normiertes Polynom vom Grad d hat d Koeffizienten, also gibt es 2^d solche Polynome. In jedem Grad erhalten wir die reduziblen Polynome als Produkt von irreduziblen von kleinerem Grad:*

d	2^d	*reduzibel*	*irreduzibel*
1	2		$x,\ x+1$
2	4	$x^2,\ x^2+x,\ x^2+1$	x^2+x+1

also

$$\mathbb{F}_4 \cong \mathbb{F}_2[x]/\left(x^2+x+1\right)$$

Siehe auch Übungsaufgaben 3.14, 6.9 und 6.11.

6.8.2 Die Einheitengruppe eines endlichen Körpers

Wir zeigen nun, dass die Elemente ungleich Null eines endlichen Körpers eine zyklische Gruppe bilden. Damit können wir die Resultate aus Abschnitt 5.4 anwenden.

Satz 6.8.8 *Die Einheitengruppe $\mathbb{F}_q^\times$ eines endlichen Körpers mit q Elementen ist zyklisch.*

Insbesondere gibt es mit Satz 5.4.3 in $\mathbb{F}_q^\times$ zu jedem Teiler d von $q-1$ genau $\varphi(d)$ Elemente der Ordnung d.

Beweis. Sei $a \in \mathbb{F}_q^\times$ und $d = \operatorname{ord}(a)$, also d ein Teiler von $\left|\mathbb{F}_q^\times\right| = q-1$. Die Elemente der zyklischen Gruppe

$$\langle a \rangle = \left\{1, a, \ldots, a^{d-1}\right\}$$

sind mit Satz 2.2.38 Nullstellen von $x^d - 1 \in \mathbb{F}_q[x]$ und, da dieses Polynom maximal d Nullstellen in $\mathbb{F}_q$ haben kann, gilt

$$\langle a \rangle = \left\{ b \in \mathbb{F}_q \mid b^d = 1 \right\}$$

Jedes Element von $\mathbb{F}_q$ der Ordnung d ist also in dieser Gruppe enthalten. Mit Satz 5.4.3 gibt es in $\langle a \rangle$ genau $\varphi(d)$ Elemente der Ordnung d (d.h. zyklische Erzeuger), nämlich die a^j mit $\mathrm{ggT}(j, d) = 1$.

Es gibt also für jeden Teiler d von $q-1$ in $\mathbb{F}_q^\times$ entweder keine oder $\varphi(d)$ Elemente der Ordnung d. Andererseits gilt mit Corollar 5.4.9

$$\sum_{d \mid (q-1)} \varphi(d) = q - 1 = \left| \mathbb{F}_q^\times \right|$$

und somit muss es in $\mathbb{F}_q^\times$ für jeden Teiler d von $q-1$ genau $\varphi(d)$ Elemente der Ordnung d geben. Insbesondere existieren $\varphi(q-1) > 0$ Elemente der Ordnung $q-1$ (d.h. zyklische Erzeuger). ■

Alternativ können wir auch den Hauptsatz 4.5.1 über endlich erzeugte abelsche Gruppen anwenden:

Beweis. Der Fall $q = 2$ also $\mathbb{F}_q^\times = \{1\}$ ist klar. Sei also $q > 2$. Da $\mathbb{F}_q^\times$ eine endliche abelsche Gruppe ist, gibt es $d_1, \ldots, d_r \geq 2$ mit $d_i \mid d_{i+1}$ für $i = 1, \ldots, r-1$, sodass

$$\mathbb{F}_q^\times \cong \mathbb{Z}/(d_1) \times \ldots \times \mathbb{Z}/(d_r)$$

Diese Gruppe enthält eine Untergruppe

$$\underbrace{\mathbb{Z}/(d_1) \times \ldots \times \mathbb{Z}/(d_1)}_{r}$$

und somit d_1^r Elemente, die Nullstellen von $x^{d_1} - 1$ sind. Ein Polynom vom Grad d_1 kann aber maximal d_1 Nullstellen haben, das heißt $r = 1$, also

$$\mathbb{F}_q^\times \cong \mathbb{Z}/(d_1)$$

■

Aus Satz 6.8.8 folgt:

Corollar 6.8.9 (Satz vom primitiven Element) *Jede endliche Erweiterung eines endlichen Körpers ist einfach (hat also ein primitves Element).*

Beweis. Ist $|K| < \infty$ und $[L:K] < \infty$, dann auch $|L| < \infty$ und somit $L^\times = \langle \alpha \rangle$ zyklisch nach Satz 6.8.8. Ist $\mathbb{F}_p = P(L) \subset K$ der Primkörper von L, dann $L = \mathbb{F}_p[\alpha] = K[\alpha]$. ■

Es gibt auch eine Version dieses Satzes für nicht-endliche Körper. Mit Corollar 6.8.9 sehen wir:

Corollar 6.8.10 *Sei q eine Primpotenz. In $\mathbb{F}_q[x]$ gibt es irreduzible Polynome vom Grad n für alle $n \in \mathbb{N}$.*

Beweis. Die Körpererweiterung $\mathbb{F}_q \subset \mathbb{F}_{q^n}$ ist mit Corollar 6.8.9 einfach, also existiert ein $\alpha \in \mathbb{F}_{q^n}$ mit $\mathbb{F}_{q^n} = \mathbb{F}_q[\alpha]$,

$$\deg(m_\alpha) = [\mathbb{F}_{q^n} : \mathbb{F}_q] = n$$

und das Minimalpolynom $m_\alpha \in \mathbb{F}_q[x]$ ist irreduzibel. ■

6.8.3 Die Unterkörper eines endlichen Körpers

Bemerkung 6.8.11 *Für einen endlichen Körper $\mathbb{F}$ mit Primkörper $\mathbb{F}_p$ ist der Frobenius-Automorphismus F ein $\mathbb{F}_p$-Isomorphismus, denn die Elemente von $\mathbb{F}_p \subset \mathbb{F}$ sind, wie oben schon bemerkt, Nullstellen von $x^p - x$ also Fixpunkte von F.*

Sei φ ein Automorphismus von $\mathbb{F}$. Dann ist

$$\mathrm{Fix}(\varphi) = \{a \in \mathbb{F} \mid \varphi(a) = a\}$$

ein Unterkörper von $\mathbb{F}$ (Übung).

Damit können wir z.B. den Primkörper von $\mathbb{F}$ beschreiben als

$$\mathbb{F}_p = \mathrm{Fix}(F)$$

Beispiel 6.8.12 *Für*

$$\begin{aligned}\mathbb{F}_4 &= \mathbb{F}_2[x]/\left(x^2+x+1\right)\\ &= \left\{\overline{0}, \overline{1}, \overline{x}, \overline{x+1}\right\}\end{aligned}$$

gilt

$$\begin{aligned}\mathrm{Fix}(F) &= \left\{a \in \mathbb{F} \mid a^2 = a\right\} = \left\{\overline{0}, \overline{1}\right\} = \mathbb{F}_2\\ \mathrm{Fix}\left(F^2\right) &= \left\{a \in \mathbb{F} \mid a^4 = a\right\} = \mathbb{F}_4\end{aligned}$$

Mit dieser Methode können wir alle Unterkörper finden:

Zunächst ist klar, dass $\mathbb{F}_{p^r}$ nur Unterkörper der Form $\mathbb{F}_{p^s}$ mit $s \mid r$ haben kann:

Bemerkung 6.8.13 *Ist $K \subset \mathbb{F}_{p^r}$ ein Unterkörper, dann ist $K \cong \mathbb{F}_{p^s}$ für einen Teiler s von r.*

Beweis. Der Körper K enthält den Primkörper $\mathbb{F}_p$, und mit $s := [K : \mathbb{F}_p]$ ist $|K| = p^s$, also $K \cong \mathbb{F}_{p^s}$ mit Satz 6.8.5. Dann gibt Satz 6.2.4, dass

$$r = [\mathbb{F}_{p^r} : \mathbb{F}_p] = [\mathbb{F}_{p^r} : K] \cdot [K : \mathbb{F}_p] = [\mathbb{F}_{p^r} : K] \cdot s$$

■

Satz 6.8.14 *In $\mathbb{F}_{p^r}$ existiert zu jedem Teiler s von r genau ein Unterkörper von $\mathbb{F}_{p^r}$ mit p^s Elementen, nämlich*

$$\mathbb{F}_{p^s} = \operatorname{Fix}\left(F^s\right) = \left\{a \in \mathbb{F}_{p^r} \mid a^{p^s} = a\right\}$$

Oder anders ausgedrückt, es gibt eine Bijektion

$$\begin{array}{ccc} \{\text{Teiler von } r\} & \rightleftarrows & \{\text{Unterkörper von } \mathbb{F}_{p^r}\} \\ s & \mapsto & \operatorname{Fix}\left(F^s\right) = \mathbb{F}_{p^s} \end{array}$$

Beweis. Mit Satz 6.8.8 ist $\mathbb{F}_{p^r}^\times = \langle \alpha \rangle$ zyklisch der Ordnung $p^r - 1$. Schreiben wir $r = s \cdot d$, dann

$$p^r - 1 = p^{sd} - 1 = \left(p^s - 1\right)\left(1 + p^s + \ldots + p^{(d-1)s}\right)$$

Mit Satz 5.4.6 ist also

$$\left\langle \alpha^{(p^r-1)/(p^s-1)} \right\rangle \subset \langle \alpha \rangle = \mathbb{F}_{p^r}^\times$$

eine Untergruppe der Ordnung $p^s - 1$, und somit ist diese in dem Fixkörper

$$\operatorname{Fix}\left(F^s\right) = \left\{a \in \mathbb{F}_{p^r} \mid a^{p^s} = a\right\}$$

enthalten, also $|\operatorname{Fix}\left(F^s\right)| = p^s$. ■

Bemerkung 6.8.15 *Aus dem Beweis sehen wir noch: Ist s ein Teiler von r und α ein zyklischer Erzeuger von*

$$\mathbb{F}_{p^r}^\times = \langle \alpha \rangle$$

dann

$$\mathbb{F}_{p^s}^\times = \left\langle \alpha^{(p^r-1)/(p^s-1)} \right\rangle$$

Siehe dazu auch Übung 6.11.

Beispiel 6.8.16 *Wir betrachten*

$$\begin{aligned}\mathbb{F}_{2^4} &\cong \mathbb{F}_2[x]/\left(x^4+x+1\right)\\ &= \{\overline{0},\overline{1},\overline{x},\overline{x+1},\overline{x^2},\overline{x^2+1},\overline{x^2+x},\overline{x^2+x+1},\\ &\quad \overline{x^3},\overline{x^3+1},\overline{x^3+x},\overline{x^3+x^2},\overline{x^3+x+1},\\ &\quad \overline{x^3+x^2+1},\overline{x^3+x^2+x},\overline{x^3+x^2+x+1}\}\end{aligned}$$

Es gilt

$$\begin{aligned}\left(\overline{x^2+x}\right)^4 &= \overline{x^8+x^4} = \overline{x^2+1+x+1} = \overline{x^2+x}\\ \left(\overline{x^2+x+1}\right)^4 &= \overline{x^8+x^4+1} = \overline{x^2+x+1}\end{aligned}$$

also

$$\begin{array}{rcl}\mathbb{F}_2 = & \operatorname{Fix}(F) & = \{a\in\mathbb{F}_{2^4} \mid a^2=a\} = \left\{\overline{0},\overline{1}\right\}\\ & \cap & \\ \mathbb{F}_{2^2} = & \operatorname{Fix}(F^2) & = \{a\in\mathbb{F}_{2^4} \mid a^4=a\} = \left\{\overline{0},\overline{1},\overline{x^2+x},\overline{x^2+x+1}\right\}\\ & \cap & \\ \mathbb{F}_{2^4} = & \operatorname{Fix}(F^4) & = \{a\in\mathbb{F}_{2^4} \mid a^{16}=a\}\end{array}$$

Siehe auch Übung 6.14 und 6.10.

Beispiel 6.8.17 *Der Körper $\mathbb{F}_{2^{12}}$ hat folgende Unterkörper: Den Primkörper*

$$\mathbb{F}_2 = \left\{a\in\mathbb{F}_{2^{12}} \mid a^2=a\right\}$$

die echten Unterkörper

$$\begin{aligned}\mathbb{F}_{2^2} = \mathbb{F}_4 &= \left\{a\in\mathbb{F}_{2^{12}} \mid a^4=a\right\}\\ \mathbb{F}_{2^4} = \mathbb{F}_{16} &= \left\{a\in\mathbb{F}_{2^{12}} \mid a^{16}=a\right\}\\ \mathbb{F}_{2^3} = \mathbb{F}_8 &= \left\{a\in\mathbb{F}_{2^{12}} \mid a^8=a\right\}\\ \mathbb{F}_{2^6} = \mathbb{F}_{64} &= \left\{a\in\mathbb{F}_{2^{12}} \mid a^{64}=a\right\}\end{aligned}$$

und sich selbst

$$\mathbb{F}_{2^{12}} = \mathbb{F}_{4096} = \left\{a\in\mathbb{F}_{2^{12}} \mid a^{4096}=a\right\}$$

Die Inklusionen zwischen den Unterkörpern sind in Abbildung 6.1 dargestellt.

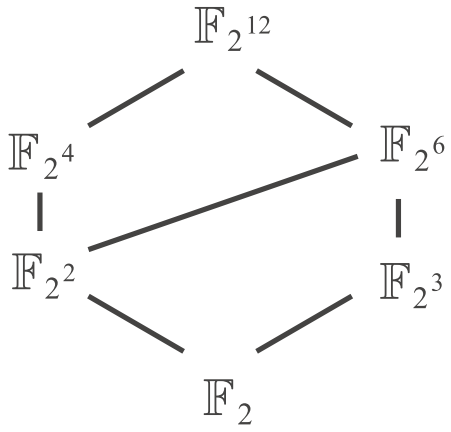


Abbildung 6.1: Unterkörper von $\mathbb{F}_{2^{12}}$

Satz 6.8.18 *Das Polynom $x^{p^r} - x \in \mathbb{F}_p[x]$ ist das Produkt aller normierten irreduziblen Polynome vom Grad d mit $d \mid r$.*

Beweis. Zeige: Ist $f \in \mathbb{F}_p[x]$ irreduzibel vom Grad d, dann gilt

$$f \mid \left(x^{p^r} - x\right) \Leftrightarrow d \mid r$$

Da $x^{p^r} - x$ nur einfache Nullstellen hat, folgt damit die Behauptung.

1) Angenommen $d \mid r$. Mit Satz 6.6.1 gibt es einen Oberkörper $K \supset \mathbb{F}_p$, in dem f eine Nullstelle $\alpha \in K$ hat und für den $[K : \mathbb{F}_p] = d$ gilt. Also ist $|K| = p^d$ und

$$K \cong \operatorname{Fix}\left(F^d\right) \subset \mathbb{F}_{p^r}$$

Das Polynom

$$x^{p^r} - x = \prod_{a \in \mathbb{F}_{p^r}} (x - a)$$

wird somit von

$$x^{p^d} - x = \prod_{a \in K} (x - a)$$

geteilt, hat also α als Nullstelle und wird damit vom Minimalpolynom f von α geteilt.

2) Angenommen $f \mid (x^{p^r} - x)$. In $\mathbb{F}_{p^r}[x]$ zerfällt mit $x^{p^r} - x$ also auch f in Linearfaktoren. Ist $\alpha \in \mathbb{F}_{p^r}$ eine Nullstelle von f, dann

$$r = [\mathbb{F}_{p^r} : \mathbb{F}_p] = [\mathbb{F}_{p^r} : \mathbb{F}_p(\alpha)] \cdot \underbrace{[\mathbb{F}_p(\alpha) : \mathbb{F}_p]}_{d}$$

■

Beispiel 6.8.19 *In* $\mathbb{F}_2[x]$ *ist*

$$\begin{array}{lllll} x^{2^1} - x = & x(x-1) & & & \\ x^{2^2} - x = & x(x-1) & (x^2+x+1) & & \\ x^{2^3} - x = & x(x-1) & & (x^3+x+1)(x^3+x^2+1) & \\ x^{2^6} - x = & x(x-1) & (x^2+x+1) & (x^3+x+1)(x^3+x^2+1) & (x^6+x+1)\ldots \end{array}$$

das Produkt aller normierten, irreduziblen Polynome vom Grad d *mit* $d \mid 1, 2, 3, 6$.

6.8.4 Die Automorphismengruppe eines endlichen Körpers

Bemerkung 6.8.20 *Jeder Automorphismus* $\varphi \in \mathrm{Aut}(K)$ *eines Körpers* K *ist ein* $P(K)$*-Automorphismus, d.h. er ist auf dem Primkörper die Identität*

$$\varphi|_{P(K)} = \mathrm{id}_{P(K)}$$

Beweis. Zunächst

$$\varphi(1) = 1$$

also für $a \in \mathbb{Z}$

$$\varphi(a \cdot 1) = a \cdot 1$$

Falls $P(K) = \mathbb{F}_p = \mathbb{Z}/p$ folgt die Behauptung, denn $a \cdot 1 = \overline{a}$.

Für $P(K) = \mathbb{Q}$ gilt

$$\varphi\left(\frac{p}{q}\right) = \frac{\varphi(p)}{\varphi(q)} = \frac{p}{q}$$

■

In Definition und Satz 6.8.2 hatten wir gesehen, dass für einen endlichen Körper K der Charakteristik p der Frobeniushomomorphismus

$$\begin{array}{rccc} F: & K & \to & K \\ & b & \mapsto & b^p \end{array}$$

ein Automorphismus ist. Wir beschreiben nun die Gruppe $\mathrm{Aut}(K)$ aller Automorphismen von K:

Satz 6.8.21 *Sei K ein Körper mit p^r Elementen, p prim. Dann ist $\mathrm{Aut}(K)$ zyklisch der Ordnung $|\mathrm{Aut}(K)| = r$ und der Frobenius F ein Erzeuger, d.h.*

$$\mathrm{Aut}(K) = \langle F \rangle$$

Beweis. Mit Satz 6.8.8 ist $K^\times = \langle \alpha \rangle$ zyklisch. Somit hat $F \in \mathrm{Aut}(K)$ die Ordnung r, denn

$$F^r(\alpha) = \alpha^{p^r} = \alpha$$

und

$$F^j(\alpha) = \alpha^{p^j} \neq \alpha$$

für $j = 1, ..., r-1$, und ein Automorphismus ist durch sein Bild von α eindeutig festgelegt. Somit ist $\langle F \rangle \subset \mathrm{Aut}(K)$ eine zyklische Untergruppe der Ordnung r. Wir zeigen Gleichheit:

Nach dem Beweis von Corollar 6.8.9 gilt

$$K = \mathbb{F}_p(\alpha)$$

und das Minimalpolynom m_α hat Grad $\deg(m_\alpha) = [K : \mathbb{F}_p] = r$.

Da $F|_{\mathbb{F}_p} = \mathrm{id}_{\mathbb{F}_p}$, sind mit α auch alle $F^j(\alpha)$, $j = 1, ..., r$ Nullstellen von m_α, d.h.

$$m_\alpha = \prod_{j=1}^{r} \left(x - F^j(\alpha)\right)$$

Sei nun $\varphi \in \mathrm{Aut}(K)$. Da $\varphi|_{\mathbb{F}_p} = \mathrm{id}_{\mathbb{F}_p}$ ist mit α auch $\varphi(\alpha)$ eine Nullstelle von m_α, also gibt es ein j mit

$$\varphi(\alpha) = F^j(\alpha)$$

und damit

$$\varphi = F^j$$

■

6.8.5 Die Galoiskorrespondenz

Im Folgenden werden wir für eine Körpererweiterung $K \subset L$ (in unserem Fall von endlichen Körpern) eine Korrespondenz der Zwischenkörper und den Untergruppen der Gruppe der K-Automorphismen von L herleiten. Diese Konzepte gehen auf Évariste Galois zurück, der sie zur Untersuchung der Lösungen von algebraischen Gleichungen verwendet hat.

Wir reformulieren Definition 6.6.3 für Körpererweiterungen:

Definition 6.8.22 *Ist $K \subset L$ eine Körpererweiterung, dann heißt die Untergruppe*

$$\mathrm{Aut}\,(K \subset L) = \{\varphi \in \mathrm{Aut}\,(L) \mid \varphi\,|_K = \mathrm{id}_K\}$$

die ***Gruppe der relativen Automorphismen*** *oder* ***Galoisgruppe*** *von $K \subset L$.*

Andere gebräuchliche Schreibweisen sind $\mathrm{Aut}_K\,(L)$, $\mathrm{Aut}\,(L/K)$ oder $\mathrm{Gal}\,(L/K)$.

Damit können wir Bemerkung 6.8.20 auch formulieren als

$$\mathrm{Aut}\,(P\,(K) \subset K) = \mathrm{Aut}\,(K)$$

Die Korrespondenzen aus Satz 5.4.3 und 6.8.14 dehnen sich direkt auf Zwischenkörper einer Erweiterung endlicher Körper aus:

Bemerkung 6.8.23 *Sei $K \subset L$ eine Erweiterung endlicher Körper, also $K = \mathbb{F}_q$ und $L = \mathbb{F}_{q^n}$ (mit einer Primpotenz $q = p^r$). Man erhält den Unterkörper K als Fixkörper*

$$K = \mathrm{Fix}\,(F_q)$$

des Automorphismus

$$\begin{array}{rccc} F_q: & L & \to & L \\ & b & \mapsto & b^q \end{array}$$

(d.h. von $F^r = F_q$). Dieser heißt auch ***relativer Frobenius****, er erzeugt die relative Automorphismengruppe*

$$\mathrm{Aut}\,(K \subset L) = \langle F_q \rangle$$

und hat Ordnung

$$|\mathrm{Aut}\,(K \subset L)| = [L : K] = n$$

Beweis. Die Abbildung F_q ist die r-te Potenz

$$F_q = F^r$$

des Frobenius $F : L \to L$, $b \mapsto b^p$. Satz 6.8.14 gibt $K = \mathbb{F}_{p^r} = \operatorname{Fix}(F^r)$.

Nach Satz 6.8.21 wird $\operatorname{Aut}(L) = \langle F \rangle$ zyklisch von F erzeugt, also die Untergruppe $\operatorname{Aut}(K \subset L)$ von einer Potenz von F, wir untersuchen welche: Mit Bemerkung 6.8.15 gibt es ein $\alpha \in L$, sodass

$$L^\times = \langle \alpha \rangle \quad \text{und} \quad K^\times = \langle \beta \rangle \quad \text{mit} \quad \beta = \alpha^{(p^{rn}-1)/(p^r-1)}$$

und $\operatorname{ord} \beta = p^r - 1$. Somit ist $F^j \notin \operatorname{Aut}(K \subset L)$ für $j < r$ und $F^r \in \operatorname{Aut}(K \subset L)$, d.h.

$$\operatorname{Aut}(K \subset L) = \langle F^r \rangle$$

■

Bemerkung 6.8.24 *Weiter erhalten wir eine Bijektion*

$$\begin{array}{ccc} \{\text{Teiler von } n\} & \rightleftarrows & \{\text{Zwischenkörper von } K \subset L\} \\ s & \mapsto & \operatorname{Fix}\left(F_q^s\right) \cong \mathbb{F}_{q^s} \end{array}$$

denn $q^n = p^{rn}$, und mit Satz 6.8.14 entsprechen die Zwischenkörper den Teilern von nr, die Vielfache von r sind.

Da $\operatorname{Aut}(K \subset L) = \langle F_q \rangle = \langle F^r \rangle$ zyklisch der Ordnung

$$|\operatorname{Aut}(K \subset L)| = [L : K] = n$$

ist, gibt Satz 5.4.3 eine Bijektion

$$\begin{array}{ccc} \{\text{Teiler von } n\} & \rightleftarrows & \{\text{Untergruppen von } \operatorname{Aut}(K \subset L)\} \\ s & \mapsto & \left\langle F_q^s \right\rangle \end{array}$$

Beide Bijektionen zusammen ergeben eine Korrespondenz der Untergruppen und Zwischenkörper:

Definition 6.8.25 *Sei $K \subset L$ eine Erweiterung endlicher Körper. Ist $U \subset \operatorname{Aut}(L)$ eine Untergruppe, dann heißt*

$$\operatorname{Fix}(U) := \{a \in L \mid \varphi(a) = a \ \forall \varphi \in U\}$$

***Fixkörper** von U, und für einen Zwischenkörper $K \subset M \subset L$*

$$\operatorname{Fix}(M) := \operatorname{Aut}(M \subset L)$$

***Fixgruppe** von M.*

Satz 6.8.26 *Ist $K \subset L$ eine Erweiterung endlicher Körper, dann ist durch*

$$\begin{array}{ccc} \left\{ \begin{array}{c} \textit{Untergruppen} \\ \textit{von } \operatorname{Aut}(K \subset L) \end{array} \right\} & \rightleftarrows & \left\{ \begin{array}{c} \textit{Zwischenkörper} \\ \textit{von } K \subset L \end{array} \right\} \\ U & \mapsto & \operatorname{Fix}(U) \\ \operatorname{Fix}(M) & \hookleftarrow & M \end{array}$$

eine Bijektion gegeben. Für jeden Zwischenkörper $K \subset M \subset L$ gilt

$$\frac{\operatorname{Aut}(K \subset L)}{\operatorname{Aut}(M \subset L)} \cong \operatorname{Aut}(K \subset M)$$

Das heißt, die Quotientengruppe der relativen Automorphismen von L über K nach den Automorphismen über M gibt die relative Automorphismengruppe von M über K. Da $|\operatorname{Aut}(K \subset L)| = [L : K]$ impliziert diese Beziehung die Gradformel für Körpererweiterungen.

Eine vergleichbare Korrespondenz gibt es in allgemeinerer Form auch für nicht-endliche Körper.

Beweis. Sei $K = \mathbb{F}_q$ und $L = \mathbb{F}_{q^n}$ und

$$\operatorname{Aut}(\mathbb{F}_q \subset \mathbb{F}_{q^n}) = \langle F_q \rangle$$

(also $\operatorname{ord} F_q = [\mathbb{F}_{q^n} : \mathbb{F}_q] = n$). Wir haben oben schon gesehen, dass

$$\begin{array}{ccc} \{\text{Untergruppen von } \langle F_q \rangle\} & \rightleftarrows & \{\text{Zwischenkörper von } \mathbb{F}_q \subset \mathbb{F}_{q^n}\} \\ \left\langle F_q^s \right\rangle & \mapsto & \operatorname{Fix}\left(F_q^s\right) \cong \mathbb{F}_{q^s} \end{array}$$

wobei $s \mid n$ eine Bijektion ist. Bemerkung 6.8.23 zeigt, dass die Fixkörper- und Fixgruppenabbildungen zueinander invers sind, insbesondere

$$\operatorname{Aut}(\mathbb{F}_{q^s} \subset \mathbb{F}_{q^n}) = \left\langle F_q^s \right\rangle$$

Für den Quotienten gilt

$$\frac{\operatorname{Aut}(\mathbb{F}_q \subset \mathbb{F}_{q^n})}{\operatorname{Aut}(\mathbb{F}_{q^s} \subset \mathbb{F}_{q^n})} = \frac{\langle F_q \rangle}{\left\langle F_q^s \right\rangle} \cong \frac{\mathbb{Z}/n\mathbb{Z}}{s\mathbb{Z}/n\mathbb{Z}} \cong \frac{\mathbb{Z}}{s\mathbb{Z}} \cong \operatorname{Aut}(\mathbb{F}_q \subset \mathbb{F}_{q^s})$$

■

Beispiel 6.8.27 *Wir beschreiben die Galoiskorrespondenz für die Körpererweiterung*

$$\mathbb{F}_{2^2} \subset \mathbb{F}_{2^{12}}$$

d.h. $q = 2^2$ *und* $n = 6$. *Die Zwischenkörper entsprechen den Teilern von* $12 = 2^2 \cdot 3$, *die ihrerseits von* 2 *geteilt werden, also*

$$\mathbb{F}_{4096} = \mathrm{Fix}\left(F_4^6\right) = \mathrm{Fix}\left(F_{4096}\right)$$

$$\mathbb{F}_{16} = \mathrm{Fix}\left(F_4^2\right) = \mathrm{Fix}\left(F_{16}\right) \qquad \mathbb{F}_{64} = \mathrm{Fix}\left(F_4^3\right) = \mathrm{Fix}\left(F_{64}\right)$$

$$\mathbb{F}_4 = \mathrm{Fix}\left(F_4\right) = \mathrm{Fix}\left(F_4\right)$$

In Termen des Frobenius F *geschrieben gilt für* $s \mid 6$

$$\mathbb{F}_{2^{2s}} = \mathrm{Fix}\left(F_4^s\right) = \mathrm{Fix}\left(F_{2^{2s}}\right) = \mathrm{Fix}\left(F^{2s}\right)$$

Siehe auch Abbildung 6.2.

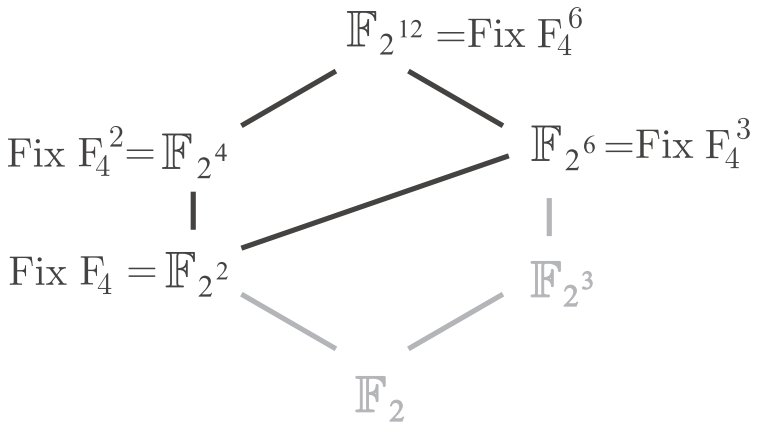


Abbildung 6.2: Galoiskorrespondenz für die Zwischenkörper von $\mathbb{F}_{2^2} \subset \mathbb{F}_{2^{12}}$

6.9 Übungen

Übung 6.1 *Sei* $K = \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$.

1) Zeigen Sie, dass $\sqrt{3} \notin \mathbb{Q}\left(\sqrt{2}\right)$.

2) *Folgern Sie* $[K : \mathbb{Q}] = 4$.

3) *Zeigen Sie* $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) = \mathbb{Q}\left(\sqrt{2} + \sqrt{3}\right)$.

4) *Bestimmen Sie das Minimalpolynom* $f \in \mathbb{Q}[x]$ *von* $\sqrt{2} + \sqrt{3}$.

5) *Bestimmen Sie alle Nullstellen von* f.

Übung 6.2 *Sei* $K \subset K[\alpha]$ *eine algebraische Körpererweiterung und* $g \in K[x]$ *das Minimalpolynom von* α.

1) *Geben Sie ein Verfahren an, um das Inverse* β^{-1} *von* $0 \neq \beta \in K[\alpha]$ *zu berechnen.*

2) *Bestimmen Sie das Inverse von*

$$\left(\sqrt{2} + \sqrt{3}\right)^2 + \sqrt{2} + \sqrt{3} \in \mathbb{Q}\left[\sqrt{2}, \sqrt{3}\right]$$

und machen Sie die Probe.

Übung 6.3 *Sei* $K \subset L$ *eine Körpererweiterung und* $a \in L$ *ein über* K *transzendentes Element.*

Zeigen Sie, dass die Körpererweiterung $K \subset K(a)$ *unendlich viele Zwischenkörper besitzt.*

Übung 6.4 *Seien* $K \subset L \subset M$ *Körpererweiterungen. Zeigen Sie*

$$K \subset M \text{ algebraisch} \iff K \subset L \text{ und } L \subset M \text{ algebraisch}$$

Übung 6.5 *Sei* $K \subset L$ *eine Körpererweiterung und* A *die Menge der über* K *algebraischen Elemente von* L. *Zeigen Sie:*

1) A *ist ein Zwischenkörper von* $K \subset L$.

2) *Die Körpererweiterung* $K \subset A$ *ist algebraisch.*

3) *Ist* $a \in L$ *algebraisch über* A, *dann schon über* K.

4) *War* L *algebraisch abgeschlossen, dann ist* A *der algebraische Abschluss von* K.

Übung 6.6 *1) Sei $\overline{\mathbb{Q}} \subset \mathbb{C}$ der Körper der algebraischen Zahlen. Zeigen Sie, dass $\overline{\mathbb{Q}}$ abzählbar ist.*

2) Sei $\mathbb{F}$ ein endlicher Körper und $\overline{\mathbb{F}} \supset \mathbb{F}$ eine algebraische Körpererweiterung von $\mathbb{F}$ zu einem algebraisch abgeschlossenen Körper $\overline{\mathbb{F}}$. Zeigen Sie, dass $\overline{\mathbb{F}}$ abzählbar unendlich ist.

Übung 6.7 *Sei K ein Körper und $f \in K[x]$. Zeigen Sie:*

1) Ist $\deg(f) = 1$, dann ist f irreduzibel.

2) Falls $\deg(f) \geq 2$ und f eine Nullstelle in K hat, dann ist f reduzibel über K.

3) Für $\deg(f) = 2$ oder 3 gilt: f hat keine Nullstelle in $K \Leftrightarrow$ f ist irreduzibel über K.

4) Geben Sie ein Gegenbeispiel für die Aussage in (3) für $\deg(f) = 4$.

5) Bestimmen Sie alle normierten, irreduziblen Polynome vom Grad ≤ 3 in $\mathbb{F}_2[x]$.

Übung 6.8 *1) Sei $\mathbb{F}_4$ ein Körper mit 4 Elementen. Zeigen Sie, dass*

$$\mathbb{F}_4 \cong \mathbb{F}_2[x] / \left(x^2 + x + 1\right)$$

2) Bestimmen Sie induktiv alle irreduziblen normierten Polynome vom Grad 2 in $\mathbb{F}_3[x]$.

3) Ist $\mathbb{F}_3[x]/(x^2+1)$ isomorph zu $\mathbb{F}_3[y]/(y^2+y-1)$?

Übung 6.9 *Betrachten Sie das Polynom*

$$f = x^9 - x \in \mathbb{F}_3[x]$$

mit Koeffizienten in dem Körper $\mathbb{F}_3 = \mathbb{Z}/3$ mit 3 Elementen.

1) Zerlegen Sie f in irreduzible Faktoren $f_i \in \mathbb{F}_3[x]$.

2) Bestimmen Sie zu jedem Faktor f_i die Nullstellen in $\mathbb{F}_9 \cong \mathbb{F}_3[x]/(x^2+1)$.

Übung 6.10 *1) Bestimmen Sie alle Unterkörper von $\mathbb{F}_{2^{36}}$ und die Inklusionsbeziehungen zwischen diesen.*

2) Beschreiben Sie die Körpererweiterung $\mathbb{F}_4 \subset \mathbb{F}_{16}$ als

$$\mathbb{F}_{16} = \mathbb{F}_4[y]/(g)$$

mit $g \in \mathbb{F}_4[y]$ irreduzibel.

Übung 6.11 *Schreiben Sie (z.B. in Maple) jeweils eine Funktion, die*

1) induktiv alle normierten, irreduziblen Polynome vom Grad $r \in \mathbb{N}$ in $\mathbb{F}_p[x]$ aufzählt.

2) für ein gegebenes normiertes irreduzibles $f \in \mathbb{F}_p[x]$ vom Grad r die Elemente von $\mathbb{F}_{p^r} \cong \mathbb{F}_p[x]/(f)$ bestimmt, d.h. für jedes Element seinen Repräsentanten vom Grad $< r$.

3) auf der Menge dieser Repräsentanten die Addition, Multiplikation und Bildung des Inversen implementiert.

4) alle zyklischen Erzeuger von $\mathbb{F}_{p^r}^\times$ bestimmt, d.h. alle $q \in \mathbb{F}_{p^r}^\times$ mit $\mathbb{F}_{p^r}^\times = \langle q \rangle$.

Hinweis: Maple-Funktionen `Irreduc`, `Rem`, `Gcdex`, `mod`.

Übung 6.12 *Sei*

$$f = x^5 - x^4 - 6x^3 + 6x^2 - 3x + 3$$

Bestimmen Sie über $\mathbb{F}_5$ und $\mathbb{F}_{13}$ jeweils die Primfaktorzerlegung und die Ordnung des Zerfällungskörpers von f.

Übung 6.13 *Sei $K = \mathbb{F}_3$, $L = \mathbb{F}_3[x]/\langle x^3 - x + 1 \rangle$ und $a = \overline{x}^2 + \overline{x} + 1 \in L$. Bestimmen Sie das Minimalpolynom von a über K und geben Sie für alle Automorphismen von L über K das Bild von a an.*

Übung 6.14 *Wieviele Elemente $a \in \mathbb{F}_{4096}$ gibt es, sodass $\mathbb{F}_{4096} = \mathbb{F}_2[a]$?*

7

Quadratische Reste

7.1 Übersicht

In diesem Kapitel wollen wir uns mit der Lösbarkeit von Gleichungen der Form

$$x^2 \equiv a \bmod p$$

mit p prim und $a \in \mathbb{Z}$ beschäftigen, also (für $p \nmid a$, anderenfalls ist $x = 0$ eine Lösung) mit der Frage, wann $\overline{a}$ ein Quadrat in $\mathbb{F}_p^\times$ ist. Diese Eigenschaft werden wir im Legendre-Symbol kodieren und einen Algorithmus zu dessen Berechnung entwickeln. Hier spielen natürlich Aussagen über endliche Körper eine entscheidende Rolle.

Zunächst wollen wir aber mit Anwendungen motivieren, warum es interessant ist zu entscheiden, ob $\overline{a} \in \mathbb{F}_p^\times$ ein Quadrat ist.

7.2 Die Anzahl der Punkte einer elliptischen Kurve über $\mathbb{F}_p$

In Beispiel 3.5.9 hatten wir elliptische Kurven, gegeben als Nullstellenmenge von Grad 3 Polynomgleichungen in zwei Variablen, kennengelernt. Wir hatten in geometrischer Weise den Punkten einer elliptischen Kurve die Struktur einer abelschen Gruppe gegeben (wobei noch die Punkte im Unendlichen hinzugefügt werden müssen, d.h. die Kurve liegt eigentlich im projektiven Raum $\mathbb{P}^2$). Abbildung 3.4 zeigt eine elliptische Kurve $E(\mathbb{R})$ in der Ebe-

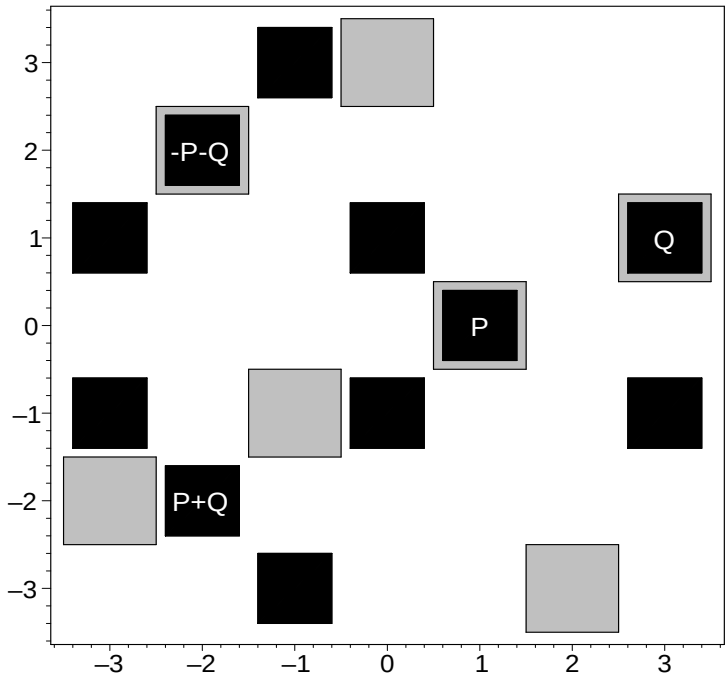


Abbildung 7.1: Elliptische Kurve über $\mathbb{F}_7$

ne $\mathbb{R}^2$ und Abbildung 3.5 die Konstruktion der Summe von zwei Punkten.

Ebenso können wir eine kubische Gleichung in $\mathbb{F}_p[x,y]$ betrachten und erhalten eine elliptische Kurve $E(\mathbb{F}_p)$ in $\mathbb{F}_p^2$, also eine endliche abelsche Gruppe.

Man kann zeigen, dass sich (für $p \geq 5$) in geeigneten Koordinaten jede Kurve als

$$E(\mathbb{F}_p) = \left\{(x,y) \in \mathbb{F}_p^2 \mid f(x,y) = 0\right\} \cup \{O\}$$

schreiben lässt mit einem Polynom

$$f = \left(x^3 + a \cdot x + b\right) - y^2 \in \mathbb{F}_p[x,y]$$

mit $4a^3+27b^2 \neq 0$ und dem Punkt im Unendlichen O, der auf jeder Geraden parallel zur y-Achse liegt und das neutrale Element der Gruppenverknüpfung ist.

In Abbildung 7.1 sind in schwarz die Punkte der Kurve

$$x^3 - 2x + 1 - y^2 = 0$$

über $\mathbb{F}_7$ markiert (wobei y nach oben aufgetragen ist). Weiter sind in grau die Punkte der Geraden

$$x - 2y - 1 = 0$$

durch zwei Punkte $P, Q \in E(\mathbb{F}_7)$ eingezeichnet. Die Summe $P+Q$ erhält man als Reflektion des dritten Schnittpunkts $-(P+Q)$ der Geraden mit der Kurve.

Man beachte: Löst man die lineare Geradengleichung nach einer Variablen auf, z.B.

$$x = 2y + 1$$

und setzt diese in f ein, erhält man ein Polynom von Grad 3 in einer Variablen

$$y^3 + 4y^2 + 2y = 0$$

das 3 Nullstellen $y = 0, 1, 2$ entsprechend den 3 Schnittpunkten besitzt (mit Vielfachheit und projektiv). Diese Aussage wird (allgemeiner) auch als der Satz von Bezout bezeichnet.

Als Anwendung kann man zum Beispiel in Public-Key Kryptosystemen statt $\mathbb{F}_p^\times$ eine Gruppe $E(\mathbb{F}_p)$ verwenden, was in der Praxis bei gleicher Sicherheit zu wesentlich kürzeren Schlüsseln führt. Es gibt auch ein Analogon zur Pollard-Faktorisierung. In diesem Zusammenhang ist es natürlich von Interesse, die Gruppenordnung, d.h. die Anzahl der Punkte von $E(\mathbb{F}_p)$, zu bestimmen. Um die Punkte zu zählen, müssen wir also entscheiden, ob $x^3 + a \cdot x + b$ für gegebenes $x \in \mathbb{F}_p$ ein Quadrat ist:

Definition 7.2.1 *Sei p eine ungerade Primzahl. Das* ***Legendre-Symbol*** *ist für $a \in \mathbb{Z}$ definiert durch*

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{für} \quad \overline{a} \in \left(\mathbb{F}_p^\times\right)^2 \\ -1 & \text{für} \quad \overline{a} \in \mathbb{F}_p^\times \setminus \left(\mathbb{F}_p^\times\right)^2 \\ 0 & \text{für} \quad \overline{a} = 0 \text{ d.h. } p \mid a \end{cases}$$

Dabei bezeichnet $\left(\mathbb{F}_p^\times\right)^2 = \left\{\overline{a}^2 \mid \overline{a} \in \mathbb{F}_p^\times\right\}$ die Untergruppe der Quadrate.

Wir können äquivalent auch schreiben

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{für} \quad x^2 \equiv a \bmod p \text{ lösbar und } p \nmid a \\ -1 & \text{für} \quad x^2 \equiv a \bmod p \text{ nicht lösbar} \\ 0 & \text{für} \quad \overline{a} = 0 \text{ d.h. } p \mid a \end{cases}$$

Im Fall $\left(\frac{a}{p}\right) = 1$ *heißt* a ***quadratischer Rest modulo p.***

Bemerkung 7.2.2 *Für* $p = 2$ *ist die Gleichung*

$$x^2 \equiv a \bmod 2$$

immer lösbar (mit $x = 0$ *für* $2 \mid a$ *bzw.* $x = 1$ *für* $2 \nmid a$*, denn* $-1 = 1 \in \mathbb{F}_2$*).*

Zurück zu der elliptischen Kurve: Mit dem Legendre-Symbol gilt für gegebenes $x \in \mathbb{F}_p$

$$\left(\frac{x^3 + a \cdot x + b}{p}\right) = \begin{cases} 1 & \Leftrightarrow \text{es gibt 2 Punkte } (x, -) \in E(\mathbb{F}_p) \\ -1 & \Leftrightarrow \text{es gibt 0 Punkte } (x, -) \in E(\mathbb{F}_p) \\ 0 & \Leftrightarrow \text{es gibt 1 Punkte } (x, -) \in E(\mathbb{F}_p) \end{cases}$$

das heißt, es existieren genau

$$1 + \left(\frac{x^3 + a \cdot x + b}{p}\right)$$

Punkte der Form $(x, -) \in E(\mathbb{F}_p)$. Summieren liefert folgenden Satz (wobei wir den unendlich fernen Punkt O nicht vergessen dürfen):

Satz 7.2.3 *Auf der elliptischen Kurve*

$$E(\mathbb{F}_p) = \left\{(x, y) \in \mathbb{F}_p^2 \mid x^3 + a \cdot x + b = y^2\right\} \cup \{O\}$$

gibt es genau

$$|E(\mathbb{F}_p)| = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + a \cdot x + b}{p}\right)$$

Punkte.

Mit dieser Formel sehen wir sofort

$$1 \leq |E(\mathbb{F}_p)| \leq 2p + 1$$

Präziser gilt folgender Satz (den wir hier nicht beweisen können):

Satz 7.2.4 (Hasse) *Für eine elliptische Kurve* $E(\mathbb{F}_p)$ *gilt*

$$p + 1 - 2\sqrt{p} \leq |E(\mathbb{F}_p)| \leq p + 1 + 2\sqrt{p}$$

Man kann zeigen, dass alle möglichen Werte auch tatsächlich angenommen werden.

7.3 Das Legendre-Symbol

Wir wollen uns nun mit der Berechnung des Legendre-Symbols beschäftigen, zunächst einige offensichtliche, aber sehr nützliche Rechenregeln:

Bemerkung 7.3.1 *Für p ungerade prim und $a, b \in \mathbb{Z}$ gilt*

1) $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ *falls* $a \equiv b \bmod p$
   Das heißt, wir können a modulo p reduzieren.

2) $\left(\frac{a^2 \cdot b}{p}\right) = \left(\frac{b}{p}\right)$ *falls* $p \nmid a$.
   Das heißt, wir können Quadrate streichen.

Beweis. Die Aussage (1) ist klar. Zu (2): Für $p \mid b$ sind beide Seiten 0, sonst

$$\overline{a}^2 \overline{b} \in \left(\mathbb{F}_p^\times\right)^2 \Leftrightarrow \overline{b} \in \left(\mathbb{F}_p^\times\right)^2$$

denn $\overline{a}^2 \in \left(\mathbb{F}_p^\times\right)^2$. ∎

Der folgende Satz erlaubt es, das Legendre-Symbol mittels Potenzieren modulo p zu berechnen, und gibt somit eine schnelle Methode, um mit dem Computer $\left(\frac{a}{p}\right)$ auszuwerten. Ein weiteres Verfahren werden wir in Übung 7.3 kennenlernen.

Satz 7.3.2 (Euler-Kriterium) *Sei p eine ungerade Primzahl und $a \in \mathbb{Z}$. Dann gilt*

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p$$

insbesondere

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$$

Beweis. Die Behauptung ist klar, wenn $p \mid a$. Wenn $\mathrm{ggT}(a, p) = 1$ ist, dann gibt der kleine Satz von Fermat

$$a^{p-1} \equiv 1 \bmod p$$

also

$$a^{\frac{p-1}{2}} \equiv \pm 1 \bmod p$$

denn $\overline{1}$ und $\overline{-1}$ sind die beiden Nullstellen von $x^2 - 1 \in \mathbb{F}_p[x]$.

Wir untersuchen noch, wann der Wert 1 oder -1 angenommen wird:

Sei $g \in \mathbb{F}_p^\times$ ein zyklischer Erzeuger. Dann

$$\begin{aligned}\left(\frac{a}{p}\right) = -1 &\iff \overline{a} \in \mathbb{F}_p^\times \text{ ist kein Quadrat} \\ &\iff \overline{a} = g^{2k+1} \text{ ist eine ungerade Potenz} \\ &\iff \overline{a}^{\frac{p-1}{2}} = \left(g^{2k+1}\right)^{\frac{p-1}{2}} = g^{k(p-1)+\frac{p-1}{2}} = g^{\frac{p-1}{2}} = -1\end{aligned}$$

■

Praktisch kann man $a^{\frac{p-1}{2}} \bmod p$ durch Potenzieren modulo p sehr schnell auswerten. Aus Satz 7.3.2 erhalten wir sofort:

Corollar 7.3.3 *Sei p eine ungerade Primzahl. Für alle $a, b \in \mathbb{Z}$ gilt*

$$\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

(Man beachte, dass die Aussage für $p \mid ab$ klar ist). Dies können wir auch wie folgt formulieren:

Bemerkung 7.3.4 *Sind a und b quadratische Reste modulo p, dann auch $a \cdot b$.*

Ist a ein quadratischer Rest und b ein Nichtrest, dann ist auch $a \cdot b$ ein Nichtrest.

Angenommen p teilt a und b nicht. Sind a und b Nichtreste, dann ist $a \cdot b$ ein quadratischer Rest.

Mit Corollar 7.3.3 sehen wir nochmals Bemerkung 7.3.1(2). Weiter folgt auch:

Corollar 7.3.5 *Die Abbildung*

$$\begin{array}{ccc}\mathbb{F}_p^\times & \to & \{-1, +1\} \\ \overline{a} & \mapsto & \left(\frac{a}{p}\right)\end{array}$$

ist ein Gruppenhomomorphismus mit Kern $\left(\mathbb{F}_p^\times\right)^2$, d.h.

$$\mathbb{F}_p^* / \left(\mathbb{F}_p^*\right)^2 \cong \{-1, +1\}$$

Entsprechend den Nebenklassen (siehe Satz 2.2.35) gibt es also jeweils genau $\frac{p-1}{2}$ Quadrate und Nichtquadrate.

Für die Berechnung des Legendre-Symbols (insbesondere von Hand) sind folgende Sätze nützlich, die auf Euler und Gauß zurückgehen:

Satz 7.3.6 (Quadratisches Reziprozitätsgesetz) *1) Sind p und q ungerade Primzahlen, dann gilt*

$$\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{p}{q}\right)$$

2) Ist p eine ungerade Primzahl, dann

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Daraus ergibt sich durch iteratives Anwenden (und Corollar 7.3.3) ein Algorithmus zur Berechnung des Legendre-Symbols, den wir vor dem Beweis zunächst erproben:

Beispiel 7.3.7 *Wir wollen entscheiden, ob*

$$x^2 \equiv 55 \bmod 103$$

eine Lösung hat. Dies ist der Fall, denn

$$\begin{aligned}\left(\frac{55}{103}\right) &= \left(\frac{5}{103}\right)\cdot\left(\frac{11}{103}\right) = -\left(\frac{103}{5}\right)\left(\frac{103}{11}\right)\\ &= -\left(\frac{3}{5}\right)\left(\frac{4}{11}\right) = -\left(\frac{5}{3}\right)\left(\frac{2}{11}\right)^2\\ &= -\left(\frac{2}{3}\right) = 1\end{aligned}$$

(da $(-1)^{\frac{102\cdot 4}{4}} = 1$ und $(-1)^{\frac{102\cdot 10}{4}} = -1$). Zur Berechnung haben wir Bemerkung 7.3.1 und Satz 7.3.6 verwendet.

Da für große Zahlen Primfaktorisierung aufwändig ist, führt man eine zusammengesetzte Version des Legendre-Symbols ein:

Definition 7.3.8 *Sei $n = p_1 \cdot \ldots \cdot p_r$ eine ungerade zusammengesetzte Zahl mit p_i prim und $a \in \mathbb{Z}$. Dann bezeichnet man*

$$\left(\frac{a}{n}\right) := \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)$$

*als das **Jacobi-Symbol**.*

Für n prim ist das Jacobi-Symbol natürlich das Legendre-Symbol.

Bemerkung 7.3.9 *Ist n ungerade prim, dann gilt*

$$\left(\frac{a}{n}\right) = -1 \Longleftrightarrow x^2 \equiv a \bmod n \text{ nicht lösbar}$$

Für n zusammengesetzt ist Vorsicht geboten: Sei

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{r} \left(\frac{a}{p_i}\right)$$

und einer der Faktoren

$$\left(\frac{a}{p_i}\right) = -1$$

Dann ist

$$x^2 \equiv a \bmod p_i$$

nicht lösbar, also erst recht die Gleichung

$$x^2 \equiv a \bmod n$$

nicht lösbar (denn eine Lösung modulo n ist auch eine modulo p_i). Insbesondere gilt

$$\left(\frac{a}{n}\right) = -1 \Longrightarrow x^2 \equiv a \bmod n \text{ nicht lösbar}$$

Finden Sie als Übung a und p, q prim mit

$$\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right) = -1$$

also $\left(\frac{a}{pq}\right) = 1$ und a kein Quadrat modulo $p \cdot q$.

Bemerkung 7.3.10 *Aus den entsprechenden Formeln für das Legendre-Symbol folgt sofort*

$$\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right) \text{ falls } a \equiv b \bmod n$$

und

$$\left(\frac{a \cdot b}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$$

Auch für das Jacobi-Symbol gilt Satz 7.3.6:

Corollar 7.3.11 *Sind $a, b > 0$ ungerade, dann*

$$\left(\frac{a}{b}\right) = (-1)^{\frac{(a-1)(b-1)}{4}} \left(\frac{b}{a}\right)$$

und

$$\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$$

Beweis. Sind $a = p_1 \cdot \ldots \cdot p_r$ und $b = q_1 \cdot \ldots \cdot q_s$, dann

$$\left(\frac{a}{b}\right) = \prod_{i,j} \left(\frac{p_i}{q_j}\right) = \prod_{i,j} (-1)^{\frac{(p_i-1)(q_j-1)}{4}} \left(\frac{q_j}{p_i}\right) = (-1)^{\frac{(a-1)(b-1)}{4}} \left(\frac{b}{a}\right)$$

wobei wir für die letzte Gleichheit noch

$$\prod_{i,j} (-1)^{\frac{(p_i-1)(q_j-1)}{4}} = (-1)^{\frac{(a-1)(b-1)}{4}}$$

zeigen müssen (wenn a und b einen gemeinsamen Faktor haben, ist die Aussage klar). Einerseits ist

$$(-1)^{\frac{(p_i-1)(q_j-1)}{4}} = \begin{cases} -1 & \text{für} \quad p_i \equiv q_j \equiv 3 \bmod 4 \\ 1 & \text{für} \quad p_i \equiv 1 \bmod 4 \text{ oder } q_j \equiv 1 \bmod 4 \end{cases}$$

also

$$\prod_{i,j} (-1)^{\frac{(p_i-1)(q_j-1)}{4}} = \begin{cases} -1 & \text{falls } a \text{ und } b \text{ eine ungerade Zahl} \\ & \text{von Faktoren} \equiv 3 \bmod 4 \text{ haben} \\ 1 & \text{sonst} \end{cases}$$

Andererseits gilt in $(\mathbb{Z}/4)^\times = \{\overline{1}, \overline{3}\}$, dass $\overline{3}^{2k} = \overline{1}$ $\forall k$, also

$a \equiv 3 \bmod 4 \Leftrightarrow a$ hat eine ungerade Zahl von Faktoren $\equiv 3 \bmod 4$

und somit folgt die Gleichheit.

Der Beweis des zweiten Teils funktioniert analog. ■

Bemerkung 7.3.12 *Damit erhalten wir einen schnellen Algorithmus um $\left(\frac{a}{b}\right)$ zu berechnen:*

1) Mit Bemerkung 7.3.10 erreicht man $a < b$.

2) Für a gerade zerlegen wir

$$\left(\frac{a}{b}\right) = \left(\frac{2}{b}\right)^k \left(\frac{c}{b}\right)$$

3) Mit Corollar 7.3.11(2) bestimme $\left(\frac{2}{b}\right)$.

4) Auf $\left(\frac{c}{b}\right)$ wenden wir das quadratische Reziprozitätsgesetz aus Corollar 7.3.11(1) an und iterieren den Prozess.

Beispiel 7.3.13 *Damit berechnen wir nochmals (einfacher)*

$$\begin{aligned}\left(\frac{55}{103}\right) &= -\left(\frac{103}{55}\right) = -\left(\frac{48}{55}\right) = -\left(\frac{2}{55}\right)^4 \left(\frac{3}{55}\right) \\ &= \left(\frac{55}{3}\right) = \left(\frac{1}{3}\right) = 1\end{aligned}$$

Beachte $1 = 1 \cdot 1$ ist immer ein Quadrat.

7.4 Beweis des quadratischen Reziprozitätsgesetzes

Wir zeigen nun Satz 7.3.6.

1) Sind p und q ungerade Primzahlen, dann gilt

$$\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{p}{q}\right)$$

2) Ist p eine ungerade Primzahl, dann

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

Beweis. Zunächst zur Aussage (2): Setze

$$f(n) := \begin{cases} (-1)^{\frac{n^2-1}{8}} & \text{für } n \text{ ungerade} \\ 0 & \text{sonst} \end{cases}$$

Wir wollen

$$f(p) = \left(\frac{2}{p}\right)$$

für p prim zeigen.

Die Einheitengruppe $\mathbb{F}_{p^2}^\times$ von $\mathbb{F}_{p^2}$ ist nach Satz 6.8.8 zyklisch. Schreiben wir $p = 2 \cdot k + 1$, dann

$$p^2 - 1 = (2 \cdot k + 1)^2 - 1 = 4 \cdot k \cdot (k + 1)$$

Da k oder $k + 1$ gerade ist, teilt $8 \mid (p^2 - 1)$ und somit enthält $\mathbb{F}_{p^2}^\times$ nach Satz 5.4.6 eine zyklische Untergruppe $\langle \xi \rangle$ der Ordnung $|\langle \xi \rangle| = 8$.

Wir betrachen nun die sogenannte Gaußsumme

$$G := \sum_{j=0}^{7} f(j)\, \xi^j = \xi - \xi^3 - \xi^5 + \xi^7$$

Wegen $\xi^4 = -1$ ist

$$G = 2\left(\xi - \xi^3\right)$$

und

$$G^2 = 4\left(\xi^2 - 2\xi^4 + \xi^6\right) = 4 \cdot 2 = 8 \neq 0 \in \mathbb{F}_p \subset \mathbb{F}_{p^2}$$

Damit muss aber auch

$$G \neq 0 \in \mathbb{F}_{p^2}$$

sein.

Wir schreiben nun G^p auf zwei verschiedene Weisen als Vielfaches von G:

- Mit dem Satz von Euler gilt

$$8^{\frac{p-1}{2}} = \left(\frac{8}{p}\right) \in \mathbb{F}_p \subset \mathbb{F}_{p^2}$$

  also

$$\begin{aligned} G^p &= \left(G^2\right)^{\frac{p-1}{2}} \cdot G = 8^{\frac{p-1}{2}} \cdot G \\ &= \left(\frac{8}{p}\right) G = \left(\frac{2}{p}\right)^3 G = \left(\frac{2}{p}\right) G \end{aligned}$$

- Andererseits ist der Frobenius ein Homomorphismus, d.h. $(x+y)^p = x^p + y^p$ in $\mathbb{F}_{p^2}$, also

$$G^p = \sum_{j=0}^{7} f(j)^p \xi^{j\cdot p} = \sum_{j=0}^{7} f(j)\,\xi^{j\cdot p}$$

(letzteres, da p ungerade). Für j ungerade gilt

$$\frac{f(pj)}{f(p)\,f(j)} = \frac{(-1)^{\frac{(pj)^2-1}{8}}}{(-1)^{\frac{p^2-1}{8}}\,(-1)^{\frac{j^2-1}{8}}} = (-1)^{\frac{(pj)^2-p^2-j^2+1}{8}} = (-1)^{(j^2-1)\frac{p^2-1}{8}} = 1$$

und (da f nur Werte ± 1 annimmt) auch $f(j) = f(p)\cdot f(pj)$. Damit ist

$$G^p = f(p)\cdot \sum_{j=0}^{7} f(j\cdot p)\,\xi^{j\cdot p} = f(p)\,G$$

da $f(a) = f(b)$, wenn $a \equiv b \bmod 8$.

Beide Rechnungen zusammen liefern

$$\left(\frac{2}{p}\right) = f(p) \in \mathbb{F}_{p^2}$$

also auch

$$\left(\frac{2}{p}\right) = f(p) \in \mathbb{Z}$$

■

Beweis. Wir zeigen nun (1):

Dazu betrachten wir $\mathbb{F}_{p^r}^\times$ für $r = q-1$. Mit dem kleinen Satz von Fermat gilt

$$p^r \equiv 1 \bmod q$$

also $q \mid (p^r - 1)$. Da $\mathbb{F}_{p^r}^\times$ zyklisch der Ordnung $p^r - 1$ ist, enthält $\mathbb{F}_{p^r}^\times$ eine Untergruppe $\langle \xi \rangle$ der Ordnung q.

Wir untersuchen jetzt G^p für die Gaußsumme

$$G := \sum_{j=0}^{q-1} \left(\frac{j}{q}\right) \xi^j = \sum_{j=10}^{q-1} \left(\frac{j}{q}\right) \xi^j$$

Angenommen es ist schon gezeigt, dass

$$G^2 = (-1)^{\frac{q-1}{2}}\, q \neq 0 \in \mathbb{F}_{p^r}$$

Man berechnet wieder G^p auf zwei verschiedene Weisen:

$$\begin{aligned} G^p &= \left(G^2\right)^{\frac{p-1}{2}} \cdot G = \left((-1)^{\frac{q-1}{2}} q\right)^{\frac{p-1}{2}} \cdot G \\ &= (-1)^{\frac{(q-1)(p-1)}{4}} \cdot \left(\frac{q}{p}\right) \cdot G \end{aligned}$$

Andererseits:

$$G^p = \sum_{j=0}^{q-1} \left(\frac{j}{q}\right) \xi^{jp} = \left(\frac{p}{q}\right) \sum_{j=0}^{q-1} \left(\frac{jp}{q}\right) \xi^{jp} = \left(\frac{p}{q}\right) \cdot G$$

da $\left(\frac{a}{q}\right) = \left(\frac{b}{q}\right)$ für $a \equiv b \bmod q$.

Bleibt noch

$$G^2 = (-1)^{\frac{q-1}{2}} q \neq 0 \in \mathbb{F}_{p^r}$$

zu zeigen. Da $\left(\frac{q-k}{q}\right) = \left(\frac{-k}{q}\right)$ und $\xi^{q-k} = \xi$ gilt

$$\begin{aligned} G^2 &= \left(\sum_{j=1}^{q-1} \left(\frac{j}{q}\right) \xi^j\right)^2 = \left(\sum_{j=1}^{q-1} \left(\frac{j}{q}\right) \xi^j\right) \cdot \left(\sum_{k=1}^{q-1} \left(\frac{-k}{q}\right) \xi^{-k}\right) \\ &= \left(\frac{-1}{q}\right) \sum_{j,k=1}^{q-1} \left(\frac{jk}{q}\right) \xi^{j-k} \overset{(i)}{=} \left(\frac{-1}{q}\right) \sum_{j,k=1}^{q-1} \left(\frac{j^2 k}{q}\right) \xi^{j-jk} \\ &= \left(\frac{-1}{q}\right) \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) \sum_{j=1}^{q-1} \xi^{j(1-k)} \overset{(ii)}{=} \left(\frac{-1}{q}\right) \sum_{k=1}^{q-1} \left(\frac{k}{q}\right) \sum_{j=0}^{q-1} \xi^{j(1-k)} \end{aligned}$$

Bei (i) haben wir verwendet, dass

$$\mathbb{Z}/q \to \mathbb{Z}/q,\ \overline{k} \mapsto \overline{jk}$$

bijektiv ist, da q prim. Die Gleichheit (ii) gilt, da es in $\mathbb{F}_q^\times$ genauso viele Quadrate wie Nichtquadrate gibt, also

$$\sum_{k=1}^{q-1} \left(\frac{k}{q}\right) = 0$$

Da $\xi \neq 1$, folgt aus

$$0 = \xi^q - 1 = (\xi - 1) \cdot \sum_{j=0}^{q-1} \xi^j$$

dass $\sum_{j=0}^{q-1} \xi^j = 0$ also

$$\sum_{j=0}^{q-1} \xi^{j(1-k)} = \begin{cases} 0 & \text{für} \quad k \neq 1 \\ q & \text{für} \quad k = 1 \end{cases}$$

und somit

$$G^2 = \left(\frac{-1}{q}\right)\left(\frac{1}{q}\right) \cdot q = \left(\frac{-1}{q}\right) \cdot q = (-1)^{\frac{q-1}{2}} q \neq 0$$

■

7.5 Übungen

Übung 7.1 *Bestimmen Sie das Jacobisymbol*

$$\left(\frac{455}{1236}\right)$$

und entscheiden Sie, ob die Gleichung $x^2 \equiv 455 \bmod 1236$ *lösbar ist. Beachten Sie:* $1236 = 2^2 \cdot 3 \cdot 103$.

Übung 7.2 *1) Berechnen Sie per Hand:*

$$\left(\frac{3}{97}\right), \ \left(\frac{5}{389}\right), \ \left(\frac{2003}{11}\right), \ \left(\frac{5!}{7}\right)$$

2) Zeigen Sie

$$\left(\frac{3}{p}\right) = \left\{ \begin{array}{ll} 1 & \textit{falls } p \equiv 1, 11 \ \textit{mod } 12 \\ -1 & \textit{falls } p \equiv 5, 7 \ \textit{mod } 12 \end{array} \right\}$$

3) Zeigen Sie

$$\left(\frac{-3}{p}\right) = \left\{ \begin{array}{lll} 1 & \textit{falls} & p \equiv 1 \bmod 3 \\ -1 & \textit{falls} & p \equiv -1 \bmod 3 \end{array} \right\}$$

Übung 7.3 *Sei* p *eine ungerade Primzahl und*

$$S = \left\{ -\frac{p-1}{2}, -\frac{p-1}{2} + 1, ..., -1, 1, ..., \frac{p-1}{2} - 1, \frac{p-1}{2} \right\}$$

Zu jedem $a \in \mathbb{Z}$ *mit* $p \nmid a$ *gibt es genau ein* $s \in S$ *mit* $a \equiv s \bmod p$.

Ist $a \in \mathbb{Z}$ *mit* $p \nmid a$, *dann sind* ε_n *und* s_n *für* $n = 1, ..., \frac{p-1}{2}$ *definiert durch*

$$na \equiv \varepsilon_n s_n \bmod p$$

mit $s_n \in S$, $s_n > 0$ *und* $\varepsilon_n \in \{1, -1\}$.

1) Bestimmen Sie $\varepsilon_1, ..., \varepsilon_5$ *und* $s_1, ..., s_5$ *für* $p = 11$ *und* $a = 2$.

2) Zeigen Sie:

$$\left(\frac{a}{p}\right) = \varepsilon_1 \cdot \ldots \cdot \varepsilon_{(p-1)/2}$$

3) Implementieren Sie damit die Berechnung des Legendre-Symbols, und erproben Sie Ihr Programm an den Beispielen aus Übung 7.2.

8

Konstruktionen mit Zirkel und Lineal

8.1 Übersicht

Bereits den alten Griechen waren die Konstruktionen des regelmäßigen n-Ecks für $n = 3, 4, 5, 6$ mit Zirkel und Lineal bekannt.

Abbildung 2.26 zeigt die Konstruktion des regelmäßigen 5-Ecks: Zunächst konstruieren wir zueinander senkrechte Geraden l und m durch den Mittelpunkt eines Kreises. Dann halbieren wir einen Radius, erhalten den Punkt Q, vierteln einen dazu senkrechten Radius und erhalten den Punkt P. Der Kreis mit Mittelpunkt P durch Q schneidet l im Punkt R. Ebenso schneidet eine Diagonale im 5-Eck dann l orthogonal in R. Siehe auch Übung 8.1.

Ob sich auch das regelmäßige 7-Eck so konstruieren lässt, blieb offen. Wir werden diese Frage in Übung 8.6 mit nein beantworten. Andere klassische Probleme sind die Dreiteilung eines Winkels, die Verdoppelung des Würfels und die Quadratur des Kreises.

Um diese Fragestellungen in die Algebra zu übersetzen, identifiziert man die Punkte der Ebene $(x, y) \in \mathbb{R}^2$ mit den komplexen Zahlen $x + i \cdot y \in \mathbb{C}$.

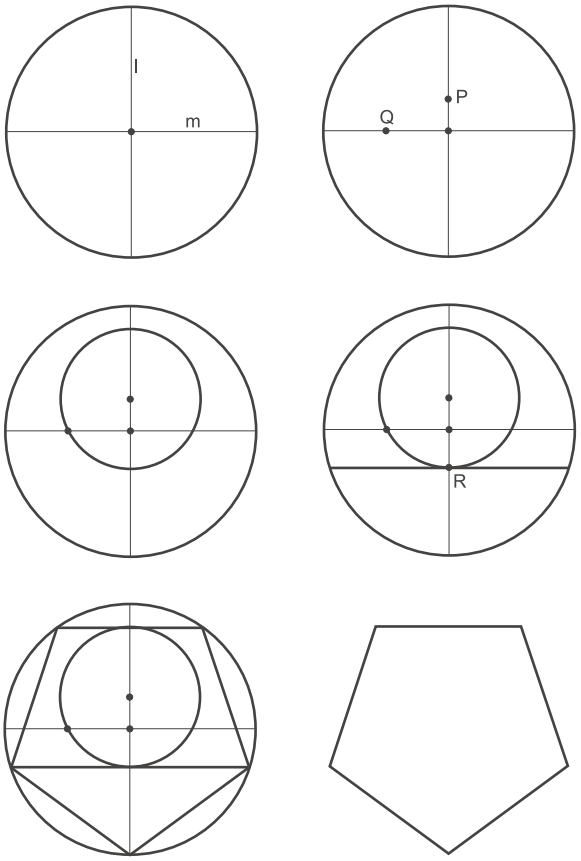


Abbildung 8.1: Konstruktion des regelmäßigen 5-Ecks

8.2 Elementare Konstruktionsschritte

Zu zwei Punkten $p, q \in \mathbb{C}$ bezeichne $\overline{pq}$ die Gerade durch p und q. Für $p \in \mathbb{C}$ sei $K(p, r)$ der Kreis mit Radius r um p.

Definition 8.2.1 *Für eine Teilmenge $M \subset \mathbb{C}$ definieren wir nun die **elementaren Konstruktionsschritte**, bei denen wir M durch $M \cup S$ ersetzen, wobei:*

Typ I. *Für $p_1, q_1, p_2, q_2 \in M$ mit $p_1 \neq q_1$, $p_2 \neq q_2$ und $\overline{p_1 q_1} \neq \overline{p_2 q_2}$*

$$S = \overline{p_1 q_1} \cap \overline{p_2 q_2}$$

Typ II. *Für $p, p_1, q_1, p_2, q_2, \in M$ mit $p_1 \neq q_1$*

$$S = \overline{p_1 q_1} \cap K(p, \|p_2 - q_2\|)$$

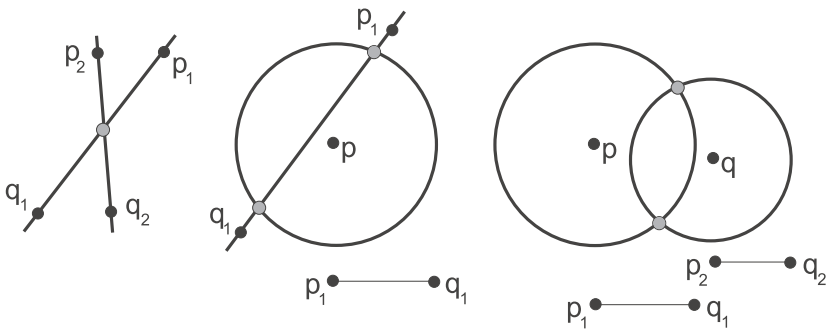


Abbildung 8.2: Elementare Konstruktionsschritte

Typ III. *Für* $p, q, p_1, q_1, p_2, q_2 \in M$ *mit* $p \neq q$

$$S = K\left(p, \|p_1 - q_1\|\right) \cap K\left(q, \|p_2 - q_2\|\right)$$

Siehe dazu auch Abbildung 8.2. In einem elementaren Konstruktionsschritt vergrößert sich M höchstens um 2 Punkte.

Definition 8.2.2 *Für eine beliebige Teilmenge* $M \subset \mathbb{C}$ *definieren wir* $\mathrm{Kon}(M)$ *als die Menge aller* $z \in \mathbb{C}$*, zu denen es ein* $n \in \mathbb{N}$ *und eine Kette*

$$M =: M_0 \subset M_1 \subset \ldots \subset M_{n-1} \subset M_n \subset \mathbb{C}$$

von Teilmengen gibt mit $z \in M_n$*, wobei* M_j *aus* M_{j-1} *für alle* j *durch einen elementaren Konstruktionsschritt entsteht. Wir bezeichnen* $\mathrm{Kon}(M)$ *als die Menge der aus* M ***mit Zirkel und Lineal konstruierbaren Punkte****.*

Um elementare Konstruktionsschritte anwenden zu können, muss M wenigstens zwei Punkte enthalten, ohne Einschränkung im Folgenden $0, 1 \in M$.

Satz 8.2.3 *Sei* $M \subset \mathbb{C}$ *mit* $0, 1 \in M$*. Dann ist* $\mathrm{Kon}(M) \subset \mathbb{C}$ *ein Unterkörper.*

Zum Beweis siehe Übung 8.2.

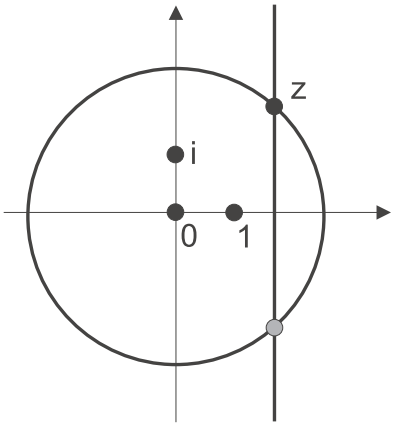


Abbildung 8.3: Konstruktion des komplex Konjugierten

Bemerkung 8.2.4 *Mit der Konstruktion in Abbildung 8.3 sehen wir*

$$z \in \mathrm{Kon}(M) \Longleftrightarrow \overline{z} \in \mathrm{Kon}(M)$$

also

$$z \in \mathrm{Kon}(M) \Longleftrightarrow \mathrm{Re}(z) \in \mathrm{Kon}(M) \text{ und } \mathrm{Im}(z) \in \mathrm{Kon}(M)$$

Bemerkung 8.2.5 *Die oben genannten Fragestellungen lassen sich dann wie folgt umformulieren:*

1) Konstruktion des n-Ecks

$$e^{\frac{2\pi i}{n}} \in \mathrm{Kon}(\{0,1\})$$

2) Dreiteilung des Winkels φ

$$e^{i\frac{\varphi}{3}} \in \mathrm{Kon}\left(\left\{0,1,e^{i\varphi}\right\}\right)$$

3) Verdoppelung des Würfels

$$\sqrt[3]{2} \in \mathrm{Kon}(\{0,1\})$$

4) Quadratur des Kreises

$$\sqrt{\pi} \in \mathrm{Kon}(\{0,1\})$$

Um die Lösbarkeit dieser Konstruktionsaufgaben zu entscheiden, verwenden wir die Theorie von algebraischen Körpererweiterungen.

Satz 8.2.6 *Sei $M \subset \mathbb{C}$ eine Teilmenge und $z \in \mathrm{Kon}(M)$. Dann ist die Körpererweiterung $\mathbb{Q}(M) \subset \mathbb{Q}(M,z)$ algebraisch und*

$$[\mathbb{Q}(M,z) : \mathbb{Q}(M)] = 2^r$$

eine 2-er Potenz.

Beweis. Ohne Einschränkung $\{0,1,i\} \subset M$. Sei

$$M = M_0 \subset M_1 \subset \ldots \subset M_n$$

eine Sequenz von elementaren Konstruktionsschritten mit

$$z \in M_n$$

Betrachte den Schritt $M_k \subset M_{k+1}$:

Typ I. Die Koordinaten $\mathrm{Re}(P)$ und $\mathrm{Im}(P)$ des Schnittpunkts P der beiden Geraden erhält man durch ein lineares Gleichungssystem über $\mathbb{Q}(M_k)$, also $\mathbb{Q}(M_k) = \mathbb{Q}(M_{k+1})$.

Typ II. Auflösen und Einsetzen der Geradengleichung in die Kreisgleichung liefert eine quadratische Gleichung $f \in \mathbb{Q}(M_k)[x]$ für den Realteil (oder den Imaginärteil) der beiden Schnittpunkte. Ist f reduzibel, dann $\mathbb{Q}(M_{k+1}) = \mathbb{Q}(M_k)$, anderenfalls $\mathbb{Q}(M_{k+1}) \cong \mathbb{Q}(M_k)[x]/(f)$, also

$$[\mathbb{Q}(M_{k+1}) : \mathbb{Q}(M_k)] = 2$$

Typ III. Die Schnittpunkte der beiden Kreise mit Mittelpunkten $a_j + i \cdot b_j \in M_k$ und Radius $r_j \in M_k$ sind durch das System

$$\begin{aligned}(x-a_1)^2 + (y-b_1)^2 &= r_1^2\\ (x-a_2)^2 + (y-b_2)^2 &= r_2^2\end{aligned}$$

gegeben, äquivalent durch

$$\begin{aligned}(x-a_1)^2 + (y-b_1)^2 &= r_1^2\\ 2(a_1-a_2)\cdot x + 2(b_1-b_2)\cdot y &= r_2^2 - r_1^2 + a_1^2 + b_1^2 - a_2^2 - b_2^2\end{aligned}$$

Da $(a_1,b_1) \neq (a_2,b_2)$, sind wir wieder in Fall II.

■

Eine hinreichende Bedingung für die Konstruierbarkeit von z aus M können wir hier nicht herleiten, dies ist Gegenstand der Galoistheorie (in Verallgemeinerung dessen, was wir in Abschnitt 6.8.5 für endliche Körper gelernt haben). Siehe auch Übungsaufgabe 8.5.

Corollar 8.2.7 *Die Verdoppelung des Würfels mit Zirkel und Lineal, d.h. Konstruktion von $\sqrt[3]{2}$ aus $\{0,1\}$ ist nicht möglich.*

Beweis. Das Minimalpolynom von $a = \sqrt[3]{2}$ über $\mathbb{Q}$ ist

$$m_a = x^3 - 2 \in \mathbb{Q}[x]$$

denn es hat Grad 3 und genau die reelle Nullstelle $a \notin \mathbb{Q}$, ist also irreduzibel. Somit gilt

$$\left[\mathbb{Q}\left[\sqrt[3]{2}\right] : \mathbb{Q}\right] = 3$$

Wäre a konstruierbar, dann gäbe es eine Körpererweiterung

$$\mathbb{Q} \subset \mathbb{Q}\left[\sqrt[3]{2}\right] \subset K$$

mit

$$[K : \mathbb{Q}] = 2^r$$

ein Widerspruch zum Gradsatz 6.2.4, da $3 \nmid 2^r$. ■

Für viele weitere Beispiele benötigt man ein tragfähiges Irreduzibilitätskriterium:

8.3 Irreduzibilität über dem Quotientenkörper

Die folgenden Argumente funktionieren völlig analog über einem beliebigen faktoriellen Ring R und seinem Quotientenkörper $Q(R)$. Um den Blick auf das Wesentliche nicht zu verstellen, beschränken wir uns im Folgenden auf den Fall $R = \mathbb{Z}$, d.h. $Q(R) = \mathbb{Q}$.

Zunächst bemerken wir, dass jedes $a \in \mathbb{Q}$ eine eindeutige Darstellung

$$a = \varepsilon \cdot \prod_{p \text{ prim}} p^{e_p(a)}$$

besitzt mit $e_p \in \mathbb{Z}$, nur endlich viele ungleich 0, und $\varepsilon \in \mathbb{Z}^\times = \{-1, +1\}$. Es gilt offenbar

$$a \in \mathbb{Z} \Longleftrightarrow e_p(a) \geq 0 \ \forall p \text{ prim}$$

und für alle $a, b \in \mathbb{Q}$

$$e_p(a \cdot b) = e_p(a) + e_p(b)$$

Für $f = a_d x^d + ... + a_0 \in \mathbb{Q}[x]$ sei

$$e_p(f) = \min(e_p(a_d), ..., e_p(a_0))$$

also

$$f \in \mathbb{Z}[x] \Longleftrightarrow e_p(f) \geq 0 \ \forall p \text{ prim}$$

Analog zu der Formel für $\mathbb{Q}$ haben wir auch für Polynome:

Lemma 8.3.1 (Gauß) *Sind $f_1, f_2 \in \mathbb{Q}[x]$ und p prim, dann*

$$e_p(f_1 \cdot f_2) = e_p(f_1) + e_p(f_2)$$

Beweis. Seien $f_1, f_2 \neq 0$, anderenfalls ist die Aussage klar. Für $f_1 \in \mathbb{Q}$ gilt die Behauptung ebenfalls, denn mit $f_2 = a_d x^d + ... + a_0 \in \mathbb{Q}[x]$ ist

$$\begin{aligned} e_p(f_1 \cdot f_2) &= \min(e_p(f_1) + e_p(a_d), ..., e_p(f_1) + e_p(a_0)) \\ &= e_p(f_1) + e_p(f_2) \end{aligned}$$

Wir können also f_i mit einer Konstanten in $\mathbb{Q}^\times = \mathbb{Q} \setminus \{0\}$ multiplizieren und damit erreichen, dass alle Koeffizienten in $\mathbb{Z}$ liegen und teilerfremd sind, also $e_p(f_i) = 0$.

Damit müssen wir nur zeigen: Sind $f_1, f_2 \in \mathbb{Z}[x]$ mit $e_p(f_1) = e_p(f_2) = 0$, dann $e_p(f_1 \cdot f_2) = 0$.

Durch $\varphi : \mathbb{Z} \to \mathbb{F}_p$ wird ein Homomorphismus

$$\tilde{\varphi} : \mathbb{Z}[x] \to \mathbb{F}_p[x], \quad \tilde{\varphi}\left(\sum_{i=0}^d a_i x^i\right) = \sum_{i=0}^d \varphi(a_i) x^i$$

induziert (siehe auch Übung 8.4) und

$$\ker \tilde{\varphi} = \{f \in \mathbb{Z}[x] \mid e_p(f) > 0\}$$

Somit folgt aus der Voraussetzung $e_p(f_i) = 0$, dass $\tilde{\varphi}(f_i) \neq 0$. Also verschwindet auch das Produkt

$$0 \neq \tilde{\varphi}(f_1) \cdot \tilde{\varphi}(f_2) = \tilde{\varphi}(f_1 \cdot f_2)$$

nicht (denn $\mathbb{F}_p[x]$ ist ein Integritätsring, siehe Beispiel 3.4.4) und damit wiederum

$$e_p(f_1 \cdot f_2) = 0$$

(man beachte $e_p(f_1 \cdot f_2) \geq 0$, da $f_1 \cdot f_2 \in \mathbb{Z}[x]$). ■

Definition 8.3.2 *Ein Polynom*

$$f = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_0 \in \mathbb{Z}[x]$$

heißt ***primitiv****, wenn*

$$\mathrm{ggT}(a_d, \ldots, a_0) = 1$$

äquivalent, wenn $e_p(f) = 0$ für alle p prim.
Beispielsweise sind normierte Polynome (d.h. $a_d = 1$) primitiv.

Satz 8.3.3 (Gauß) *Ist $f \in \mathbb{Z}[x]$ primitiv, dann gilt*

$$f \in \mathbb{Z}[x] \text{ irreduzibel} \iff f \in \mathbb{Q}[x] \text{ irreduzibel}$$

Beweis. Für ein primitives Polynom ist $\Leftarrow$ klar, für die Umkehrung: Sei $f = g_1 \cdot g_2$ mit $g_i \in \mathbb{Q}[x]$. Durch Multiplikation von g_1 mit einer Konstanten in $\mathbb{Q}$ (und teilen von g_2 durch diese Konstante) können wir annehmen, dass $g_1 \in \mathbb{Z}[x]$ primitiv ist, d.h. $e_p(g_1) = 0$ $\forall p$ prim. Mit Lemma 8.3.1 und $e_p(f) = 0$ also auch

$$e_p(g_2) = e_p(f) - e_p(g_1) = 0$$

für alle p prim und damit $g_2 \in \mathbb{Z}[x]$. ■

Beispiel 8.3.4 *Sei $n \in \mathbb{N}$ kein Quadrat in $\mathbb{Z}$. Dann ist $x^2 - n \in \mathbb{Z}[x]$ irreduzibel, also auch irreduzibel in $\mathbb{Q}[x]$, und somit*

$$\sqrt{n} \notin \mathbb{Q}$$

irrational.

Der Satz 3.7.13 von Gauß folgt aus Satz 8.3.3 (wenn man dort $\mathbb{Z}$ durch einen allgemeinen faktoriellen Ring ersetzt), siehe dazu Übung 8.3.

8.4 Nicht-Konstruierbarkeit des 9-Ecks

Satz 8.4.1 *Die Konstruktion eines regelmäßigen 9-Ecks mit Zirkel und Lineal ist nicht möglich.*

Beweis. Mit Bemerkung 8.2.4 ist $e^{2\pi i/9}$ konstruierbar aus $\{0,1\}$ genau dann, wenn

$$a = e^{2\pi i/9} + e^{-2\pi i/9} = 2\,\mathrm{Re}\left(e^{2\pi i/9}\right)$$

konstruierbar ist, siehe Abbildung 8.4. Es gilt

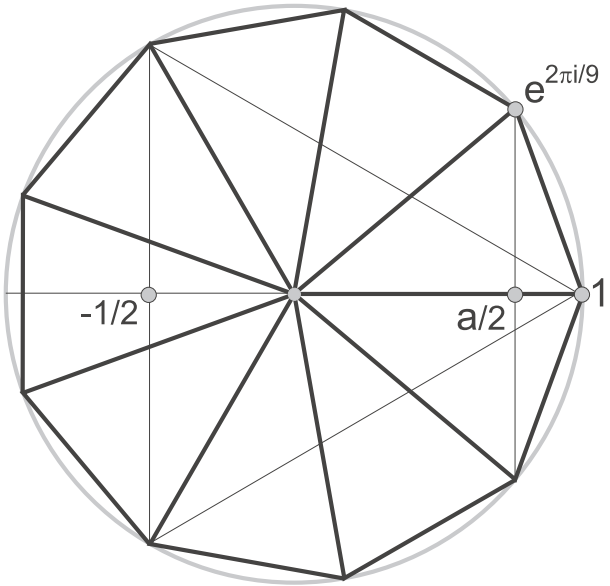


Abbildung 8.4: Regelmäßiges 9-Eck

$$\begin{aligned} a^3 &= e^{2\pi i/3} + 3e^{2\pi i/9} + 3e^{-2\pi i/9} + e^{-2\pi i3} \\ &= 3a - 1 \end{aligned}$$

Das entsprechende Polynom

$$f = x^3 - 3x + 1$$

ist irreduzibel in $\mathbb{Z}[x]$: Angenommen

$$\begin{aligned} f = x^3 - 3x + 1 &= (c_1 \cdot x + c_0)\left(d_2 \cdot x^2 + d_1 \cdot x + d_0\right) \\ &= c_1 d_2 \cdot x^2 + \ldots + c_0 d_0 \end{aligned}$$

dann $c_i \mid 1$ in $\mathbb{Z}$, also

$$c_i \in \{-1, +1\}$$

Da aber $-\frac{c_0}{c_1} \in \{-1, +1\}$ keine Nullstelle von f ist, folgt f irreduzibel in $\mathbb{Z}[x]$ und mit Satz 8.3.3 auch irreduzibel in $\mathbb{Q}[x]$.

Somit ist $f = m_a$ das Minimalpolynom von a, und es gilt

$$\big[\mathbb{Q}(a) : \mathbb{Q}\big] = \deg f = 3$$

also ist a nicht mit Zirkel und Lineal konstruierbar. ■

Insbesondere sehen wir auch, dass die Dreiteilung des 120°-Winkels im gleichseitigen Dreieck mit Zirkel und Lineal nicht möglich ist.

Siehe auch Übungsaufgabe 8.6 zum 7-Eck.

8.5 Übungen

Übung 8.1 *Konstruieren Sie mit Zirkel und Lineal das regelmäßige* $3, 4, 5$ *und* 6*-Eck, und zeigen Sie die Korrektheit Ihres Verfahrens.*

Übung 8.2 *Sei* $M \subset \mathbb{C}$ *eine endliche Teilmenge mit* $\{0, 1\} \subset M$*. Zeigen Sie:*

1) *Die Menge* $\mathrm{Kon}(M) \subset \mathbb{C}$ *der aus* M *mit Zirkel und Lineal konstruierbaren Punkte bildet einen Unterkörper, d.h. sind* $a, b \in \mathrm{Kon}(M)$*,* $a \neq 0$ *dann auch*

$$a + b,\ -b,\ a \cdot b,\ \frac{1}{a} \in \mathrm{Kon}(M)$$

2) $\mathrm{Kon}(M)$ *ist quadratisch abgeschlossen, d.h. mit* $a = r \cdot e^{i\varphi} \in \mathrm{Kon}(M)$ *ist auch* $\sqrt{a} = \sqrt{r} \cdot e^{i\varphi/2} \in \mathrm{Kon}(M)$*.*

Übung 8.3 *Zeigen Sie den Satz von Gauß: Sei* R *ein Integritätsring. Dann gilt*

$$R \text{ faktoriell} \iff R[x] \text{ faktoriell}$$

Übung 8.4 *1) Sei $\varphi : R \to S$ ein Homomorphismus von faktoriellen Ringen und*

$$\tilde{\varphi} : R[x] \to S[x]$$
$$\tilde{\varphi}\left(\sum_{i=0}^{d} a_i x^i\right) = \sum_{i=0}^{d} \varphi(a_i)\, x^i$$

der induzierte Homomorphismus von Polynomringen. Sei $f \in R[x]$ mit $\deg \tilde{\varphi}(f) = \deg f > 0$ ein primitives Polynom. Zeigen Sie:

Ist f irreduzibel in $S[x]$, dann auch in $R[x]$.

2) Sei $f \in \mathbb{Z}[x]$ und p eine Primzahl, die den Leitkoeffizienten von f nicht teilt. Zeigen Sie:

Ist f irreduzibel in $\mathbb{Z}/p[x]$, dann auch in $\mathbb{Q}[x]$.

Übung 8.5 *Sei*

$$f = x^4 + x + 1 \in \mathbb{Q}[x]$$

1) Zeigen Sie, dass f keine reelle Nullstelle hat und über $\mathbb{Q}$ irreduzibel ist.

2) Sei

$$f = (x-a)(x-\overline{a})(x-b)\left(x-\overline{b}\right) \in \mathbb{C}[x]$$

die Zerlegung von f in Linearfaktoren in $\mathbb{C}[x]$. Zeigen Sie, dass $\gamma = a\overline{a} + b\overline{b}$ eine Nullstelle von $x^3 - 4x - 1$ ist.

3) Zeigen Sie, dass $a, \overline{a}, b, \overline{b}$ nicht mit Zirkel und Lineal konstruierbar sind, jedoch

$$[\mathbb{Q}(a) : \mathbb{Q}] = [\mathbb{Q}(\overline{a}) : \mathbb{Q}] = [\mathbb{Q}(b) : \mathbb{Q}] = \left[\mathbb{Q}\left(\overline{b}\right) : \mathbb{Q}\right] = 2^2$$

Übung 8.6 *Sei*

$$a = e^{2\pi i/7} + e^{-2\pi i/7} = 2\,\mathrm{Re}\left(e^{2\pi i/7}\right)$$

und

$$f = x^3 + x^2 - 2x - 1$$

Zeigen Sie:

1) a ist eine Nullstelle von p.

2) f ist irreduzibel in $\mathbb{Q}[x]$.

3) Das reguläre 7-Eck lässt sich nicht mit Zirkel und Lineal aus $\{0, 1\}$ konstruieren.

Index

Literaturverzeichnis

[1] M. Artin: Algebra, Birkhäuser (2003)

[2] S. Bosch: Algebra, Springer (1993)

[3] P. Bundschuh: Einführung in die Zahlentheorie, Springer (1998)

[4] G. Fischer, R. Sacher: Einführung in die Algebra, Teubner (1983)

[5] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.4.12*; `http://www.gap-system.org`, (2008).

[6] G.H. Hardy, E.M. Wright: An introduction to the theory of numbers, Oxford (1956)

[7] J. C. Jantzen, J. Schwermer: Algebra, Springer (2006)

[8] C. Karpfinger, K. Meyberg: Algebra, Spektrum Akademischer Verlag (2008)

[9] E. Kunz: Algebra, Vieweg (1994)

[10] Maple (Waterloo Maple Inc.): Maple 14, `http://www.maplesoft.com/` (2010).

[11] R. Remmert, P. Ullrich: Elementare Zahlentheorie, Birkhäuser (1987)

[12] P. Ribenboim: Die Welt der Primzahlen, Springer (2006)

[13] R. Schulze-Pillot: Einführung in die Algebra und Zahlentheorie, Springer (2008)

[14] V. Shoup: A Computational Introduction to Number Theory and Algebra, Cambridge University Press (2005)

[15] J. Wolfart: Einführung in die Algebra und Zahlentheorie, Vieweg (1996)

[16] G. Wüstholz: Algebra, Vieweg (2004).