Jürgen Müller

Elementare Zahlentheorie und Algebra

Skriptum zur Vorlesung
Wintersemester 2015/2016

Basierend auf dem Skript der entsprechenden Vorlesung von
Professor Dr. Lutz Mattner aus dem Wintersemester 2014/15

Universität Trier

Fachbereich IV
Mathematik/Analysis

Inhaltsverzeichnis

1 Natürliche und ganze Zahlen

Wir gehen zunächst (noch einmal) kurz auf die Definition, d.h. das "Wesen" natürlicher bzw. ganzer Zahlen ein.

Die **natürlichen Zahlen** können axiomatisch beschrieben werden als ein Tripel $(\mathbb{N}, 1, N)$ mit den drei Eigenschaften (**Peano-Axiome**):

(N1) $\mathbb{N}$ ist eine Menge mit $1 \in \mathbb{N}$.

(N2) $N : \mathbb{N} \to \mathbb{N}$ ist eine injektive Funktion mit $1 \notin N(\mathbb{N})$. (N für „Nachfolger")

(N3) (Prinzip der vollständigen Induktion) Ist $A \subset \mathbb{N}$ mit $1 \in A$ und $N(A) \subset A$, so ist $A = \mathbb{N}$.

Man kann zeigen: Durch obige Axiome (N1)–(N3) ist $(\mathbb{N}, 1, N)$ bis auf Isomorphie eindeutig bestimmt[1]; daher denkt man sich ein solches Tripel fixiert, redet von *den* natürlichen Zahlen, und schreibt meist kurz $\mathbb{N}$ statt $(\mathbb{N}, 1, N)$.

Definition 1.1

1. Es seien M eine nichtleere Menge und $f : M \times M \to M$ eine Funktion. Dann heißt f **(innere, binäre) Verknüpfung** auf M. Man wählt dann oft ein nichtalphabetisches Zeichen wie $\cdot$, $\circ$, $*$, $\times$, $+$, ... für f und schreibt xfy statt $f(x, y)$ für $x, y \in M$, also etwa

$$x \cdot y\,,\ x \circ y\,,\ x * y\,,\ x \times y\,,\ x + y\,.$$

Im Fall des **Multiplikationssymbols** $\cdot$ schreibt man meist kurz xy statt $x \cdot y$.

2. Eine Verknüpfung $\cdot$ auf M heißt **assoziativ** falls

$$x\,(yz) \;=\; (xy)\,z \quad \text{für } x, y, z \in M,$$

und **kommutativ** falls

$$xy \;=\; yx \quad \text{für } x, y \in M$$

gilt. Ein $e \in M$ heißt **linksneutral** (bezüglich $\cdot$) falls

$$ex \;=\; x \quad \text{für } x \in M,$$

rechtsneutral falls $xe = x$ für $x \in M$, und **neutral** falls

$$ex \;=\; xe \;=\; x \quad \text{für } x \in M$$

gilt.

[1] Damit ist folgendes gemeint: Wir nennen, zumindest vorübergehend, jedes den Axiomen (N1)–(N3) gehorchende Tripel $(\mathbb{N}, 1, N)$ *ein* **System natürlicher Zahlen**. Sind dann $(\mathbb{N}, 1, N)$ und $(\mathbb{N}', 1', N')$ zwei Systeme natürlicher Zahlen, so gibt es eine Bijektion $\varphi : \mathbb{N} \to \mathbb{N}'$, für die erstens $\varphi(1) = 1'$ und $\varphi(N(n)) = N'(\varphi(n))$ für $n \in \mathbb{N}$ gilt, und zweitens (was aber aus dem vorhergehenden schon folgt) mit der Umkehrabbildung $\psi := \varphi^{-1} : \mathbb{N}' \to \mathbb{N}$ auch $\psi(1') = 1$ und $\psi(N'(m)) = N(\psi(m))$ für $m \in \mathbb{N}'$.

Bei assoziativen Verknüpfungen lässt man die Klammern meist weg, setzt also zum Beispiel $xyz := (xy)z = x(yz)$. Das **Pluszeichen** $+$ wird üblicherweise nur für kommutative Verknüpfungen benutzt.

Neutrale Elemente sind (im Falle der Existenz) eindeutig; genauer gilt: Ist e linksneutral und e' rechtsneutral für die Verknüpfung $\cdot$ auf M, so ist $e = e'$, also e einziges neutrales Element, denn die sukzessive Anwendung der beiden Voraussetzungen liefert $e' = ee' = e$.

Definition 1.2 Es sei $\cdot$ eine assoziative Verknüpfung auf M. Dann heißt $(M, \cdot)$ **Halbgruppe**. Existiert ein neutrales Element e (bezüglich $\cdot$), so heißt $(M, \cdot, e)$ **Monoid**. Wir schreiben oft kurz M statt $(M, \cdot)$ oder $(M, \cdot, e)$. Kommutative Halbgruppen heißen auch **abelsch**.

Man kann zeigen: Auf $\mathbb{N}$ existieren eindeutig bestimmte, assoziative und kommutative Verknpfungen $+$ und $\cdot$ auf $\mathbb{N}$ derart, dass

$$n + 1 = N(n), \qquad n + N(m) = N(n + m)$$

und

$$m \cdot 1 = m, \qquad m \cdot N(n) = mn + m$$

für $m, n \in \mathbb{N}$ gilt. Also sind $(\mathbb{N}, +)$ eine abelsche Halbgruppe und $(\mathbb{N}, \cdot, 1)$ ein abelsches Monoid.

Ferner definiert man zur Abkürzung $2 := 1 + 1$, $3 := 2 + 1$, $4 := 3 + 1$, $5 := 4 + 1$, $6 := 5 + 1$, $7 := 6 + 1$, $8 := 7 + 1$, und $9 := 8 + 1$.

Definition 1.3 Es sei $(M, \cdot, e)$ ein Monoid. Ist $x \in M$, so heißt ein $y \in M$ **linksinvers** (zu x) falls $yx = e$, **rechtsinvers** (zu x) falls $xy = e$, und **invers** (zu x) falls $yx = xy = e$; entsprechend heißt dann jeweils x **(links-, rechts-)invertierbar**. Ist jedes $x \in M$ invertierbar, so heißt M **Gruppe**.

Bemerkung 1.4 Es sei $(M, \cdot, e)$ ein Monoid.

1. Inverse sind im Falle der Existenz eindeutig bestimmt; genauer gilt: Sind $x, y_1, y_2 \in M$ mit y_1 links- und y_2 rechtsinvers zu x, so ist

$$y_1 \;=\; y_1 e \;=\; y_1(xy_2) \;=\; (y_1 x)y_2 \;=\; ey_2 \;=\; y_2.$$

Man bezeichnet das Inverse zu x mit x^{-1}. Bei Verwendung des Verknüpfungszeichens $+$ schreibt man meist $-x$ (und dann auch kurz $x - y$ satt $x + (-y)$).

2. Es seien $x, y \in M$ invertierbar. Dann sind auch x^{-1} und xy invertierbar mit $(x^{-1})^{-1} = x$ und

$$(xy)^{-1} \;=\; y^{-1}x^{-1}.$$

(Man beachte: es gilt $x^{-1}x = xx^{-1} = e$ und $xyy^{-1}x^{-1} = xx^{-1} = e$ sowie $y^{-1}x^{-1}xy = y^{-1}y = e$).

Setzt man

$$M^* \;:=\; \{x \in M : x \text{ invertierbar}\},$$

so ist damit $(M^*, \cdot|_{M^* \times M^*}, e)$ eine Gruppe (für deren Multiplikation wir wieder $\cdot$ schreiben).

(Denn: Aus $x, y \in M^*$ folgt $xy \in M^*$; daher ist $\cdot$ eine Verknüpfung auf M^*. Das neutrale Element e von M ist zu sich selbst invers, also ein Element von M^*; daher ist $(M^*, \cdot, e)$ ein Monoid. Ist $x \in M^*$, so hat x in M ein Inverses x^{-1} und es gilt $x^{-1} \in M^*$.)

3. M ist schon dann eine Gruppe, wenn zu jedem $x \in M$ ein Rechtsinverses existiert ([Ü]). Entsprechendes gilt mit Linksinvers statt Rechtsinvers.

4. Sind $a, b \in M$ und ist a invertierbar, so sind die Gleichungen $ax = b$ und $ya = b$ eindeutig lösbar, nämlich durch $x = a^{-1}b$ beziehungsweise $y = ba^{-1}$. Ist M eine Gruppe, so sind die Gleichungen damit für alle a, b eindeutig lösbar.

Beispiel 1.5 Es sei $M \neq \emptyset$ ein Menge. Dann ist

$$S(M) \;:=\; \{f \in M^M : f \text{ Bijektion von } M \text{ auf } M\}$$

mit der Komposition $\circ$ von Funktionen als Verknüpfung eine Gruppe, mit neutralem Element id_M; zu $f \in S(M)$ invers ist die Umkehrfunktion, die glücklicherweise sowieso schon mit f^{-1} bezeichnet wird. $S(M)$ heißt **symmetrische Gruppe** von M, und ein Element $f \in S(M)$ heißt **Permutation** von M.

Für $n \in \mathbb{N}$ heißt speziell $S_n := S(\{1, \ldots, n\})$ die **n-te symmetrische Gruppe**. Für $n \geq 3$ ist S_n nicht abelsch ([Ü]).

Wir kommen jetzt zu algebraischen Strukturen mit zwei Verknüpfungen.

Definition 1.6 Es sei R eine Menge und es seien $+$ und $\cdot$ Verknüpfungen auf R mit:

(R1) $(R, +, 0)$ ist eine abelsche Gruppe.

(R2) $(R, \cdot, 1)$ ist ein Monoid.

(R3) Die Verknüpfung $\cdot$ ist **distributiv über** $+$, d.h. für $x, y, z \in R$ gilt

$$(x + y)z \;=\; (xz) + (yz) \qquad \text{und} \qquad z(x + y) \;=\; (zx) + (zy).$$

Dann heißt $(R, +, \cdot)$ **Ring**, und das neutrale Element 1 zu $\cdot$ heißt **Eins(element)**. Ist M dabei abelsch, so heißt der Ring $(R, +, \cdot)$ **kommutativ**.

Wir schreiben manchmal deutlicher 0_R und 1_R für die neutralen Elemente eines Ringes. Andererseits schreiben wir oft kurz R statt $(R, +, \cdot)$.

Bemerkung 1.7 Durch geeignetes Hinzufügen eines Elementes 0 lässt sich die Halbgruppe $(\mathbb{N}, +)$ zunächst zu einem Monoid $(\mathbb{N}_0, +, 0)$ erweitern. Damit lässt sich wiederum durch Äquivalenzklassenbildung in $\mathbb{N}_0 \times \mathbb{N}_0$ das Monoid $(\mathbb{N}_0, +, 0)$ zur (abelschen) Gruppe $(\mathbb{Z}, +, 0)$ der **ganzen Zahlen** erweitern. Mit geeigneter Erweiterung der Multiplikation wird $(\mathbb{Z}, +, \cdot)$ zu einem kommutativen Ring mit Einselement $1 = 1_{\mathbb{Z}}$.

Man verwendet (wie in $(\mathbb{Z}, +, \cdot)$) auch in allgemeinen Ringen Punkt-vor-Strich-Schreibweisen, also zum Beispiel $x + yz \coloneqq x + (yz)$.

Bemerkung 1.8 Es sei R ein Ring. Dann gilt für $x, y, z \in R$ ([Ü]):

1. $0 \cdot x = x \cdot 0 = 0$.
2. $(-x)y = x(-y) = -xy$.
3. $(-x)(-y) = xy$.
4. $x(y - z) = xy - xz$ und $(x - y)z = xz - yz$.

Wie aus der Einführung in die Mathematik bekannt, lässt sich $\mathbb{Z}$ mit einer Ordnung $<$ versehen, die mit den Verknüpfungen $+$ und $\cdot$ in Sinne der üblichen Monotoniegesetze verträglich ist (genauer: ist $x < y$, so gilt $x + z < y + z$ für alle z und $xz < yz$, falls $z > 0$).

Wichtig für uns ist insbesondere die Tatsache, dass jede nichtleere Menge $A \subset \mathbb{Z}$ ein Minimum hat, falls sie nach unten beschränkt ist, und ein Maximum falls sie nach oben beschränkt ist.

Wir verwenden Minkowski-Schreibweisen wie $A + B \coloneqq \{x + y : x \in A, y \in B\}$, $AB \coloneqq \{xy : x \in A, y \in B\}$ für $A, B \subset \mathbb{Z}$. Bei einpunktigen Mengen $A = \{a\}$ lassen wir die Klammern weg, schreiben also etwa $a + B$ statt $\{a\} + B$. Außerdem sei wie üblich $|a| := \operatorname{sign}(a) \cdot a$.

Satz 1.9 *(Division mit Rest)*
Es sei $(a, b) \in \mathbb{Z}^2$ mit $a \neq 0$. Dann existiert genau ein Paar $(q, r) \in \mathbb{Z}^2$ mit $b = qa + r$ und $0 \leq r < |a|$.

Beweis. Da $a \neq 0$ gilt, ist

$$L := \mathbb{N}_0 \cap (b - a\mathbb{Z}) \neq \emptyset$$

und $0 \leq r := \min L < |a|$ (man beachte: mit $y \in b - a\mathbb{Z}$ ist auch $y - |a| \in b - a\mathbb{Z}$). Für q so, dass $b - qa = r$ gilt die Behauptung.

(Eindeutigkeit: [Ü]). □

Als Anwendung beweisen wir ein Ergebnis über die Darstellung natürlicher Zahlen[2].

Satz 1.10 *Es sei $q \in \mathbb{N}$ mit $q \geq 2$. Dann existiert für jedes $n \in \mathbb{N}_0$ genau eine Folge $a = (a_j) = \big(a_j(n)\big) \in \{0, \ldots, q-1\}^{(\mathbb{N}_0)}$ mit*

$$n = \sum_{j \in \mathbb{N}_0} a_j(n) q^j.$$

Beweis. 1. Eindeutigkeit: Angenommen, es existieren $a, \widetilde{a} \in \{0, \ldots, q-1\}^{(\mathbb{N}_0)}$ mit $a \neq \tilde{a}$ und $\sum\limits_{j \in \mathbb{N}_0} a_j q^j = \sum\limits_{j \in \mathbb{N}_0} \widetilde{a}_j q^j$. Dann gilt für $m := \max\{j : a_j \neq \widetilde{a}_j\}$ (ohne Einschränkung $a_m > \widetilde{a}_m$)

$$0 = (a_m - \widetilde{a}_m) q^m + \sum_{j=0}^{m-1} (a_j - \widetilde{a}_j) q^j \geq q^m - (q-1) \sum_{j=0}^{m-1} q^j = 1.$$

Widerspruch.

---

[2] Im Weiteren verwenden wir Summen und Produktschreibweisen in recht allgemeiner Form: Ist $(M, \cdot, e)$ ein Monoid und sind $x_1, \ldots, x_N \in M$, so setzen wir $\prod\limits_{\ell=1}^{0} x_\ell := e$ und $\prod\limits_{\ell=1}^{k} x_\ell := (\prod\limits_{\ell=1}^{k-1} x_\ell) \cdot x_k$ für $k = 1, \ldots, N$. Außerdem schreiben wir $x^k := \prod\limits_{\ell=1}^{k} x$ (also im Falle $x_1 = \ldots = x_k = x$). Insbesondere ist $x^0 = e$. Ist x invertierbar, so setzen wir auch $x^{-k} := (x^{-1})^k$ für $k \in \mathbb{N}$.

Ist M abelsch, so kann die Reihenfolge bei der Produktbildung beliebig vertauscht werden. In diesem Fall ist also für endliche Indexmengen J und $(x_j)_{j \in J} \in M^J$ das Produkt $\prod\limits_{j \in J} x_j$ (wohl-)definiert durch $\prod\limits_{j \in J} x_j := \prod\limits_{\ell=1}^{k} x_{j_\ell}$, wobei $J = \{j_1, \ldots, j_k\}$ eine beliebige Abzählung von J ist.

Weiter schreiben wir für nicht notwendig endliche Indexmengen J und $(x_j)_{j \in J} \in M^{(J)}$, wobei

$$M^{(J)} := \{x = (x_j)_{j \in J} \in M^J : \{j \in J : x_j \neq e\} \text{ endlich}\},$$

auch kurz $\prod\limits_{j \in J} x_j := \prod\limits_{j \in J,\, x_j \neq e} x_j$.

Im Falle des Pluszeiches als Verknüpfung schreiben wir statt $\prod$ jeweils $\sum$. Außerdem schreiben wir dann ka statt a^k.

2. Existenz.

$n = 0$: Man setze $a_j(0) := 0$ für $j \in \mathbb{N}_0$.

$n - 1 \to n$: Es sei $k \in \mathbb{N}_0$ mit $q^k \leq n < q^{k+1}$. Division mit Rest ergibt

$$n = mq^k + n'$$

mit $0 < m < q$ und $0 \leq n' < q^k$, also insbesondere $n' < n$.
Nach Induktionsvoraussetzung (Behauptung gilt für jedes $n' < n$) existiert eine Folge $\big(a_j(n')\big)$ mit

$$n' = \sum_{j \in \mathbb{N}_0} a_j(n') q^j.$$

Dabei ist $a_j(n') = 0$ für $j \geq k$, da $n' < q^k$. Setzt man

$$a_j(n) := \begin{cases} a_j(n') & \text{für } j \neq k \\ m & \text{für } j = k \end{cases},$$

so ist

$$n = mq^k + n' = \sum_{j \in \mathbb{N}_0} a_j(n) q^j.$$

□

Für jedes q ist die durch Satz 1.10 wohldefinierte Abbildung

$$\mathbb{N}_0 \ni n \mapsto \big(a_j(n)\big)_{j \in \mathbb{N}_0} \in \{0, \ldots, q-1\}^{(\mathbb{N}_0)}$$

bijektiv. Mit $r = r(n) := \max\{j : a_j(n) \neq 0\}$ für $n \in \mathbb{N}$ heißt

$$(a_r a_{r-1} \ldots a_0)_q = (a_{r(n)}(n) \ldots a_0(n))_q$$

die q-**adische Darstellung** von n. Im Falle $q = 9 + 1 =:$ Zehn spricht man auch von der **Dezimal-**, im Falle $q = 2$ von der **Binär-**, und im Falle $q =$ Zehn $+ 6$ von der **Hexadezimaldarstellung**. Schließlich schreibt man im Dezimalfall auch kurz $a_r \ldots a_0$ statt $(a_r \ldots a_0)_{\text{Zehn}}$, also zum Beispiel Zehn $= 10$.

2 Teiler und Primzahlen

Definition 2.1 Für $a, b \in \mathbb{Z}$ bedeutet a **teilt** b, oder a ist ein **Teiler** von b, dass ein $q \in \mathbb{Z}$ existiert mit $b = a \cdot q$, d. h. falls $b \in a\mathbb{Z}$ gilt. Man schreibt dann $a|b$ und anderenfalls $a \nmid b$. Für $a \in \mathbb{Z}$ und $B \subset \mathbb{Z}$ schreiben wir $a|B$ falls $a|b$ für jedes $b \in B$ gilt, wenn also $B \subset a\mathbb{Z}$ gilt.

Bemerkung 2.2 Es seien $a, b, c \in \mathbb{Z}$. Aus obiger Definition ergibt sich leicht ([Ü]):

1. $\pm 1|b$, $\pm b|b$ und $a|0$.
2. Aus $a|b$ und $b|c$ folgt $a|c$.
3. Aus $a|b$ und $a|c$ folgt $a|(b\mathbb{Z} + c\mathbb{Z})$, d. h. $a|(bx + cy)$ für alle $x, y \in \mathbb{Z}$.
4. Aus $a|b$ folgt $b = 0$ oder $|a| \leq |b|$.

Wir verwenden im Weiteren Rechenregeln für Minkowskisummen und -produkte wie etwa $A(B + C) \subset AB + AC$ für $A, B, C \subset \mathbb{Z}$, $(A + B)c = Ac + Bc$ für $A, B \subset \mathbb{Z}$, $c \in \mathbb{Z}$ oder auch

$$(a\mathbb{Z})(b\mathbb{Z}) = a(b\mathbb{Z}) = (ab)\mathbb{Z} \qquad (a, b \in \mathbb{Z}),$$

die sich unmittelbar aus entsprechenden Rechenregeln in $\mathbb{Z}$ ergeben ([Ü]).

Definition 2.3 Es seien $a, b \in \mathbb{Z}$ mit $a \neq 0$ oder $b \neq 0$. Dann heißt

$$\mathrm{ggT}(a, b) := \max\{k \in \mathbb{N} : k|a \text{ und } k|b\}$$

größter gemeinsamer Teiler von a und b. Im Falle $\mathrm{ggT}(a, b) = 1$ heißen a, b **teilerfremd**. Zudem setzen wir noch $\mathrm{ggT}(0, 0) := 0$.

Damit ergibt sich für die Minkowskisumme $a\mathbb{Z} + b\mathbb{Z}$ folgende wichtige Formel:

Satz 2.4 *Es seien $a, b \in \mathbb{Z}$ und es sei $d := \mathrm{ggT}(a, b)$. Dann ist*

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}.$$

Insbesondere sind a, b teilerfremd genau dann, wenn $1 \in a\mathbb{Z} + b\mathbb{Z}$.

Beweis. Ist $a = b = 0$, so ist $d = 0$ und die Behauptung trivial. Es seien also $a \neq 0$ oder $b \neq 0$. Wir setzen

$$L := a\mathbb{Z} + b\mathbb{Z} \qquad \text{und} \qquad m := \min(\mathbb{N} \cap L).$$

Dann ist $m\mathbb{Z} \subset L$ (denn $m\mathbb{Z} \subset (a\mathbb{Z} + b\mathbb{Z})\mathbb{Z} \subset (a\mathbb{Z})\mathbb{Z} + (b\mathbb{Z})\mathbb{Z} = L$).

Aus $d|a$ und $d|b$ folgt $d|(a\mathbb{Z} + b\mathbb{Z})$ nach Bemerkung 2.2.3. Also ist $L \subset d\mathbb{Z}$ und insbesondere $m \in d\mathbb{Z}$, d. h. $d|m$.

Weiter gilt $m|a$.

(Denn: Es sei $a = qm + r$ wie in Satz 1.9. Dann ist

$$r = a + m(-q) \in a + m\mathbb{Z} \subset a + L = L$$

und $0 \leq r < |m|$, also $r = 0$ nach Definition von m. Damit ist m Teiler von a.)

Genauso gilt $m|b$, also ist $m \leq \mathrm{ggT}(a, b) = d$. Mit $d|m$ folgt $d = m$ und damit auch $d\mathbb{Z} = m\mathbb{Z} = L$. □

Bemerkung 2.5 Ein Verfahren zur Berechnung des $\mathrm{ggT}(a, b)$ ist der **Euklidische Algorithmus**[3]: Sind $a, b \in \mathbb{Z} \setminus \{0\}$, so wendet man sukzessive Division mit Rest an, startend mit $r_0 = b, r_1 = |a|$:

$$\begin{aligned} (b =)\ r_0 &= q_1 r_1 + r_2 \quad (= q_1|a| + r_2) \\ r_1 &= q_2 r_2 + r_3 \\ &\vdots \end{aligned}$$

Da nach Satz 1.9 dabei $r_1 > r_2 > \cdots (\geq 0)$ gilt, bricht das Verfahren nach endlich vielen Schritten ab (d. h. $r_n > r_{n+1} = 0$ für ein $n \in \mathbb{N}$). Also ergibt sich als letzte Gleichung

$$r_{n-1} = q_n r_n.$$

Dabei gilt $r_n = \mathrm{ggT}(a, b)$.

[3] Die Benennung mehrerer mathematischer Ergebnisse nach Euklid verweist auf deren Darstellung in dessen ungefähr um 300 v.d.Z. verfassten und über mehr als zwei Jahrtausende in Präzision und Didaktik als vorbildlich angesehenen und viel benutzten Lehrbuches (nach unseren heutigen Begriffen wohl eher für Studenten als für Schüler konzipiert) *Die Elemente*. Höchstens einige dieser Ergebnisse können von Euklid selbst stammen, der Euklidische Algorithmus zum Beispiel nicht. Siehe dazu die Kommentare in der in mehreren Auflagen verbreiteten deutschsprachigen Ausgabe von Clemens Thaer.

(Denn:
$\leq$: Durch Nachverfolgen des Gleichungssystems von unten nach oben sieht man: $r_{n-1} \in r_n\mathbb{Z}, r_{n-2} = q_{n-1}r_{n-1} + r_n \in r_n\mathbb{Z}, \ldots, r_1 \in r_n\mathbb{Z}, r_0 \in r_n\mathbb{Z}$, also $r_n|a$ und $r_n|b$.
$\geq$: Wie man durch Lesen des Gleichungssystems von oben nach unten sieht, ist $r_2 \in a\mathbb{Z} + b\mathbb{Z}, \ldots, r_n \in a\mathbb{Z} + b\mathbb{Z} = \mathrm{ggT}(a,b)\mathbb{Z}$ nach Satz 2.4. Aus $r_n \geq 1$ folgt $r_n \geq \mathrm{ggT}(a,b)$.)

Sind etwa $a = 1029$ und $b = 1071$, so ergibt sich

$$\left.\begin{array}{c} 1071 = 1 \cdot 1029 + 42 \\ 1029 = 24 \cdot 42 + 21 \\ 42 = 2 \cdot 21 + 0 \end{array}\right\} \text{Also: } \mathrm{ggT}(1029, 1071) = 21.$$

Nach Satz 2.4 ist damit $1029 \cdot \mathbb{Z} + 1071 \cdot \mathbb{Z} = 21 \cdot \mathbb{Z}$.

Als weitere Folgerungen aus Satz 2.4 erhalten wir

Satz 2.6 *Es seien $a, b, c \in \mathbb{Z}$ mit $\mathrm{ggT}(a,b) = 1$. Dann gilt:*

1. *Aus $a|bc$ folgt $a|c$.*
2. *Aus $a|c$ und $b|c$ folgt $ab|c$.*
3. *Ist $\mathrm{ggT}(a,c) = 1$, so ist auch $\mathrm{ggT}(a,bc) = 1$.*

Beweis. Nach Satz 2.4 ist $1 \in a\mathbb{Z} + b\mathbb{Z}$ und damit auch

$$c \in (a\mathbb{Z} + b\mathbb{Z})c = (ac)\mathbb{Z} + (bc)\mathbb{Z}. \tag{2.1}$$

1. Es gelte $a|bc$. Mit $a|ac$ gilt dann $a|(ac)\mathbb{Z} + (bc)\mathbb{Z}$ nach Bemerkung 2.2.3 , also $a|c$ nach (2.1). 2. Es gelte $a|c$ und $b|c$, also $c \in a\mathbb{Z}$ und $c \in b\mathbb{Z}$. Mit (2.1) folgt

$$c \in (a\mathbb{Z})c + (b\mathbb{Z})c \subset (a\mathbb{Z})(b\mathbb{Z}) + (b\mathbb{Z})(a\mathbb{Z}) = (ab)\mathbb{Z}.$$

2. Es gelte $\mathrm{ggT}(a,c) = 1$. Dann ist $1 \in a\mathbb{Z} + c\mathbb{Z}$. Also folgt mit (2.1)

$$1 = 1 \cdot 1 \in (a\mathbb{Z} + b\mathbb{Z})(a\mathbb{Z} + c\mathbb{Z}) \subset a\mathbb{Z} + (bc)\mathbb{Z}.$$

Nach Satz 2.4 sind a und bc teilerfremd. □

Bemerkung und Definition 2.7 Eine Zahl $p \in \mathbb{N} \setminus \{1\}$ heißt **Primzahl** falls sie nur die Teiler ± 1 und $\pm p$ hat. Wir setzen

$$\mathbb{P} := \{p : p \text{ Primzahl}\}.$$

Für $p \in \mathbb{P}$ und $b, c \in \mathbb{Z}$ folgt aus $p|bc$ schon $p|b$ oder $p|c$.

(Gilt nämlich $p|bc$ und ist p kein Teiler von b, also $\mathrm{ggT}(b,p) = 1$ wegen p prim, so folgt $p|c$ nach Satz 2.6.1.)

Allgemeiner ergibt sich daraus mittels Induktion über die Mächtigkeit von B:
Ist $B \subset \mathbb{Z}$ endlich und ist p prim, so folgt aus $p| \prod\limits_{b\in B} b$ schon $p|b$ für ein $b \in B$.

Der folgende Satz zeigt, dass jede natürliche Zahl $n \geq 2$ eine Primfaktorzerlegung hat und dass diese in geeigneter Weise eindeutig ist. Primzahlen können gewissermaßen als „Elementarbausteine“ der natürlichen Zahlen angesehen werden.

Satz 2.8 *(Primfaktorzerlegung, Fundamentalsatz der Arithmetik)*
Für jedes $n \in \mathbb{N}$ existiert genau ein Tupel $(\alpha_p(n))_{p\in\mathbb{P}} \in \mathbb{N}_0^{(\mathbb{P})}$ mit

$$\boxed{n = \prod_{p\in\mathbb{P}} p^{\alpha_p(n)}\,.}$$

Beweis. 1. Eindeutigkeit: Wir zeigen per Induktion nach $k \in \mathbb{N}_0$:

Ist $n = \prod\limits_{p\in\mathbb{P}} p^{\nu_p}$ mit $(\nu_p) \in \mathbb{N}_0^{(\mathbb{P})}$ sowie $\sum\limits_{p\in\mathbb{P}} \nu_p = k$, und ist $n = \prod\limits_{p\in\mathbb{P}} p^{\mu_p}$ mit $(\mu_p) \in \mathbb{N}_0^{(\mathbb{P})}$, so gilt $\mu_p = \nu_p$ für alle $p \in \mathbb{P}$.

$k = 0$: Hier ist $\nu_p = 0$ $(p \in \mathbb{P})$. Dann muss auch $\mu_p = 0$ für alle p gelten.

$k \to k+1$: Es sei $\prod\limits_{p\in\mathbb{P}} p^{\nu_p} = \prod\limits_{p\in\mathbb{P}} p^{\mu_p}$ mit $\sum\limits_{p\in\mathbb{P}} \nu_p = k+1$. Ist $\nu_q \neq 0$, so folgt aus $q \Big| \prod\limits_{p\in\mathbb{P}} p^{\mu_p}$ mit B/D 2.7 die Existenz eines $p \in \mathbb{P}$ mit $\mu_p > 0$ und $q|p$. Dann ist schon $q = p$ (da p Primzahl). Also gilt

$$\left(\prod_{p\in\mathbb{P}\setminus\{q\}} p^{\nu_p}\right) q^{\nu_q - 1} = \left(\prod_{p\in\mathbb{P}\setminus\{q\}} p^{\mu_p}\right) q^{\mu_q - 1}.$$

Wegen $\left(\sum\limits_{p\in\mathbb{P}\setminus\{q\}} \nu_p\right) + \nu_q - 1 = k$ ist die Induktionsvoraussetzung anwendbar. Damit ist $\nu_p = \mu_p$ für $p \in \mathbb{P} \setminus \{q\}$ und $\nu_q - 1 = \mu_q - 1$, also $\nu_p = \mu_p$ für alle $p \in \mathbb{P}$.

2. Existenz: Es sei $n \in \mathbb{N} \setminus \{1\}$. Dann existiert ein Primteiler p_1 von n.
(Denn: $p_1 := \min\{k > 1 : k|n\}$ ist eine Primzahl, da p_1 sonst einen Teiler a mit $1 < a < p_1$ hätte, der dann auch Teiler von n wäre im Widerspruch zur Minimalität von p_1.)

Damit ist $n = p_1 n_1$ für ein $n_1 \in \mathbb{N}$ mit $1 \leq n_1 < n$.

Ist $n_1 > 1$, so hat mit der gleichen Argumentation n_1 einen Primteiler p_2, also $n_1 = p_2 n_2$ mit $1 \leq n_2 < n_1$. Aus $n > n_1 > n_2 \ldots$ ergibt sich, dass dieses „Faktorisierungsverfahren“ nach endlich vielen Schritten N bei 1 landet. Also erhält man $n = \prod_{j=1}^{N} p_j$, d. h. eine Darstellung von n als Produkt von (endlich vielen) Primzahlen.

Definiert man $\alpha_p(n)$ als die Anzahl der $j \in \{1, \ldots, N\}$ mit $p_j = p$, so gilt damit

$$n = \prod_{j=1}^{N} p_j = \prod_{p \in \mathbb{P}} p^{\alpha_p(n)}.$$

Für $n = 1$ ist $\alpha_p(1) := 0$ $(p \in \mathbb{P})$ geeignet. □

Bemerkung 2.9 1. Nach dem Fundamentalsatz der Arithmetik ist die Abbildung

$$\mathbb{N} \ni n \mapsto (\alpha_p(n))_{p \in \mathbb{P}} \in \mathbb{N}_0^{(\mathbb{P})}$$

wohldefineirt und bijektiv mit der Umkehrabbildung

$$\mathbb{N}_0^{(\mathbb{P})} \ni (\nu_p)_{p \in \mathbb{P}} \mapsto \prod_{p \in \mathbb{P}} p^{\nu_p} \in \mathbb{N}\,.$$

2. Für $n \in \mathbb{N}$ und $p \in \mathbb{P}$ ist $\alpha_p(n) > 0$ genau dann, wenn p ein Teiler von n ist. Damit ist auch

$$\boxed{n = \prod_{p \in \mathbb{P},\, p \mid n} p^{\alpha_p(n)}\,.}$$

Insbesondere hat jedes $n > 1$ einen Primteiler.

Wir wollen uns nun mit der Frage der “Häufigkeit” von Primzahlen in der Folge der natürlichen Zahlen beschäftigen. Wir schreiben im Weiteren $\#J \in \mathbb{N}_0 \cup \{\infty\}$ für die Anzahl der Elemente einer Menge J. Für $(a_j)_{j \in I} \in [0, \infty)^J$ (also hier (a_j) nicht abbrechend) setzen wir zudem $\sum\limits_{j \in I} a_j := \sup\limits_{E \subset J \text{ endlich}} \sum\limits_{j \in E} a_j \in [0, \infty]$. Zunächst beweisen wir

Satz 2.10 *(Euklid)*
Es gibt unendlich viele Primzahlen, d. h. $\#\mathbb{P} = \sum\limits_{p \in \mathbb{P}} 1 = \infty$.

Beweis. Angenommen, $\mathbb{P}$ sei endlich. Dann ist $n := 1 + \prod_{p\in\mathbb{P}} p \in \mathbb{N}$ und $n > 1$. Ist p_0 ein Primteiler von n, so teilt p_0 auch $\prod_{p\in\mathbb{P}} p$ und damit auch $1 = n - \prod_{p\in\mathbb{P}} p$. Widerspruch. □

Genauer als in Satz 2.10 gilt

Satz 2.11

$$\sum_{p\in\mathbb{P}} \frac{1}{p} = \infty.$$

Beweis. Es sei $E \subset \mathbb{P}$ endlich. Dann folgt aus $\dfrac{1}{1-x} \le \mathrm{e}^{2x}$ $(0 \le x \le 1/2)$

$$\prod_{p\in E}\left(\sum_{\nu\in\mathbb{N}_0} \frac{1}{p^\nu}\right) = \prod_{p\in E} \frac{1}{1-\frac{1}{p}} \le \exp\left(2\sum_{p\in E}\frac{1}{p}\right).$$

Setzt man

$$M_E := \{n = \prod_{p\in E} p^{\nu_p} : (\nu_p) \in \mathbb{N}_0^E\},$$

so ergibt sich mit der Eindeutigkeitsaussage aus dem Fundamentalsatz der Arithmetik

$$\prod_{p\in E}\left(\sum_{\nu\in\mathbb{N}_0} \frac{1}{p^\nu}\right) = \sum_{(\nu_p)\in\mathbb{N}_0^E}\left(\prod_{p\in E}\frac{1}{p^{\nu_p}}\right) = \sum_{n\in M_E}\frac{1}{n}.$$

Weiter ist $\bigcup_{E\subset\mathbb{P} \text{ endlich}} M_E = \mathbb{N}$ nach der Existenzaussage des Fundamentalsatzes. Hieraus folgt

$$\sup_{E\subset\mathbb{P} \text{ endlich}} \sum_{n\in M_E}\frac{1}{n} = \sup_{F\subset\mathbb{N} \text{ endlich}} \sum_{n\in F}\frac{1}{n} = \infty,$$

also auch

$$\infty = \sup_{E\subset\mathbb{P} \text{ endlich}} \frac{1}{2}\log\left(\sum_{n\in M_E}\frac{1}{n}\right) \le \sum_{p\in\mathbb{P}}\frac{1}{p}.$$

□

Eine noch genauere Aussage über die Häufigkeit der Primzahlen in $\mathbb{N}$ macht der bekannte Primzahlsatz, der 1896 gleichzeitig und unabhängig von de la Vallée-Poussin und Hadamard bewiesen wurde. Bezeichnet man mit $\pi(x)$ die Anzahl der Primzahlen $\le x$, so gilt:

$$\pi(x) \sim \frac{x}{\log x} \quad \left(\sim \int_2^x \frac{\mathrm{d}t}{\log t} =: \mathrm{Li}(x)\right) \qquad \text{für } x \to \infty$$

(wobei $f(x) \sim g(x)$ bedeutet, dass $f(x)/g(x) \to 1$ gilt).

Wir beweisen eine Vorstufe, die auf Tschebyscheff zurückgeht und mit elementaren Methoden auskommt. Hilfsmittel ist folgender Satz von Legendre ($\lfloor\cdot\rfloor$ = Gaußklammer).

Satz 2.12 *Für $n \in \mathbb{N}$ und $p \in \mathbb{P}$ gilt*

$$\alpha_p(n!) = \sum_{\nu\in\mathbb{N}} \left\lfloor \frac{n}{p^\nu} \right\rfloor \quad \left(= \sum_{\nu=1}^{\lfloor \frac{\log n}{\log p} \rfloor} \left\lfloor \frac{n}{p^\nu} \right\rfloor \right).$$

Beweis. Zunächst gilt für $n, a \in \mathbb{N}$ ([Ü]):

$$\left\lfloor \frac{n}{a} \right\rfloor = \#\{k \in \{1,\dots,n\} : a|k\}.$$

Dies im letzten Schritt verwendend erhalten wir

$$\alpha_p(n!) \;=\; \sum_{k=1}^{n} \alpha_p(k) \;=\; \sum_{k=1}^{n} \sum_{\nu\geq 1,\, p^\nu|k} 1 \;=\; \sum_{\nu\geq 1} \sum_{\substack{k=1 \\ p^\nu|k}}^{n} 1 \;=\; \sum_{\nu=1}^{\lfloor \frac{\log n}{\log p} \rfloor} \left\lfloor \frac{n}{p^\nu} \right\rfloor$$

(man beachte: $\lfloor n/p^\nu \rfloor = 0$ für $\nu > \log n/\log p$). □

Satz 2.13 *(Tschebyscheff)*
Für $n \in \mathbb{N} \setminus \{1\}$ gilt

$$\frac{1}{4}\,\frac{n}{\log n} \leq \pi(n) \leq 6\,\frac{n}{\log n}.$$

Beweis. 1. Für $n \in \mathbb{N}$ ist und unter Verwendung von Satz 2.12 im letzten Schritt

$$\begin{aligned} s_n \;&:=\; \log \binom{2n}{n} \;=\; \log\Big((2n)!\Big) - 2\log(n!) \\ &=\; \sum_{p\in\mathbb{P}} \alpha_p\Big((2n)!\Big)\,\log p - 2\sum_{p\in\mathbb{P}} \alpha_p(n!)\log p \\ &=\; \sum_{(\mathbb{P}\ni)\,p\leq 2n} \log p \sum_{\nu=1}^{\lfloor \frac{\log 2n}{\log p} \rfloor} \left(\left\lfloor \frac{2n}{p^\nu} \right\rfloor - 2\left\lfloor \frac{n}{p^\nu} \right\rfloor \right). \end{aligned}$$

Weiter gilt für $x \in \mathbb{R}$

$$\lfloor 2x \rfloor - 2\lfloor x \rfloor = \begin{cases} 0 & \text{falls } 0 \leq x - \lfloor x \rfloor < 1/2, \\ 1 & \text{falls } 1/2 \leq x - \lfloor x \rfloor < 1. \end{cases}$$

Damit ergibt sich einerseits

$$s_n \le \sum_{p\le 2n} \log p \sum_{\nu=1}^{\left\lfloor \frac{\log 2n}{\log p}\right\rfloor} 1 = \sum_{p\le 2n} \log p \left\lfloor \frac{\log 2n}{\log p}\right\rfloor \le \pi(2n)\log(2n) \tag{2.2}$$

und andererseits wegen $1/2 \le n/p < 1$ für $n < p \le 2n$

$$s_n \ge \sum_{p\le 2n} \log p \cdot \left(\left\lfloor \frac{2n}{p}\right\rfloor - 2\left\lfloor \frac{n}{p}\right\rfloor\right) \ge \sum_{n<p\le 2n} \log p. \tag{2.3}$$

2. Für $n \in \mathbb{N}$ gilt

$$2^n \;\le\; \prod_{k=1}^{n} \frac{n+k}{k} \;=\; \binom{2n}{n} \;\le\; \sum_{k=0}^{2n}\binom{2n}{k} \;=\; (1+1)^{2n} \;=\; 2^{2n}$$

und daher

$$n\log 2 \;\le\; s_n \;\le\; 2n\log 2.$$

3. Beweis von "$\ldots \le \pi(n)$": Für $n \in \mathbb{N}$ gilt mit 2. und (2.2)

$$n\log 2 \le s_n \le \pi(2n)\log(2n)$$

Aus $\log 2 > 5/8$ und der Monotonie von $x \mapsto x/\log(x)$ auf $[\mathrm{e},\infty)$ folgt

$$\pi(2n+1) \ge \pi(2n) \ge \frac{n\log 2}{\log(2n)} > \underbrace{\frac{n\log 2}{2n+1}}_{\ge 1/4 \text{ für } n\ge 2} \frac{2n+1}{\log(2n+1)} \ge \frac{1}{4}\frac{2n+1}{\log(2n+1)} \ge \frac{1}{4}\frac{2n}{\log(2n)};$$

damit ist die Teilbehauptung "$\ldots \le \pi(n)$" außer für $n = 2, 3$ bewiesen, für diese letzteren Werte aber offenbar auch richtig.

4. Beweis von "$\pi(n) \le \ldots$": Wir setzen

$$\vartheta(x) \;:=\; \sum_{p\le x} \log p \qquad \text{für } x \in [0,\infty).$$

Für $n \in \mathbb{N}$ erhalten wir mit (2.3) und 2.

$$\vartheta(2n) - \vartheta(n) = \sum_{n<p\le 2n} \log p \le s_n \le 2n\log 2.$$

Damit folgt für $k \in \mathbb{N}_0$

$$\vartheta(2^{k+1}) - \vartheta(2^k) \;\le\; 2^{k+1}\log 2,$$

also, unter Verwendung von $\vartheta(1) = 0$ im ersten Schritt,

$$\vartheta(2^{k+1}) \;=\; \sum_{\ell=0}^{k}\left(\vartheta(2^{\ell+1}) - \vartheta(2^\ell)\right) \;\le\; \sum_{\ell=0}^{k} 2^{\ell+1}\log 2 \;=\; 2(2^{k+1}-1)\log 2 \;\le\; 2^{k+2}\log 2.$$

Zu gegebenem $n \in \mathbb{N}$ sei $k \in \mathbb{N}_0$ mit $2^k \leq n < 2^{k+1}$. Dann gilt für $0 < y < n$

$$\begin{aligned}\Big(\pi(n) - \pi(y)\Big) \log y &= \sum_{y<p\leq n} \log y \leq \sum_{y<p\leq n} \log p \leq \vartheta(n) \\ &\leq \vartheta(2^{k+1}) \leq 2^{k+2} \log 2 \leq 4n \log 2,\end{aligned}$$

speziell für $y = n^{2/3}$ also

$$\pi(n) \frac{2}{3} \log n \leq \underbrace{\pi(n^{2/3})}_{\leq n^{2/3}} \frac{2}{3} \log n + 4n \log 2,$$

und damit

$$\pi(n) \leq n^{2/3} + \frac{3}{2} \frac{4n \log 2}{\log n} = \frac{n}{\log n} \Big(\frac{\log n}{n^{1/3}} + 6 \log 2 \Big).$$

Da $x \mapsto \dfrac{\log x}{x^{1/3}}$ an $x = \mathrm{e}^3$ maximal wird, folgt

$$\pi(n) \leq \frac{n}{\log n} \Big(\frac{3}{\mathrm{e}} + 6 \log 2 \Big) < 6 \frac{n}{\log n}.$$

□

Bemerkung 2.14 Ein äußerst schwieriges Problem ist die konkrete Bestimmung großer Primzahlen. Ein möglicher Ansatz liegt darin, Primzahlen der Form

$$2^k - 1 \text{ oder } 2^k + 1$$

mit $k \in \mathbb{N}$ zu suchen. Dabei gilt:

1. Ist $2^k - 1 \in \mathbb{P}$, so ist $k \in \mathbb{P}$.
2. Ist $2^k + 1 \in \mathbb{P}$, so ist $k = 2^n$ für ein $n \in \mathbb{N}_0$.

Denn: Wir verwenden im Weiteren immer wieder: Sind $x \in \mathbb{Z}$ und $m \in \mathbb{N}$, so gilt

$$(x-1) \Big| \Big((x-1) \sum_{j=0}^{m-1} x^j = x^m - 1 \Big)$$

und im Falle, dass m ungerade ist,

$$(x+1) | (x^m + 1)$$

(da $x + 1 = -(-x - 1)$ und $x^m + 1 = -((-x)^m - 1)$).

1. Es sei $k \in \mathbb{N} \setminus \mathbb{P}$. Dann ist $k = 1$, also $2^k - 1 = 1 \notin \mathbb{P}$, oder $k = r \cdot s$ mit gewissen $r, s \in \mathbb{N} \setminus \{1\}$, also $(2^r - 1) | \Big((2^r)^s - 1 = 2^k - 1 \Big)$ mit $1 < 2^r - 1 < 2^k - 1$, und damit wieder $2^k - 1 \notin \mathbb{P}$.

2. Es sei nun $k \in \mathbb{N}$, aber $k \neq 2^n$ für jedes $n \in \mathbb{N}_0$, also $k = 2^m s$ für ein $m \in \mathbb{N}_0$ und ein $s \in \mathbb{N} \setminus \{1\}$ mit s ungerade. Dann gilt $(2^{2^m} + 1) | \Big((2^{2^m})^s + 1 = 2^k + 1 \Big)$ mit $1 < 2^{2^m} + 1 < 2^k + 1$. Also ist $2^k + 1 \notin \mathbb{P}$.

Man nennt $M_k := 2^k - 1$ **k-te Mersenne-Zahl** und $F_n := 2^{2^n} + 1$ **n-te Fermat-Zahl**. Man kann zeigen:

1. Es gilt $M_p \in \mathbb{P}$ unter anderem für $p \in \{2, 3, 5, 7, 13, 17, 19\}$. Mindestens 48 Mersenne-Zahlen sind prim, die größte bis 2013 als Primzahl identifizierte Mersenne-Zahl ist $2^{57885161} - 1$, mit 17425170 Stellen im Dezimalsystem; siehe dazu die Webseite https://primes.utm.edu/mersenne/index.html#known von Chris K. Caldwell. Andererseits ist

$$M_{11} \;=\; 2^{11} - 1 \;=\; 2047 \;= 23 \cdot 89 \;\notin\; \mathbb{P}.$$

   Bis heute weder bekannt, ob M_p für unendlich viele $p \in \mathbb{P}$ prim ist, noch ob M_p für unendlich viele $p \in \mathbb{P}$ nicht prim ist.

2. Es gilt $F_n \in \mathbb{P}$ für $n \in \{0, 1, 2, 3, 4\}$, aber $F_5 = 2^{2^5} + 1 = 2^{32} + 1 \notin \mathbb{P}$.

   (Denn (Euler, 1732): Es ist $641 = 5^4 + 2^4 = 5 \cdot 2^7 + 1$ und

$$(5^4 + 2^4) | (5^4 2^{28} + 2^{32}), \quad (5 \cdot 2^7 + 1) | (5^4 2^{28} - 1)$$

   (beachte: $(a+1) | (a+1)(a-1)(a^2+1) = a^4 - 1$). Also gilt auch $641 | 2^{32} + 1 = F_5$.)

   Unter den Fermat-Zahlen sind bis heute keine Primzahlen außer $F_0, \ldots, F_4$ bekannt.

3 Restklassenringe und Anwendungen

Wir betrachten in diesem Abschnitt spezielle, für die Zahlentheorie wichtige Gruppen und Ringe.

Bemerkung und Definition 3.1 Es sei $m \in \mathbb{N}_0$. Für $a, a' \in \mathbb{Z}$ setzen wir

$$a \equiv a' \bmod m \ :\Leftrightarrow\ a \equiv_m a' \ :\Leftrightarrow\ m|(a-a') \ \Leftrightarrow\ a - a' \in m\mathbb{Z}.$$

Damit ist $\equiv_m$ eine Äquivalenzrelation auf $\mathbb{Z}$, genannt **Kongruenz modulo** m.

(Denn: Die Symmetrie und die Reflexivität von $\equiv_m$ sind klar. Die Transitivität aber auch, denn $m|(a-a')$ und $m|(a'-a'')$ implizieren zusammen $m|(a-a'+a'-a'')$, also $m|(a-a'')$.)

Für $a \in \mathbb{Z}$ ist die zugehörige Äquivalenzklasse $[a] := [a]_m := \{a' \in \mathbb{Z} : a \equiv_m a'\}$ gegeben durch $a + m\mathbb{Z}$, denn wir haben die Äquivalenzkette

$$a' \in [a] \Leftrightarrow a' \equiv_m a \Leftrightarrow a' - a \in m\mathbb{Z} \Leftrightarrow a' \in a + m\mathbb{Z}.$$

Dabei ist speziell $a + 0\mathbb{Z} = \{a\}$.

Man nennt $[a]_m$ **Restklasse modulo** m und schreibt $\mathbb{Z}_m$ für die Quotientenmenge $\mathbb{Z}/_{\equiv_m} = \{[a]_m : a \in \mathbb{Z}\}$. Damit ist dann

$$\mathbb{Z}_m \ = \ \begin{cases} \{[0]_m, [1]_m, \ldots, [m-1]_m\} & m\text{-elementig} \quad \text{falls } m > 0, \\ \{\{a\} : a \in \mathbb{Z}\} & \text{falls } m = 0. \end{cases}$$

(*Denn*: Die Behauptung ist klar für $m = 0$. Ist $m > 0$, so existiert zu $a \in \mathbb{Z}$ nach Satz 1.9 genau ein Paar $(q, r) \in \mathbb{Z}^2$ mit $a = qm + r$ und $0 \le r \le m-1$, also genau ein $r \in \{0, \ldots, m-1\}$ mit $a \equiv_m r$, also $a \in [r]$ für genau ein $r \in \{0, \ldots, m-1\}$.)

Auf $\mathbb{Z}_m$ sind durch

$$\begin{aligned} [a]_m + [b]_m &:= [a+b]_m \quad \text{für } a, b \in \mathbb{Z}, \\ [a]_m \cdot [b]_m &:= [ab]_m \quad \text{für } a, b \in \mathbb{Z} \end{aligned}$$

zwei Verknüpfungen $+$ und $\cdot$ wohldefiniert. Mit diesen ist $(\mathbb{Z}_m, +, \cdot)$ ein kommutativer Ring, mit dem Nullelement $[0]_m$ und dem Einselement $[1]_m$, und heißt der **Restklassenring** zum **Modul** m.

(*Denn*: $+$ und $\cdot$ sind wohldefiniert, da für $a, a', b, b' \in \mathbb{Z}$ mit $[a] = [a']$ und $[b] = [b']$ unter Verwendung von Satz 2.2.3 erstens $(a+b) - (a'+b') = a - a' + b - b' \in m\mathbb{Z}$ und damit $[a+b] = [a'+b']$ gilt, und zweitens $ab - a'b' = a\,(b-b') + (a-a')\,b' \in m\mathbb{Z}$ und damit $[ab] = [a'b']$. Dass $+$ und $\cdot$ Verknüpfungen sind ist klar. Die weiteren Behauptungen ergeben sich unmittelbar aus den eben als legal erkannten repräsentantenweisen Definitionen der Addition und der Multiplikation unter Verwendung der entsprechenden Eigenschaften in $(\mathbb{Z}, +, \cdot)$.)

Definition 3.2 Ein Ring heißt **nullteilerfrei** wenn für beliebige $x, y \in R$ aus $xy = 0$ schon $x = 0$ oder $y = 0$ folgt. Ein kommutativer und nullteilerfreier Ring mit Einselement $1 \neq 0$ heißt **Integritätsring** oder **Integritätsbereich**. Ein kommutativer Ring R mit Einselement 1, für den $(R \setminus \{0\}, \cdot, 1)$ eine Gruppe ist[4] heißt **Körper**.

Bemerkung 3.3 1. Jeder Körper ist ein Integritätsbereich, denn für $x, y \in R \setminus \{0\}$ ist auch $xy \in R \setminus \{0\}$, da $\cdot$ eine Verknüpfung auf $R \setminus \{0\}$ ist. Außerdem gilt: Ist R ein kommutativer Ring mit $1 \neq 0$ und so, dass jedes $a \neq 0$ invertierbar ist, so ist R schon ein Körper (sind $x, y \in R \setminus \{0\}$, so ist $0 \neq y = x^{-1}xy$, also $xy \neq 0$).

2. Ein Ring R ist genau dann nullteilerfrei, wenn für $x, y, z \in R$ folgende **Kürzungsregeln** gelten:

$$\left.\begin{array}{l} xy = xz \\ yx = zx \end{array}\right\} \Rightarrow \; x = 0 \text{ oder } y = z.$$

(*Denn*: Gelten die Kürzungsregeln, so ist R nullteilerfrei (wähle $z = 0$). Die Gleichung $xy = xz$ ist äquivalent zu $x(y - z) = 0$. Ist nun R nullteilerfrei, so folgt aus $xy = xz$ direkt $x = 0$ oder $y - z = 0$, also $x = 0$ oder $y = z$. Entsprechendes gilt für die zweite Kürzungsregel.)

Beispiel 3.4 1. $(\mathbb{Z}, +, \cdot)$ ist ein Integritätsring, aber kein Körper; $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +\cdot)$ sind Körper.

2. Für den Restklssenring $\mathbb{Z}_4$ gilt

$$\mathbb{Z}_4 \;=\; \Big\{[0]_4, [1]_4, [2]_4, [3]_4\Big\}$$

und etwa

$$[2]_4 + [3]_4 = [5]_4 \;=\; [1]_4$$

sowie

$$[2]_4[2]_4 \;=\; [4]_4 \;=\; [0]_4\,.$$

Damit ist $(\mathbb{Z}_4, +, \cdot)$ nicht nullteilerfrei, also kein Integritätsring (und erst recht kein Körper). Als Nullteiler kann $[2]_4$ kein multiplikatives Inverses haben, was man auch leicht durch Ausprobieren der nur vier Möglichkeiten sieht, d.h. die Gleichung $[2]_4 \cdot [x]_4 = [1]_4$, oder äquivalent die Kongruenz $2x \equiv 1 \mod 4$, hat keine Lösung.

Eine nette Anwendung von Kongruenzen sind einfache Teilbarkeitskriterien:

Satz 3.5 *Es sei $n \in \mathbb{N}$ mit der Dezimaldarstellung $n = a_r a_{r-1} \ldots a_0$. Dann gilt:*

[4] Genauer müsste man, da vereinbarungsgemäß $\cdot$ die Multiplikation auf ganz R bezeichnen soll, hier eigentlich $(R \setminus \{0\}, \cdot|_{R\setminus\{0\} \times R\setminus\{0\}}, 1)$ schreiben.

1. $n \equiv \sum_{j=0}^{r} a_j \mod 3$,

2. $n \equiv \sum_{j=0}^{r} a_j \mod 9$,

3. $n \equiv \sum_{j=0}^{r} (-1)^j a_j \mod 11$.

Beweis. Für jedes $m \in \mathbb{N}$ gilt

$$[n]_m = \left[\sum_{j=0}^{r} a_j \cdot 10^j\right]_m = \sum_{j=0}^{r} [a_j]_m [10]_m^j.$$

Speziell für $m \in \{3, 9\}$ ist $[10]_m = [1]_m$ und damit

$$[n]_m = \sum_{j=0}^{r} [a_j]_m = \left[\sum_{j=0}^{r} a_j\right]_m$$

und wir erhalten die ersten beiden Aussagen. Speziell für $m = 11$ ist $[10]_m = [-1]_m$ und damit (den Modul m in der Notation weglassend)

$$[n] = \sum_{j=0}^{r} [a_j][-1]^j = \sum_{j=0}^{r} [a_j][(-1)^j] = \left[\sum_{j=0}^{r} a_j (-1)^j\right]$$

und wir erhalten die dritte Aussage. □

Zurück zur allgemeinen Theorie der Ringe $\mathbb{Z}_m$: Wir haben in Beispiel 3.4.2 gesehen, dass $(\mathbb{Z}_m \setminus \{0\}, \cdot, [1]_m)$ im Allgemeinen keine Gruppe ist. Die Invertierbarkeit eines gegebenen Elements von $\mathbb{Z}_m$ klärt nun

Satz 3.6 *Es sei $m \in \mathbb{N}$. Dann gilt: Zu $a \in \mathbb{Z}$ existiert genau dann ein $x \in \mathbb{Z}$ mit $ax \equiv 1 \mod m$, also äquivalent dazu $[a]_m \cdot [x]_m = [1]_m$, wenn $\mathrm{ggT}(a, m) = 1$ ist.*

Beweis. Es gilt $ax \equiv 1 \mod m$ für ein $x \in \mathbb{Z}$ genau dann, wenn $1 \in ax + m\mathbb{Z}$ für ein $x \in \mathbb{Z}$, also genau dann, wenn $1 \in a\mathbb{Z} + m\mathbb{Z}$. Nach Satz 2.4 gilt dies genau dann, wenn $\mathrm{ggT}(a, m) = 1$ ist. □

Bemerkung und Definition 3.7 Sei $m \in \mathbb{N}$. Für das Monoid $(\mathbb{Z}_m, \cdot, [1]_m)$ ist die (abelsche) Gruppe seiner invertierbaren Elemente

$$\mathbb{Z}_m^* = \{[a]_m : a \in \{0, \ldots, m-1\}, \mathrm{ggT}(a, m) = 1\}$$

mit $[0]_m \notin \mathbb{Z}_m^*$ für $m \geq 2$.

(*Denn*: Nach Bemerkung 1.4.2 ist die Menge $\mathbb{Z}_m^*$ der invertierbaren Elemente von $\mathbb{Z}_m$ bezüglich $\cdot$ eine Gruppe. Die behauptete Darstellung von $\mathbb{Z}_m^*$ ergibt sich aus der Darstellung von $\mathbb{Z}_m$ aus Bemerkung/Definition 3.1 mittels Satz 3.6.)

Die Elemente von $\mathbb{Z}_m^*$ heißen **prime Restklassen modulo** m.

Beispiel 3.8 $\mathbb{Z}_4^* = \big\{[1]_4, [3]\big\}$ ist eine zweielementige Gruppe (bezüglich $\cdot$).

Satz 3.9 *Es sei $p \in \mathbb{P}$. Dann ist*

$$\mathbb{Z}_p^* \;=\; \Big\{[1]_p, [2]_p, \ldots, [p-1]_p\Big\} \;=\; \mathbb{Z}_p \setminus \{[0]_p\}$$

und

$$\boxed{(\mathbb{Z}_p, +, \cdot) \quad \textit{ein Körper}}$$

mit p Elementen.

Beweis. Da p prim ist, gilt $\mathrm{ggT}(a, p) = 1$ für $a \in \{1, \ldots, p-1\}$ und damit $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{[0]_p\}$ nach Bemerkung/Definition 3.7. Also ist $(\mathbb{Z}_p \setminus \{[0]_p\}, \cdot, [1]_p)$ eine Gruppe, und folglich der kommutative Ring $(\mathbb{Z}_p, +, \cdot)$ ein Körper. □

Bemerkung 3.10 Ist $m \in \mathbb{N} \setminus \mathbb{P}$, so ist der Ring $(\mathbb{Z}_m, +, \cdot)$ kein Körper, denn entweder ist $m = 1$ und damit $\mathbb{Z}_1 = \{[0]_1\}$ kein Körper oder es existiert ein $a \in \{2, \ldots, m-1\}$ mit $a|m$, also $([0]_m \neq)\, [a]_m \notin \mathbb{Z}_m^*$ nach Bemerkung/Definition 3.7.

Definition 3.11 Es seien $(M, \cdot)$ eine Halbgruppe und $U \subset M$. Dann heißt U eine **Unterhalbgruppe**, falls $(U, \cdot|_{U\times U})$ eine Halbgruppe ist. Ist $(M, \cdot, e)$ ein Monoid und ist U Unterhalbgruppe von M mit $e \in U$, so heißt U **Untermonoid** von M. Sind dabei $(M, \cdot, e)$ und $(U, \cdot|_{U\times U}, e)$ Gruppen, so heißt U **Untergruppe** von M.

Man schreibt in den obigen Fällen jeweils wieder $\cdot$ statt $\cdot|_{U\times U}$.

Wir konzentrieren uns nun auf Gruppen.

Bemerkung 3.12 Es seien $(G, \cdot, e)$ eine Gruppe und $U \subset G$, $U \neq \emptyset$. Dann sind die folgenden Aussagen äquivalent:

(i) U ist Untergruppe von G.
(ii) $e \in U$ und aus $a, b \in U$ folgt $a^{-1} \in U$, $ab \in U$.
(iii) Aus $a, b \in U$ folgt $a^{-1}b \in U$.

Ist U endlich, so ist außerdem (i) äquivalent zu:

(iv) Aus $a, b \in U$ folgt $ab \in U$.

(*Denn*: (i) $\Rightarrow$ (ii): Es gelte (i). Nach Definition ist $e \in U$. Sind $a, b \in U$, so ist $ab \in U$ da $\cdot|_{U\times U}$ eine Verknüpfung auf U ist. Außerdem ist $a^{-1} \in U$ aufgrund der Eindeutigkeit der Inversen (in G). Folglich gilt (ii).

(ii) $\Rightarrow$ (i): Klar.

(ii) $\Rightarrow$ (iii): Klar.

(iii) $\Rightarrow$ (ii): Es gelte (iii). Ist $a \in U$, so ist zunächst $e = a^{-1}a \in U$ und damit auch $a^{-1} = a^{-1}e$, also wiederum für $b \in U$ auch $ab = (a^{-1})^{-1}b \in U$.

(ii) $\Rightarrow$ (iv): Klar.

U endlich und (iv) $\Rightarrow$ (iii): Es sei $a \in U$ fixiert. Dann ist die Abbildung

$$U \ni x \mapsto ax \in aU := \{ax : x \in U\}$$

wegen der Existenz von a^{-1} injektiv, also Bijektion, und es gilt nach Voraussetzung $aU \subset U$, so dass wegen der Endlichkeit von U schon $aU = U$ gelten muss. Daher existiert zu jedem $b \in U$ ein $x \in U$ mit $ax = b$, also $a^{-1}b = x \in U$. Damit gilt (iii).)

Beispiele 3.13 1. Ist $(G, \cdot, e)$ eine beliebige Gruppe, so sind $U = G$ und $U = \{e\}$ stets Untergruppen, die sogenannten **trivialen Untergruppen**.
2. Ist $G = (\mathbb{C}, +, 0)$, so haben wir folgende Kette ineinandergeschachtelter Untergruppen:

$$\{0\} \subset m\mathbb{Z} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \quad \text{für } m \in \mathbb{N}.$$

3. Ist $G = (\mathbb{C} \setminus \{0\}, \cdot, 1)$, so haben wir folgende Inklusionen von Untergruppen:

$$\{1\} \subset \left\{ \begin{matrix} \{-1, 1\} \subset \mathbb{Q} \setminus \{0\} \\ \mathbb{Q}_+ \subset \mathbb{R}_+ \end{matrix} \right\} \subset \mathbb{R} \setminus \{0\} \subset \mathbb{C} \setminus \{0\}.$$

Bemerkung und Definition 3.14 Ist $(G, \cdot, e)$ eine Gruppe und ist $\mathcal{U}$ eine Menge von Untergruppen, so ist auch $\bigcap \mathcal{U} = \bigcap_{U\in\mathcal{U}} U$ eine Untergruppe[5], denn es gilt $e \in \bigcap \mathcal{U}$, und mit $a, b \in \bigcap \mathcal{U}$ ist auch $a^{-1}b \in \bigcap \mathcal{U}$.

Ist nun $M \subset G$ eine beliebige Teilmenge, so heißt

$$\langle M \rangle := \bigcap_{U \supset M,\, U \text{ Untergruppe}} U,$$

also $\bigcap \mathcal{U}$ mit $\mathcal{U} := \{U \supset M : U \text{ Untergruppe von } G\}$, die **von M erzeugte Untergruppe**. M heißt dann auch ein **Erzeugendensystem** von $\langle M \rangle$. Ist speziell $M = \{a\}$, so schreiben wir kurz $\langle a \rangle$ statt $\langle \{a\} \rangle$ und nennen a ein **erzeugendes Element** von $\langle a \rangle$.

[5] Dies gilt auch im Fall von $\mathcal{U} = \emptyset$, in welchem $\bigcap \mathcal{U} := G$ ist.

Unter Verwendung der vor Satz 1.10 eingeführten Schreibweisen zeigen wir

Satz 3.15 *Es seien G eine Gruppe und $M \subset G$, $M \neq \emptyset$. Dann gilt*

1. $\langle M\rangle = \bigcup\limits_{n\in\mathbb{N}} \Big\{ \prod\limits_{j=1}^{n} a_j^{\varepsilon_j} : a_j \in M,\, \varepsilon_j \in \{-1,1\}\ (j=1,\dots,n)\Big\}$.

2. *Ist G abelsch, so ist auch* $\langle M\rangle = \Big\{ \prod\limits_{a\in M} a^{\nu_a} : (\nu_a)_{a\in M} \in \mathbb{Z}^{(M)}\Big\}$.

Beweis. 1. Es sei U_1 die rechte Seite in 1.

$\langle M\rangle \subset U_1$: Es gilt $M \subset U_1$ und U_1 ist eine Untergruppe von G nach Kriterium 3.12.(iii), denn mit $a, b \in U_1$, wobei $a = a_1^{\varepsilon_1}\cdots a_n^{\varepsilon_n}$ und $b = b_1^{\delta_1}\cdots b_m^{\delta_m}$ mit $a_j, b_k \in M$ und $\varepsilon_j, \delta_k \in \{-1,1\}$, ist auch

$$a^{-1}b \;=\; a_n^{-\varepsilon_n}\cdots a_1^{-\varepsilon_1}\cdot b_1^{\delta_1}\cdots b_m^{\delta_m} \;\in\; U_1.$$

Also ist nach Definition $\langle M\rangle \subset U_1$.

$U_1 \subset \langle M\rangle$: Ist U eine Untergruppe von G mit $M \subset U$, so gilt $U_1 \subset U$ nach dem Kriterium 3.12(ii); also ist $U_1 \subset \langle M\rangle$.

2. Nun sei G abelsch und U_2 die rechte Seite in 2.

$U_2 \subset \langle M\rangle$: Genauso wie $U_1 \subset \langle M\rangle$.

$U_1 \subset U_2$: Sind $a_1, \dots a_n \in M$ sowie $\varepsilon_1, \dots, \varepsilon_n \in \{-1,1\}$ und setzt man $\nu_a := \sum\limits_{j:a_j=a} \varepsilon_j$ $(a \in M)$, so gilt

$$a_1^{\varepsilon_1}\cdot \ldots \cdot a_n^{\varepsilon_n} \;=\; \prod_{a\in M} a^{\nu_a} \;\in\; U_2.$$

□

Bemerkung und Definition 3.16 Es sei G eine Gruppe.

1. Für $a \in G$ ist nach Satz 3.15

$$\langle a\rangle \;=\; \{a^k : k \in \mathbb{Z}\}$$

die von a erzeugte Untergruppe. G heißt **zyklisch**, falls $\langle a\rangle = G$ für ein $a \in G$ gilt.

2. Für eine Untergruppe U von G heißt

$$\operatorname{ord} U \;:=\; \#U \;\in\; \mathbb{N}\cup\{\infty\}$$

die **Ordnung** von U, und speziell

$$\operatorname{ord} a \;:=\; \operatorname{ord}\langle a\rangle$$

die **Ordnung** von a.

Beispiele 3.17 1. Es sei $G = (\mathbb{Z}, +, 0)$. Dann gilt $\langle a \rangle = a\mathbb{Z}$ für $a \in \mathbb{Z}$, und insbesondere

$$\mathbb{Z} \;=\; \langle 1 \rangle \;=\; \langle -1 \rangle.$$

Also ist $\mathbb{Z}$ zyklisch und ± 1 sind erzeugende Elemente (und zwar die einzigen).

2. Ist $G = (\mathbb{Z}_m, +, [0])$, so gilt $\langle [a] \rangle = \{k[a] : k \in \mathbb{Z}\} = \{[ka] : k \in \mathbb{Z}\}$, also insbesondere

$$\mathbb{Z}_m \;=\; \langle [1] \rangle$$

zyklisch. Allgemeiner ist $\mathbb{Z}_m = \langle [a] \rangle$ für ein $a \in \mathbb{Z}$ genau dann, wenn $[a]$, eine prime Restklasse modulo m ist, was man sich mit Satz 3.6 überlegt.

Satz 3.18 *Es seien G eine Gruppe und $x \in G$. Dann gilt* $\operatorname{ord}(x) < \infty$ *genau dann, wenn ein $n \in \mathbb{N}$ existiert mit $x^n = e$. In diesem Fall ist* $\operatorname{ord}(x) = \min\{n \in \mathbb{N} : x^n = e\}$ *und*

$$x^{k \operatorname{ord}(x) + j} = x^j \qquad \text{für } k, j \in \mathbb{Z}.$$

Außerdem gilt für $n \in \mathbb{Z}$

$$x^n = e \;\Leftrightarrow\; \operatorname{ord}(x) | n.$$

Beweis. $\Rightarrow$: Angenommen, es gibt kein $n \in \mathbb{N}$ mit $x^n = e$. Für $j, k \in \mathbb{Z}$ mit $j < k$ gilt dann $x^{k-j} \neq e$, also $x^j \neq x^k$. Folglich ist $\operatorname{ord}(x) = \infty$, im Widerspruch zur Voraussetzung.

$\Leftarrow$ und Zusatzbehauptung: Nach Voraussetzung existiert

$$m \;:=\; \min\{n \in \mathbb{N} : x^n = e\}.$$

Für $k, j \in \mathbb{Z}$ gilt damit

$$x^{km+j} \;=\; (x^m)^k x^j \;=\; x^j.$$

Ist $n \in \mathbb{Z}$, so ist $n = km + j$ mit $k \in \mathbb{Z}$ und $j \in \{0, \ldots, m-1\}$ nach Satz 1.9 (Division mit Rest). Also ist

$$\langle x \rangle = \{x^n : n \in \mathbb{Z}\} = \{x^0, x^1, \ldots, x^{m-1}\}.$$

Weiter ist die Funktion $\{0, \ldots, m-1\} \ni j \mapsto x^j$ injektiv, denn sonst gäbe es $j, k \in \{0, \ldots, m-1\}$ mit $j < k$ und $x^j = x^k$, also $x^{k-j} = e$ mit $1 \leq k - j < m$ im Widerspruch zur Minimalität von m. Also ist $\operatorname{ord} x = \operatorname{ord} \langle x \rangle = m$.

Außerdem ist $x^n = e$ genau dann, wenn $j = 0$ ist, also genau dann, wenn $m | n$. $\square$

Bemerkung und Definition 3.19 Es seien G eine Gruppe und $H \subset G$ eine Untergruppe. Setzt man für $a, a' \in G$

$$a \sim a' :\Leftrightarrow a^{-1}a' \in H \quad (\Leftrightarrow a' \in aH := \{ax : x \in H\}),$$

so sieht man leicht, dass $\sim$ eine Äquivalenzrelation auf G ist; die Äquivalenzklassen sind dann gerade die Mengen aH mit $a \in G$, genannt **Linksnebenklassen** von H.

Durch Betrachtung von $a'a^{-1}$ anstelle von $a^{-1}a'$ erhält man entsprechend die **Rechtsnebenklassen** Ha von H. Für abelsche Gruppen gilt natürlich $aH = Ha$ für $a \in G$. Stets (also auch im nichtabelschen Fall) ist für $a \in G$ wegen der Injektivität von $H \ni x \mapsto ax$ und von $H \ni x \mapsto xa$

$$\#(aH) \;=\; \operatorname{ord} H \;=\; \#(Ha).$$

Weiter setzen wir

$$G/H := G/_H \;:=\; \{aH : a \in G\} \quad \text{und} \quad {}_H\backslash G \;:=\; \{Ha : a \in G\}\,.$$

Dann gilt ([Ü]): $\#(G/_H) = \#({}_H\backslash G)$ und der gemeinsame Wert

$$G : H \;:=\; \#(G/_H) \;\in\; \mathbb{N} \cup \{\infty\}$$

heißt **Index** von H (in G).

Beispiel 3.20 Es seien $G = (\mathbb{Z}, +, 0)$, $m \in \mathbb{N}$ und $H := m\mathbb{Z}$. Dann gilt

$$Ha \;=\; aH \;=\; a + m\mathbb{Z} \;=\; [a]_m \quad \text{für } a \in G,$$

d. h. Links- und Rechtsnebenklassen sind hier gerade die Restklassen modulo m. Weiter ist $G/_H = \mathbb{Z}_m$ und damit $G : H = m$.

Satz 3.21 *(Lagrange).*
Es seien G eine endliche Gruppe und H eine Untergruppe. Dann gilt

$$\operatorname{ord} G = \operatorname{ord} H \cdot (G : H)\,.$$

Beweis. Die Linksnebenklassen aH bilden als Äquivalenzklassen ein Zerlegung von G (also $G = \bigcup_{aH \in G/_H} aH$ und $aH \cap bH = \emptyset$ falls $aH \neq bH$). Damit ist

$$\operatorname{ord} G = \sum_{aH \in G/_H} \#(aH) = \sum_{aH \in G/_H} \operatorname{ord} H = \operatorname{ord} H \cdot (G : H).$$

□

Bemerkung 3.22 Als Anwendung des Satzes von Lagrange ergibt sich: Ist G eine endliche Gruppe und ist $x \in G$, so gilt

$$\operatorname{ord}(x) | \operatorname{ord}(G) \quad \text{und} \quad x^{\operatorname{ord}(G)} = e.$$

(*Denn*: Satz 3.21 mit $H := \langle x \rangle$ liefert $\operatorname{ord}(G) = \operatorname{ord}(x) \cdot \Big(G : \langle x \rangle\Big)$, also ist $\operatorname{ord}(x)$ ein Teiler von $\operatorname{ord}(G)$. Mit Satz 3.18 folgt $x^{\operatorname{ord}(G)} = e$).

Durch Anwendung auf die Gruppen $(\mathbb{Z}_m^*, \cdot, [1])$ ergeben sich rein zahlentheoretische Konsequenzen, in deren Formulierung der Begriff Gruppe nicht vorkommt.

Definition 3.23 Die durch

$$\varphi(m) \;:=\; \operatorname{ord}(\mathbb{Z}_m^*) \;=\; \#\{a \in \{0, \ldots, m-1\} : \operatorname{ggT}(a, m) = 1\} \qquad (m \in \mathbb{N})$$

definierte Funktion heißt **Eulersche φ-Funktion**.

Offenbar gilt $\varphi(1) = 1$ und $\varphi(p) = p - 1$ für $p \in \mathbb{P}$ nach Satz 3.9.

Satz 3.24

1. (Euler) Sind $m \in \mathbb{N}$ und $a \in \mathbb{Z}$ teilerfremd, so gilt

$$a^{\varphi(m)} \equiv 1 \mod m.$$

2. (kleiner Satz von Fermat) Sind $p \in \mathbb{P}$ und $a \in \mathbb{Z}$ und ist p kein Teiler von a, so gilt

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

Beweis. 1. Bemerkung 3.22 angewandt auf $G = (\mathbb{Z}_m^*, \cdot, [1])$ liefert

$$[1]_m \;=\; [a]_m^{\operatorname{ord}(\mathbb{Z}_m^*)} \;=\; [a]_m^{\varphi(m)} \;=\; \left[a^{\varphi(m)}\right]_m,$$

also $a^{\varphi(m)} \equiv 1 \mod m$.

2. Ist p kein Teiler von a, so ist $\operatorname{ggT}(a, p) = 1$, da $p \in \mathbb{P}$, und nach 1. ist dann

$$a^{p-1} \;=\; a^{\varphi(p)} \;\equiv\; 1 \mod p.$$

□

Bemerkung und Definition 3.25 Nach dem Fermatschen Satz 3.24.2 gilt für $n \in \mathbb{N}$:

$$\textit{Existiert ein } a \in \mathbb{N} \textit{ mit } ggT(a,n) = 1 \textit{ und } a^{n-1} \not\equiv 1 \mod n, \textit{ so ist } n \notin \mathbb{P}.$$

Dies kann somit als Test genutzt werden, um die Primalität einer natürlichen Zahl n auszuschließen. Ein Zahl $n \in \mathbb{N} \setminus (\mathbb{P} \cup \{1\})$ heißt **pseudoprim zur Basis** $a > 1$, falls $a^{n-1} \equiv 1 \mod n$ gilt. Wir werden im nächsten Abschnitt sehen, dass es Zahlen gibt, die pseudoprim zu „vielen“ Basen a sind. Daher kann man obigen Ansatz nicht ohne Weiteres nutzen, um von einer Zahl nachzuweisen, dass sie prim ist[6].

[6] Eine gewisse Modifikation ist jedoch Grundlage eines Algorithmus, der von jeder natürlichen Zahl n in polynomialer Zeit entscheidet, ob sie prim ist oder nicht. Siehe Agrawal, M., Kayal, N., und Saxena, N. (2004), PRIMES is in P, *Annals of Mathematics* **160**, 781–793.

4 Lineare Kongruenzen und Anwendungen

Wir betrachten jetzt "lineare Modulogleichungen", genannt **lineare Kongruenzen** der Form

$$[a]_m[x]_m \;=\; [b]_m$$

im Restklassenring $\mathbb{Z}_m$ und damit im Allgemeinen nicht in einem Körper; siehe Bemerkung 3.10.

Satz 4.1 *Es seien $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$, und $d := \mathrm{ggT}(a, m)$.*

1. Die Gleichung

$$ax \;\equiv\; b \mod m, \tag{4.1}$$

hat genau dann eine Lösung $x \in \mathbb{Z}$, wenn d ein Teiler von b ist. In diesem Fall löst $x \in \mathbb{Z}$ die Gleichung (4.1) genau dann, wenn x Lösung der (wegen $a/d, b/d \in \mathbb{Z}$ und $m/d \in \mathbb{N}$ sinnvollen) Gleichung

$$\frac{a}{d}\,x \;\equiv\; \frac{b}{d} \mod \frac{m}{d}. \tag{4.2}$$

2. Ist $x \in \mathbb{Z}$ eine Lösung von (4.2), so ist $L := \{x + k\frac{m}{d} : k \in \{0, \ldots, d-1\}\}$ eine d-elementige Menge paarweise modulo m inkongruenter Lösungen von (4.1) und die Lösungsmenge von (4.1) ist $L + m\mathbb{Z}$.

Beweis. 1. Die Gleichung (4.1) ist genau dann lösbar, wenn $x, y \in \mathbb{Z}$ existieren mit $ax + my = b$, also genau dann, wenn $b \in a\mathbb{Z} + m\mathbb{Z}$, d. h. $b \in d\mathbb{Z}$ nach Satz 2.4.

Es gelte nun $d|b$. Dann gilt für $x \in \mathbb{Z}$ die Äquivalenzkette

$$x \text{ löst } (4.1) \;\Leftrightarrow\; m|(ax-b) \;\Leftrightarrow\; \frac{m}{d}\Big|\Big(\frac{a}{d}\,x - \frac{b}{d}\Big) \;\Leftrightarrow\; x \text{ löst } (4.2).$$

2. Nach 1. können wir $d|b$ annehmen. Wegen $\mathrm{ggT}\big(a/d, m/d\big) = 1$ ist $[a/d]_{m/d} \in \mathbb{Z}^*_{m/d}$ nach Bemerkung/Definition 3.7, hat also ein Inverses $[c]_{m/d}$, und für $x \in \mathbb{Z}$ gilt die Äquivalenzkette

$$x \text{ löst } (4.2) \;\Leftrightarrow\; \Big[\frac{a}{d}\Big]_{\frac{m}{d}}[x]_{\frac{m}{d}} = \Big[\frac{b}{d}\Big]_{\frac{m}{d}} \;\Leftrightarrow\; [x]_{\frac{m}{d}} = \Big[\frac{cb}{d}\Big]_{\frac{m}{d}}.$$

Sind nun x Lösung von (4.2) und $y \in \mathbb{Z}$, so ergibt sich

$$\begin{aligned} y \text{ löst } (4.2) \;&\Leftrightarrow\; [y]_{\frac{m}{d}} = [x]_{\frac{m}{d}} \\ &\Leftrightarrow\; \text{Es gibt ein } n \in \mathbb{Z} \text{ mit } y = x + n\frac{m}{d} \\ &\Leftrightarrow\; \text{Es gibt } \ell \in \mathbb{Z} \text{ und } k \in \{0, \ldots, d-1\} \text{ mit } y = x + \ell m + k\frac{m}{d} \\ &\Leftrightarrow\; y \in L + m\mathbb{Z}. \end{aligned}$$

Für $j,k \in \{0,\dots,d-1\}$ mit $j \neq k$ und für $x \in \mathbb{Z}$ ist dabei $x + \frac{km}{d} \not\equiv x + \frac{jm}{d} \mod m$, wegen $|\frac{km}{d} - \frac{jm}{d}| < m$. Insbesondere ist damit auch $\#L = d$. □

Beispiele 4.2 1. Wir betrachten die Kongruenz

$$6x \equiv 3 \mod 27.$$

In der Notation von Satz 4.1 ist hier $a = 6, b = 3, m = 27$, also $d = \mathrm{ggT}(6,27) = 3$ und damit $d|b$. Daher ist die Kongruenz lösbar und wir betrachten (4.2), also

$$2x \equiv 1 \mod 9.$$

Eine Lösung ist $x = 5$. Also ist hier $L = \{5,14,23\}$ und $\{5,14,23\} + 27 \cdot \mathbb{Z}$ die Lösungsmenge von (4.1).

2. Die Kongruenz

$$6x \equiv 2 \mod 27$$

hat nach Satz 4.1 wegen $\mathrm{ggT}(6,27) = 3 \not| 2$ keine Lösung.

Von grundlegender Bedeutung ist das folgende Ergebnis über simultane Kongruenzen.

Satz 4.3 *Es seien $m_1,\dots,m_N \in \mathbb{N}$ paarweise teilerfremd und es sei $m := \prod_{j=1}^{N} m_j$.*

1. Für $x,x' \in \mathbb{Z}$ ist $x \equiv x' \mod m$ genau dann, wenn $x \equiv x' \mod m_j$ für $j \in \{1,\dots,N\}$ gilt.

2. Durch

$$f\big([x]_m\big) := \big([x]_{m_1},\dots,[x]_{m_n}\big) \quad \text{für } [x]_m \in \mathbb{Z}_m$$

wird eine Bijektion von $\mathbb{Z}_m$ auf $\bigtimes_{j=1}^{N} \mathbb{Z}_{m_j}$ wohldefiniert.

3. (Chinesischer Restsatz)[7] *Sind $b_1,\dots,b_N \in \mathbb{Z}$, so existiert ein $x \in \mathbb{Z}$ mit*

$$x \equiv b_j \mod m_j \quad \text{für } j \in \{1,\dots,N\}, \tag{4.3}$$

und mit jedem solchen x ist die Lösungsmenge von (4.3) dann $[x]_m = x + m\mathbb{Z}$.

[7] Der Name des Satzes geht auf die folgende Aufgabe im Handbuch der Arithmetik des Chinesischen Mathematikers Sun-Tse (etwa 3. Jahrhundert n. Chr.) zurück: *Es soll eine Anzahl von Dingen gezählt werden. Zählt man sie zu je drei, dann bleiben zwei übrig. Zählt man sie zu je fünf, dann bleiben drei übrig. Zählt man sie zu je sieben, dann bleiben zwei übrig. Wie viele sind es?* Die (minimale) Lösung berechnen wir in Beispiel 4.5.

Beweis. 1. Sind $x, x' \in \mathbb{Z}$, so gilt die Äquivalenz

$$m_j|(x - x') \quad \text{für } j \in \{1, \ldots, N\} \quad \Leftrightarrow \quad m|(x - x');$$

dabei ist "$\Leftarrow$" klar, und "$\Rightarrow$" ergibt sich unter Verwendung der paarweisen Teilerfremdheit der m_j induktiv mit Satz 2.6.2 und 2.6.3.

2. Nach 1. ist f wohldefiniert und injektiv. Wegen

$$\#\Big(\bigtimes_{j=1}^{N} \mathbb{Z}_{m_j}\Big) = \prod_{j=1}^{N} \#\mathbb{Z}_{m_j} \;=\; \prod_{j=1}^{N} m_j \;=\; m \;=\; \#\mathbb{Z}_m \;<\; \infty$$

ist f damit schon bijektiv.

3. Nach 2. existiert zu jedem Tupel $(b_1, \ldots, b_N) \in \mathbb{Z}^N$ genau ein $[x]_m \in \mathbb{Z}_m$ mit

$$([x]_{m_1}, \ldots, [x]_{m_N}) \;=\; f([x]_m) \;=\; ([b_1]_{m_1}, \ldots, [b_N]_{m_N}).$$

Damit gilt (4.3), und ein $y \in \mathbb{Z}$ ist genau dann Lösung von (4.3) wenn $y \in [x]_m$ gilt. □

Bemerkung 4.4 Die Berechnung einer Lösung von (4.3) lässt sich wie folgt auf die Berechnung je einer Lösung von N Gleichungen vom Typ (4.1) zurückführen:

Mit der Notation und den Voraussetzungen von Satz 4.3 sei für $j \in \{1, \ldots, N\}$

$$a_j \;:=\; \frac{m}{m_j}$$

und damit $\mathrm{ggT}(a_j, m_j) = 1$ nach Satz 2.6.3 (induktiv angewandt), so dass nach Satz 4.1 ein $x_j \in \mathbb{Z}$ existiert mit

$$a_j x_j \;\equiv\; b_j \mod m_j.$$

Damit ist

$$x \;:=\; \sum_{k=1}^{N} a_k x_k$$

eine Lösung von (4.3), denn für jedes j gilt $m_j | a_k$ für $k \neq j$, und damit ist

$$x \;\equiv\; a_j x_j \;\equiv\; b_j \mod m_j.$$

Beispiel 4.5 Wir betrachten das System

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

In der Notation von Bemerkung 4.4 ist hier $m_1 = 3$, $m_2 = 5$, $m_3 = 7$, $a_1 = 35$, $a_2 = 21$, $a_3 = 15$, $m = 105$. Lösungen $x_1, x_2, x_3 \in \mathbb{Z}$ der nun zu betrachtenden Kongruenzen

$$\begin{aligned} 35x_1 &\equiv 2 \mod 3 \\ 21x_2 &\equiv 3 \mod 5 \\ 15x_3 &\equiv 2 \mod 7 \end{aligned}$$

sind $x_1 = 1$, $x_2 = 3$, $x_3 = 2$. Damit ist

$$x \coloneqq a_1x_1 + a_2x_2 + a_3x_3 = 35 \cdot 1 + 21 \cdot 3 + 15 \cdot 2 = 128$$

eine Lösung des Ausgangssystems und die Lösungsmenge ist gegeben durch $128 + 105\mathbb{Z} = 23 + 105\mathbb{Z}$. Die minimale positive Lösung ist also 23.

Definition 4.6 1. Ist $n \in \mathbb{N}$ pseudoprim zur Basis a für jedes a mit $\mathrm{ggT}(a, n) = 1$, so heißt n eine **Carmichaelzahl**[8].

2. Eine Zahl $n \in \mathbb{N}$ heißt **quadratfrei**, falls für $d \in \mathbb{N}$ mit $d^2|n$ schon $d = 1$ ist. Dies ist genau dann der Fall, wenn $n = \prod_{p|n} p$ gilt ([Ü]).

Satz 4.7 *Es sei $n \in \mathbb{N} \setminus (\mathbb{P} \cup \{1\})$ quadratfrei mit $(p-1)|(n-1)$ für alle Primteiler p von n. Dann ist n eine Carmichael-Zahl.*

Beweis. Es sei $a > 1$ mit $\mathrm{ggT}(a, n) = 1$. Für jedes $p \in \mathbb{P}$ mit $p|n$ ist dann auch $\mathrm{ggT}(a, p) = 1$. Ist $n - 1 = k(p - 1)$, so folgt aus dem kleinen Satz von Fermat 3.24.2

$$1 \equiv (a^{p-1})^k = a^{(p-1)k} = a^{n-1} \mod p.$$

Wegen der Quadratfreiheit von n liefert nun Satz 4.3.1

$$a^{n-1} \equiv 1 \mod n. \qquad \square$$

Beispiel 4.8 Es ist $561 = 3 \cdot 11 \cdot 17$ und es gilt $2|560, 10|560$, und $16|560$. Also ist 561 nach Satz 4.7 eine Carmichael-Zahl (und genauer die kleinste).

Wir betrachten noch einmal die Eulersche φ-Funktion. Mit f aus Satz 4.3 gilt

[8] Man kann zeigen, dass unendlich viele Carmichaelzahlen existieren. Der Beweis von C. Pomerance, W. R. Alford und A. Granville stammt aus dem Jahr 1994.

Satz 4.9 *Es seien $m_1, \dots, m_N \in \mathbb{N}$ paarweise teilerfremd.*

1. *Die Restriktion $f|_{\mathbb{Z}_m^*}$ ist eine Bijektion von $\mathbb{Z}_m^*$ auf $\bigtimes_{j=1}^{N} \mathbb{Z}_{m_j}^*$.*
2. *Es gilt*

$$\boxed{\varphi\Big(\prod_{j=1}^{N} m_j\Big) \;=\; \prod_{j=1}^{N} \varphi(m_j)}$$

Beweis. 1. Für $[x]_m \in \mathbb{Z}_m$ gilt die Äquivalenzkette

$$\begin{aligned} [x]_m \in \mathbb{Z}_m^* \;&\Leftrightarrow\; \mathrm{ggT}(m,x) = 1 \\ &\Leftrightarrow\; \mathrm{ggT}(m_j,x) = 1 \quad \text{für } j \in \{1,\dots,N\} \\ &\Leftrightarrow\; [x]_{m_j} \in \mathbb{Z}_{m_j}^* \quad \text{für } j \in \{1,\dots,N\} \\ &\Leftrightarrow\; f\big([x]_m\big) \in \bigtimes_{j=1}^{N} \mathbb{Z}_{m_j}^* \end{aligned}$$

wegen Satz 3.7 für den ersten und den dritten Schritt, und Satz 2.6.3 für den zweiten. Da f injektiv ist, folgt die Behauptung.

2. Unter Benutzung von Teil 1. im dritten Schritt erhalten wir

$$\varphi\Big(\prod_{j=1}^{N} m_j\Big) \;=\; \varphi(m) \;=\; \#\mathbb{Z}_m^* \;=\; \#\Big(\bigtimes_{j=1}^{N} \mathbb{Z}_{m_j}^*\Big) \;=\; \prod_{j=1}^{N} \#\mathbb{Z}_{m_j}^* \;=\; \prod_{j=1}^{N} \varphi(m_j).$$

□

Satz 4.10 *Es gilt*

$$\varphi(n) = n \cdot \prod_{p|n} \Big(1 - \frac{1}{p}\Big) \qquad \textit{für } n \in \mathbb{N}$$

und insbesondere

$$\varphi(p^k) = p^k - p^{k-1} \qquad \textit{für } k \in \mathbb{N} \textit{ und } p \in \mathbb{P}.$$

Beweis. Es sei zunächst $p \in \mathbb{P}, k \in \mathbb{N}$. Dann ist

$$\Big\{a \in \big\{1,\dots,p^k\big\} \,:\, \mathrm{ggT}(a,p^k) = 1\Big\} \;=\; \{1,\dots,p^k\} \setminus \{p, 2p, \dots, p^{k-1}p\}$$

und folglich $\varphi(p^k) = p^k - p^{k-1}$.

Ist nun $n \in \mathbb{N}$, so gilt $n = \prod_{p|n} p^{\alpha_p(n)}$. Wegen der Teilerfremdheit von p^j und q^k für unterschiedliche Primzahlen p, q und beliebige Exponenten j, k erhalten wir unter

Verwendung von Satz 4.9 im ersten Schritt

$$\begin{aligned}\varphi(n) &= \prod_{p|n} \varphi(p^{\alpha_p(n)}) = \prod_{p|n} \left(p^{\alpha_p(n)} - p^{\alpha_p(n)-1}\right) \\ &= \left(\prod_{p|n} p^{\alpha_p(n)}\right) \prod_{p|n} \left(1 - \frac{1}{p}\right) = n \prod_{p|n} \left(1 - \frac{1}{p}\right).\end{aligned}$$

□

Wir wenden zum Abschluss dieses Abschnitts die erhaltene Theorie auf die sogenannte RSA-Kryptographie an. Diese beruht auf folgender Beobachtung

Bemerkung 4.11 Es seien $p, q \in \mathbb{P}$ mit $p \neq q$ und

$$m := pq,$$

also $\varphi(m) = (p-1)(q-1)$ nach Satz 4.10. Ist $a \in \mathbb{N}$ teilerfremd zu $\varphi(m)$, so existiert nach Satz 3.6 ein (modulo $\varphi(m)$ eindeutig bestimmtes) $b \in \mathbb{N}$ mit $ab \equiv 1 \mod \varphi(m)$. Mit diesen a, b gilt

$$(x^a)^b \equiv x \mod m \quad \text{für } x \in \mathbb{Z}. \tag{4.4}$$

(*Denn*: Wegen $\varphi(m) = (p-1)(q-1)$ gilt $ab \equiv 1 \mod (p-1)$, also gibt es ein $k \in \mathbb{N}_0$ mit

$$ab = k\,(p-1) + 1$$

und damit erhalten wir für $x \in \mathbb{Z}$, unter Verwendung des Satzes von Fermat 3.24.2 im ersten Fall des dritten Schrittes,

$$(x^a)^b = x^{ab} = \left(x^{p-1}\right)^k x \equiv \left\{ \begin{array}{lll} 1 \cdot x & \mod p & \text{falls } p \nmid x, \\ 0 & \mod p & \text{falls } p \mid x \end{array} \right\} \equiv x \mod p.$$

Analog erhalten wir

$$(x^a)^b \equiv x \mod q \quad \text{für } x \in \mathbb{Z}.$$

Mit Satz 4.3.1 und der Teilerfremdheit von p, q folgt (4.4).)

Bemerkung 4.12 (Prinzip der RSA-Kryptographie)

Das RSA-Verfahren[9], ein sogenanntes asymmetrisches Verschlüsselungsverfahren, beruht auf folgenden Grundgedanken

[9] Benannt nach den Autoren Rivest, Shamir, Adleman der Erstveröffentlichung im Jahre 1977.

- Der Empfänger E wählt p, q, a, b wie im Bemerkung 4.11 und stellt dem Sender S (oder auch mehreren Sendern) den öffentlichen Schlüssel (m, a) zur Verfügung
- S erstellt eine Nachricht x in Form eines Tupels

  $$x = (x_1, \ldots, x_N) \in \{0, \ldots, m-1\}^N$$

  und berechnet und sendet

  $$y := (y_1, \ldots, y_N) \quad \coloneqq \quad (x_1^a, \ldots, x_N^a) \mod m.$$

- E berechnet daraus

  $$(y_1^b, \ldots, y_N^b) \mod m,$$

  also x wegen (4.4)

Wesentlich dabei: Für große p, q ist $\varphi(m)$ und damit auch b aus der Kenntnis von m und a derzeit praktisch nicht berechenbar.

5 Gruppenmorphismen, Normalteiler, Faktorgruppen

Grob gesprochen ist ein Morphismus einer gegebenen Klasse algebraischer Strukturen" eine "strukturerhaltende Abbildung" eines "Objektes" dieser Klasse in ein anderes. Wir beschränken die Präzisierung dieser Idee in diesem Abschnitt im Wesentlichen auf die Klasse aller Gruppen[10].

Definition 5.1 Es seien $(G,\cdot) = (G,\cdot_G)$, $(H,\cdot) = (H,\cdot_H)$ Halbgruppen und $\varphi : G \to H$ eine Funktion.

1. Gilt[11]

$$\varphi(ab) = \varphi(a)\varphi(b) \quad \text{für } a,b \in G, \tag{5.1}$$

so heißt φ **(Halbgruppen-)morphismus**[12] (von G nach H).

2. Sind $(G,\cdot,e_G)$ und $(H,\cdot,e_H)$ Monoide und erfüllt φ neben (5.1) auch

$$\varphi(e_G) = e_H,$$

so heißt φ **(Monoid-)morphismus** (von G nach H).

Sind G und H Gruppen, so spricht man auch von einem **Gruppenmorphismus**. Ist φ zudem injektiv, so heißt φ **(Gruppen-)monomorphismus** und ist φ zudem bijektiv, so heißt φ **(Gruppen-)isomorphismus**.

3. Um deulich zu machen, dass φ ein Morphismus ist, schreiben wir manchmal auch $\varphi : (G,\cdot) \to (H,\cdot)$ bezehungsweise $\varphi : (G,\cdot,e_G) \to (H,\cdot,e_H)$.

Bemerkung 5.2 1. Ist G eine Gruppe, so ist offenbar $\mathrm{id}_G : G \to G$ ein Isomorphismus.

2. Sind F,G,H Gruppen und $\varphi : F \to G$, $\psi : G \to H$ Morphismen, so ist auch $\psi \circ \varphi : F \to H$ ein Morphismus.

Satz 5.3 *Es seien $(G,\cdot,e)$ eine Gruppe, $(H,\cdot)$ eine Halbgruppe und $\varphi : G \to H$ ein Halbgruppenmorphismus. Dann ist $(\varphi(G),\cdot,\varphi(e))$ eine Gruppe und es gilt*

$$\varphi(a^{-1}) = \varphi(a)^{-1} \quad \textit{für } a \in G. \tag{5.2}$$

Ist $(H,\cdot,e_H)$ eine Gruppe, so ist φ auch ein Gruppenmorphismus.

[10] Später betrachten wir analog zum Beispiel Ringmorphismen. Eine allgemeine Präzisierung und Untersuchung "strukturerhaltender Abbildungen algebraischer Strukturen" ist Gegenstand der **Universellen Algebra**. Eine noch allgemeinere Sichtweise liefert die **Kategorientheorie**, in der dann die Gemeinsamkeiten von z.B. einerseits Gruppenmorphismen und andererseits stetigen Abbildungen zwischen metrischen Räumen studiert werden.

[11] Die präzisere Notation wäre $\varphi(a \cdot_G b) = \varphi(a) \cdot_H \varphi(b)$.

[12] Oder **Morphismus (von Halbgruppen)**. Analog für später zu definierende andere Sorten von Morphismen.

Beweis. Nach (5.1) ist $\cdot_H$ eine Verknüpfung auf $\varphi(G)$ (und damit $\varphi(G)$ eine Unterhalbgruppe von H). Ist $u \in \varphi(G)$, so gilt für $a \in G$ mit $u = \varphi(a)$

$$u = \varphi(a) = \varphi(ae) = \varphi(a)\varphi(e) = u\varphi(e)$$

und entsprechend $u = \varphi(e)u$. Also ist $\varphi(e)$ neutrales Element in $\varphi(G)$. Schließlich ergibt sich für $a \in G$

$$\varphi(e) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1})$$

und entsprechend $\varphi(e) = \varphi(a^{-1})\varphi(a)$. Folglich ist $\varphi(a^{-1})$ invers zu $\varphi(a)$ in $\varphi(G)$.

Ist $(H, \cdot_H, e_H)$ eine Gruppe, so erhalten wir zudem $\varphi(e) = \varphi(ee) = \varphi(e)\varphi(e)$, also

$$e_H = \varphi(e)(\varphi(e))^{-1} = \varphi(e)\varphi(e)(\varphi(e))^{-1} = \varphi(e).$$

□

Beispiele 5.4 1. Es sei $m \in \mathbb{N}$ und es sei $\varphi : \mathbb{Z} \to \mathbb{Z}_m$, definiert durch

$$\varphi(a) \;:=\; [a]_m \quad \text{für } a \in \mathbb{Z},$$

ist φ ein Gruppenmorphismus von $(\mathbb{Z}, +, 0)$ nach $(\mathbb{Z}_m, +, [0])$, denn für $a, b \in \mathbb{Z}$ gilt

$$\varphi(a+b) \;=\; [a+b] \;=\; [a] + [b] \;=\; \varphi(a) + \varphi(b).$$

φ ist surjektiv, aber nicht injektiv, da etwa $\varphi(0) = [0] = \varphi(m)$.

2. Die Abbildung $\varphi : \mathbb{R} \to \mathbb{C}$ definiert durch

$$\varphi(a) \;:=\; (a, 0) = \; a + \mathrm{i}0 \quad \text{für } a \in \mathbb{R}$$

ist ein Gruppenmonomorphismus von $(\mathbb{R}, +, 0)$ nach $(\mathbb{C}, +, 0)$.

3. Es sei K ein Körper und es sei $n \in \mathbb{N}$. Dann ist die Menge $K^{n\times n}$ der $(n \times n)$-Matrizen mit Einträgen in K mit der Matrixmultiplikation und der Einheitsmatrix $E = E_n$ ein Monoid. Die Determinante $\det : K^{n\times n} \to K$ ist nach dem Determinantenmultiplikationssatz ein Monoidmorphismus nach $(K, \cdot, 1)$. Die Menge der invertierbaren Elemente

$$\mathrm{GL}_n(K) := (K^{n\times n})^* = \{A \in K^{n\times n} : A \text{ invertierbar}\}$$

heißt hier **allgemeine lineare Gruppe**. Die Restriktion $\det = \det|_{\mathrm{GL}_n(K)}$ ein Gruppenmorphismus nach $(K \setminus \{0\}, \cdot, 1)$.

Definition 5.5 Es sei $\varphi : G \to H$ ein Gruppenmorphismus, und sei e_H das neutrale Element von H. Dann heißt

$$\operatorname{Kern}\varphi \;:=\; \varphi^{-1}(\{e_H\})$$

der **Kern** von φ.

Beispiel 5.6 In Beispiel 5.4.1 ist $\operatorname{Kern}\varphi = \{x \in \mathbb{Z} : [x] = [0]\} = m\mathbb{Z}$, in 2. ist $\operatorname{Kern}\varphi = \{0\}$ und in 3. gilt $\operatorname{Kern}(\det) = \{A : \det(A) = 1\}$.

Satz 5.7 *Es seien G, H Gruppen und und $\varphi : G \to H$ ein Morphismus.*

1. *Ist $U \subset G$ eine Untergruppe, so ist das Bild $\varphi(U) \subset H$ eine Untergruppe.*
2. *Ist $V \subset H$ eine Untergruppe, so ist das Urbild $\varphi^{-1}(V) \subset G$ eine Untergruppe.*
3. *$\operatorname{Kern}\varphi$ ist eine Untergruppe von G.*
4. *φ ist genau dann ein Monomorphismus, wenn $\operatorname{Kern}\varphi = \{e_G\}$ gilt.*
5. *Ist φ ein Isomorphismus, so ist auch φ^{-1} ein Isomorphismus.*

Beweis. 1. ergibt sich unmittelbar aus Satz 5.3.

2. und 3. als [Ü].

4. "⇒": Ist φ injektiv, so ist $\operatorname{Kern}\varphi = \{e_G\}$ mit 3.

"⇐": Es gelte $\operatorname{Kern}\varphi = \{e_G\}$. Für $a, b \in G$ mit $\varphi(a) = \varphi(b)$ folgt dann

$$e_H \;=\; \varphi(a)\Big(\varphi(b)\Big)^{-1} \;=\; \varphi(a)\varphi(b^{-1}) \;=\; \varphi(ab^{-1}),$$

also $ab^{-1} = e_G$ und damit $a = b$.

5. Es seien $u, v \in H$. Da φ surjektiv ist, existieren $a, b \in G$ mit $u = h(a), v = h(b)$, und es folgt

$$\varphi^{-1}(uv) \;=\; \varphi^{-1}\Big(\varphi(a)\varphi(b)\Big) \;=\; \varphi^{-1}\Big(\varphi(ab)\Big) \;=\; ab \;=\; \varphi^{-1}(u)\varphi^{-1}(v).$$

Also ist φ^{-1} ein Morphismus von H nach G. □

Zwei Gruppen G und H heißen **isomorph**, falls ein Isomorphismus $\varphi : G \to H$ existiert. Wir schreiben dann auch kurz $G \simeq H$. Ein typisches Anliegen der Algebra liegt darin, möglichst viele Gruppen mittels Isomorphismen auf "bekannte" Gruppen zurückzuführen. Speziell für zyklische Gruppen leistet dies der folgende Satz.

Satz 5.8 *Es seien G, H Gruppen.*

1. *Ist G isomorph zu H und ist G zyklisch, so ist auch H zyklisch.*
2. *G ist genau dann zyklisch, wenn G isomorph zu $(\mathbb{Z}, +, 0)$ oder isomorph zu $(\mathbb{Z}_m, +, [0])$ für ein $m \in \mathbb{N}$ ist.*

Beweis. 1. Ist $x \in G$ mit

$$G \;=\; \langle x\rangle \;=\; \{x^k : k \in \mathbb{Z}\}$$

und ist $\varphi : G \to H$ ein Isomorphismus, so gilt

$$H \;=\; \varphi(G) \;=\; \{\varphi(x^k) : k \in \mathbb{Z}\} \;=\; \{\Big(\varphi(x)\Big)^k : k \in \mathbb{Z}\} \;=\; \langle\varphi(x)\rangle.$$

2. "$\Leftarrow$": Die Gruppen $\mathbb{Z}$ und $\mathbb{Z}_m$ sind zyklisch nach Beispiel 3.17. Nach 1. ist G zyklisch.

"$\Rightarrow$": Es sei G eine zyklische Gruppe und es sei $x \in G$ mit $G = \langle x \rangle$, also insbesondere

$$\operatorname{ord}(x) \;=\; \operatorname{ord}(G).$$

Dann definiert

$$\varphi(a) \;:=\; x^a \quad \text{für } a \in \mathbb{Z}$$

einen surjektiven Morphismus von $\mathbb{Z}$ auf G, denn für $a, b \in \mathbb{Z}$ gilt

$$\varphi(a+b) \;=\; x^{a+b} \;= x^a x^b \;=\; \varphi(a)\varphi(b)$$

und für $y \in G = \langle x \rangle$ existiert ein $a \in \mathbb{Z}$ mit $y = x^a$, also $y = \varphi(a)$.

1. Fall: $\operatorname{ord}(G) = \infty$. Dann ist φ injektiv und damit Isomorphismus, denn sonst gäbe es $a, b \in \mathbb{Z}$ mit $a < b$ und $x^a = x^b$, also $e = x^{b-a}$ und folglich $\operatorname{ord}(G) = \operatorname{ord}(x) < \infty$ nach Satz 3.18.

2. Fall: $\operatorname{ord}(G) = m \in \mathbb{N}$. Nach Satz 3.18 gilt dann $x^{a+bm} = x^a$ für $a, b \in \mathbb{Z}$. Also wohldefiniert

$$\psi\big([a]_m\big) \;:=\; \varphi(a) = x^a \quad \text{für } [a]_m \in \mathbb{Z}_m$$

eine Abbildung $\psi : \mathbb{Z}_m \to G$, die injektiv ist da wegen $\operatorname{ord}(G) = m$ die $x^0, x^1, \ldots, x^{m-1}$ paarweise verschieden sind, die surjektiv ist wegen der Surjektivität von φ, und die ein Morphismus ist wegen

$$\begin{aligned} \psi([a]+[b]) \;&=\; \psi([a+b]) \;=\; \varphi(a+b) \\ &=\; \varphi(a)\varphi(b) \;=\; \psi([a])\psi([b]) \quad \text{für } [a],[b] \in \mathbb{Z}_m. \end{aligned}$$

□

Beispiel 5.9 Für $m \in \mathbb{N}$ hat die zyklische Untergruppe $\langle \mathrm{e}^{2\pi \mathrm{i}/m} \rangle$ von $(\mathbb{C} \setminus \{0\}, \cdot, 1)$ die Ordnung m, denn es gilt $(\mathrm{e}^{2\pi\mathrm{i}/m})^m = \mathrm{e}^{2\pi\mathrm{i}} = 1$ und $(\mathrm{e}^{2\pi\mathrm{i}/m})^k = \mathrm{e}^{2\pi\mathrm{i}k/m} \neq 1$ für $k \in \{1, \ldots, m-1\}$. Also ist $\langle \mathrm{e}^{2\pi\mathrm{i}/m} \rangle$ isomorph zu $(\mathbb{Z}_m, +, 0)$.

Überraschender ist folgende Anwendung von Satz 5.8:

Satz 5.10 *Es sei $p \in \mathbb{P}$. Dann ist jede Gruppe der Ordnung p isomorph zu $(\mathbb{Z}_p, +, 0)$.*

Beweis. Ist $x \in G \setminus \{e\}$, so ist $\operatorname{ord}(x) > 1$ und nach dem Satz 3.21 von Lagrange $\operatorname{ord}(x) | \operatorname{ord}(G)$, also $\operatorname{ord}(x) = p = \operatorname{ord}(G)$. Damit ist $G = \langle x \rangle$ zyklisch, und folglich nach Satz 5.8 isomorph zu $\mathbb{Z}_p$. □

Für allgemeinere endliche Gruppenordungen gibt es keine derartig präzisen Aussagen. Immerhin gilt:

Satz 5.11 *Es sei $n \in \mathbb{N}$. Dann ist jede Gruppe der Ordnung n isomorph zu einer Untergruppe der symmetrischen Gruppe S_n.*

Beweis. Es sei $(G, \cdot, e)$ eine Gruppe der Ordnung n. Dann können wir eine Bijektion

$$\{1, \dots, n\} \ni j \mapsto x_j \in G$$

wählen. Ist $a \in G$, so existiert zu jedem $j \in \{1, \dots, n\}$ genau ein $\sigma_a(j) \in \{1, \dots, n\}$ mit

$$ax_j \;=\; x_{\sigma_a(j)}.$$

Die dadurch definierte Abbildung $\sigma_a : \{1, \dots, n\} \to \{1, \dots, n\}$ injektiv, denn für $j \neq k$ ist $ax_j \neq ax_k$ und folglich $\sigma_a(j) \neq \sigma_a(k)$, und damit ist σ_a als Abbildung zwischen zwei gleichmächtigen endlichen Mengen schon bijektiv, also $\sigma_a \in S_n$.

Wir definieren $\varphi : G \to S_n$ durch

$$\varphi(a) \;:=\; \sigma_a \quad \text{für } a \in G.$$

Für $a, b \in G$ gilt für $j \in \{1, \dots, n\}$ dann

$$x_{\sigma_{ab}(j)} \;=\; (ab)x_j \;=\; a(bx_j) \;=\; ax_{\sigma_b(j)} \;=\; x_{\sigma_a(\sigma_b(j))}$$

und damit

$$\varphi(ab)(j) \;=\; \sigma_{ab}(j) = \sigma_a\Big(\sigma_b(j)\Big) = \Big(\varphi(a) \circ \varphi(b)\Big)(j),$$

also $\varphi(ab) = \varphi(a) \circ \varphi(b)$; damit ist φ ein Morphismus.

Ist nun $a \in \operatorname{Kern} \varphi$, d.h. ist $\sigma_a = \mathrm{id}_{\{1,\dots,n\}}$, so gilt $ax_j = x_{\sigma_a(j)} = x_j$ für $j \in \{1, \dots, n\}$, und speziell für $x_j = e$ folgt $a = e$. Also ist φ nach Satz 5.7.4 injektiv, und damit ein Isomorphismus von G auf die Untergruppe $\varphi(G) \subset S_n$. □

Der Satz ist eher eine Reichhaltigkeitsaussage über der Menge aller Untergruppen von S_n als eine Strukturaussage über eine beliebige Gruppe der Ordnung n.

Für das vertiefte Studium von Gruppen erweisen sich nun diejenigen Untergruppen als wichtig, bei denen die in Bemerkung und Definition 3.19 eingeführten Links- und Rechtsnebenklassen übereinstimmen:

Definition 5.12 Es seien G eine Gruppe und $U \subset G$ eine Untergruppe mit

$$gU \;=\; Ug \quad \text{für } g \in G.$$

Dann heißt U **Normalteiler**, oder **normale** Untergruppe, von G, in Zeichen

$$U \;\lhd\; G.$$

Beispiele 5.13 1. Ist G abelsch, so ist jede Untergruppe $U \subset G$ Normalteiler.

2. In jeder Gruppe G sind G und $\{e\}$ sind Normalteiler.

3. Es seien $G = (S_3, \circ, \mathrm{id})$ und $U := \{\mathrm{id}, (1;2)\}$[13] Dann ist U eine Untergruppe und hat nach dem Satz 3.21 von Lagrange wegen $\mathrm{ord}(S_3) = 3! = 6$ und $\mathrm{ord}\, U = 2$ drei Linksnebenklassen, nämlich

$$\mathrm{id}U = U, \qquad (1;3)U = \{(1;3), (1;2;3)\}, \qquad (2;3)U = \{(2;3), (1;3;2)\},$$

und drei Rechtsnebenklassen

$$U\mathrm{id} = U, \qquad U(1;3) = \{(1;3), (1;3;2)\}, \qquad U(2;3) = \{(2;3), (1;2;3)\},$$

Hier ist zum Beispiel $(1;3)U \neq U(1;3)$, also U nicht normal.

Bemerkung und Definition 5.14 Es sei U eine Untergruppe von G. Dann ist für $g \in G$

$$U^g \;:=\; gUg^{-1} \;:=\; \{gag^{-1} : a \in U\}$$

eine Untergruppe von G ([Ü]). U^g heißt die zu U durch g **konjugierte** Untergruppe.

Die folgenden drei Aussagen sind äquivalent:

(i) $U \lhd G$.

(ii) $U^g = U$ für $g \in G$.

(iii) $U^g \subset U$ für $g \in G$.

(*Denn*: (i) $\Leftrightarrow$ (ii): Hier gilt sogar für jedes $g \in G$ die Äquivalenz

$$gU = Ug \;\Leftrightarrow\; U^g = U,$$

denn aus $gU = Ug$ folgt $U^g = gUg^{-1} = (gU)g^{-1} = (Ug)g^{-1} = U$, und aus $gUg^{-1} = U$ folgt $gU = gU(g^{-1}g) = (gUg^{-1})g = Ug$.

(ii) $\Rightarrow$ (iii) ist trivial.

(iii) $\Rightarrow$ (ii): Es sei $g \in G$. Dann gilt $U^{g^{-1}} \subset U$, also $U = (U^{g^{-1}})^g \subset U^g$. Nach Vorausssetzung ist damit $U^g = U$.)

[13] Für $\sigma, \tau \in S_n$ schreiben wieder kurz $\tau\sigma$ statt $\tau \circ \sigma$. Weiter verwenden wir folgende Zykelschreibweise: Für $r \in \{2, \ldots, n\}$ heißt ein $\sigma \in S_n$ ein **r-Zyklus** (oder **r-Zykel**) wenn es paarweise verschiedene $j_1, \ldots, j_r \in \{1, \ldots, n\}$ gibt mit

$$\sigma(j_1) = j_2, \ \ldots, \ \sigma(j_{r-1}) = j_r, \ \sigma(j_r) = j_1$$

und $\sigma(k) = k$ für $k \in \{1, \ldots, n\} \setminus \{j_1, \ldots, j_r\}$; und wir schreiben dann

$$(j_1; \ldots; j_r) \;:=\; \sigma.$$

2-Zykel heißen auch **Transpositionen**.

Satz 5.15 *Es sei $\varphi : G \to H$ ein Gruppenmorphismus.*

1. Ist $N \subset H$ ein Normalteiler von H, so ist $\varphi^{-1}(N)$ ein Normalteiler von G.

2. Kern φ *ist ein Normalteiler von G.*

Beweis. 1. Es gelte $N \lhd H$. Für $g \in G$ gilt dann mit (5.1) und (5.2)

$$\varphi\Big(g\varphi^{-1}(N)g^{-1}\Big) \;=\; \varphi(g)\varphi\Big(\varphi^{-1}(N)\Big)(\varphi(g))^{-1} \;\subset\; \varphi(g)N(\varphi(g))^{-1} \;=\; N$$

und damit

$$\Big(\varphi^{-1}(N)\Big)^g \;=\; g\varphi^{-1}(N)g^{-1} \;\subset\; \varphi^{-1}(N).$$

Also gilt $\varphi^{-1}(N) \lhd G$ nach Bemerkung/Definition 5.14.

2. Folgt aus 1. mit $N := \{e_H\}$, wobei e_H das neutrale Element von H sei. □

Beispiel 5.16 Es sei K ein Körper.

1. Es sei $n \in \mathbb{N}$ und $G := \mathrm{GL}_n(K)$ die allgemeine lineare Gruppe wie in Beispiel 5.4.3. Dann ist nach Satz 5.15 die **spezielle lineare Gruppe**

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

ein Normalteiler von $\mathrm{GL}_n(K)$.

2. Es sei nun $G := \mathrm{SL}_2(K)$ und

$$B_t \;:=\; \begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix} \quad \text{für } t \in K.$$

Dann ist $(K, +, 0) \ni t \mapsto B_t \in \mathrm{SL}_2(K)$ ein Gruppenmorphismus, denn für $s, t \in K$ gilt $\det(B_t) = 1$, also $B_t \in \mathrm{SL}_2(K)$, und

$$B_sB_t \;=\; \begin{bmatrix} 1 & s \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix} \;=\; \begin{bmatrix} 1 & s+t \\ 0 & 1 \end{bmatrix} \;=\; B_{s+t}.$$

Damit ist nach Satz 5.7.1

$$U \;:=\; \{B_t : t \in K\}$$

als Bild von K unter einem Gruppenmorphismus eine Untergruppe von $\mathrm{SL}_2(K)$.

Für $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ gilt nun für $t \in K$

$$AB_tA^{-1} \;=\; \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\begin{bmatrix} 1 & t \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix} \;=\; \begin{bmatrix} 1 & 0 \\ -t & 1 \end{bmatrix},$$

also $AB_tA^{-1} \notin U$ zum Beispiel für $t = 1$, also $U^A \not\subset U$. Damit ist U kein Normalteiler von $\mathrm{SL}_2(K)$ nach Bemerkung/Definition 5.14.

Bemerkung 5.17 Ist G eine Halbgruppe, so ist auch $\mathrm{Pot}(G)$ mit dem Mengenprodukt

$$ST := S \cdot T \quad := \quad \{st : s \in S, t \in T\} \qquad \text{für } S, T \subset G$$

eine Halbgruppe. Ist dabei G eine Gruppe mit neutalem Element e und N ein Normalteiler von G, so folgt aus

$$(aN)(bN) = a(Nb)N = a(bN)N = (ab)N \quad \text{für } a, b \in G,$$

dass und die Abbildung $\pi_N : G \to \mathrm{Pot}(G)$, definiert durch

$$\pi_N(g) \quad := \quad gN \qquad \text{für } g \in G,$$

ein Halbgruppenmorphismus mit $\pi_N(e) = eN = N$ ist. Nach Satz 5.3 ist damit $(G/N, \cdot, N) = (\pi_N(G), \cdot, \pi_N(e))$ eine Gruppe und π_N ein surjektiver Gruppenmorphismus nach $(G/N, \cdot, N)$. Dabei ist $\operatorname{Kern} \pi_N = N$ (für $g \in G$ gilt die Äquivalenzkette $g \in \operatorname{Kern} \pi_N \Leftrightarrow gN = N \Leftrightarrow g \in N$.)

Damit ergeben sich zwei wichtige Eigenschaften von Normalteilern:

- Die Nebenklassen eines Normalteilers $N \lhd G$ bilden auf natürliche Weise eine Gruppe.
- Eine Menge $N \subset G$ ist genau dann ein Normalteiler von G, wenn sie Kern eines Gruppenmorphismus $\varphi : G \to H$ für ein geeignetes H ist (also eine Verschärfung von Satz 5.15.2).

Definition 5.18 In der Situation aus Bemerkung 5.17 heißt G/N die **Faktorgruppe**, oder **Quotientengruppe**, von G nach N, und die Abbildung π_N heißt **kanonischer Morphismus** von G auf G/N.

Beispiele 5.19 1. Es seien $G := (\mathbb{Z}, +, 0)$, $m \in \mathbb{N}$, und $N := m\mathbb{Z}$. Dann ist

$$\mathbb{Z}/(m\mathbb{Z}) \quad = \quad \{a + m\mathbb{Z} : a \in \mathbb{Z}\} \quad = \quad \mathbb{Z}_m$$

und $\pi_{m\mathbb{Z}}(a) = a + m\mathbb{Z} = [a]_m$ für $a \in \mathbb{Z}$ sowie $\operatorname{Kern} \pi_{m\mathbb{Z}} = m\mathbb{Z}$; vgl. Beispiel 5.4.1.

2. Es sei $G := S_n$ mit $n \geq 2$ und $H := (\{1, -1\}, \cdot, 1)$. Wir setzen als aus der Linearen Algebra bekannt voraus, dass durch

$$\operatorname{sign}(\sigma) \quad := \quad (-1)^k \qquad \text{falls } \sigma \text{ als Produkt von } k \text{ Transpositionen schreibbar}$$

eine Funktion sign auf S_n wohldefiniert wird. Dann ist offenbar $\operatorname{sign} : S_n \to H$ ein Gruppenmorphismus. Der Normalteiler

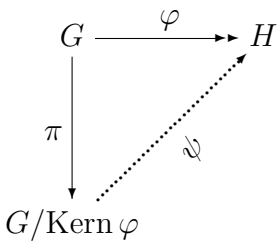
$$A_n \quad := \quad \operatorname{Kern} \operatorname{sign} \quad = \quad \{\sigma \in S_n : \operatorname{sign}(\sigma) = 1\}$$

heißt n-te **alternierende Gruppe**[14]. Hier gilt, wie man sich leicht überlegt,

$$S_n/A_n \;=\; \{A_n, (1;2)A_n\},$$

also $S_n : A_n = 2$. Aus $\operatorname{ord}(S_n) = n!$ ergibt sich $\operatorname{ord}(A_n) = n!/2$ nach dem Satz von Lagrange.

Der folgende Satz ist von zentraler Bedeutung für die Gruppentheorie.



Satz 5.20 *(Isomorphiesatz[15] der Gruppentheorie) Es seien $\varphi : G \to H$ ein surjektiver Gruppenmorphismus und $\pi := \pi_{\operatorname{Kern}\varphi}$. Dann existiert genau eine Funktion $\psi : G/\operatorname{Kern}\varphi \to H$ mit $\psi \circ \pi = \varphi$, und diese ist ein Gruppenisomorphismus; insbesondere sind also $G/\operatorname{Kern}\varphi$ und H isomorph.*

Beweis. Wir setzen $N := \operatorname{Kern}\varphi$. Ist e das neutrale Element in H, so gilt für $a, b \in G$ die Äquivalenzkette

$$\varphi(a) = \varphi(b) \;\Leftrightarrow\; \varphi\big(a^{-1}b\big) = e \;\Leftrightarrow\; a^{-1}b \in N \;\Leftrightarrow\; aN = bN \;\Leftrightarrow\; \pi(a) = \pi(b).$$

Damit, und mit der Surjektivität von π, wohldefiniert

$$\psi(\pi(a)) \;:=\; \varphi(a) \quad \text{für } a \in G$$

eine Funktion $\psi : G/N \to H$ mit $\psi \circ \pi = \varphi$. Die Eindeutigkeit von ψ ist klar wegen der Surjektivität von π. Für $a, b \in G$ gilt nun

$$\psi(\pi(a)\pi(b)) \;=\; \psi(\pi(ab)) \;=\; \varphi(ab) \;=\; \varphi(a)\varphi(b) \;=\; \psi(\pi(a))\psi(\pi(b));$$

also ist ψ ein Gruppenmorphismus. ψ ist surjektiv wegen der Surjektivität von φ. Für $a \in G$ gilt die Äquivalenzkette

$$\psi(\pi(a)) = \varphi(a) = e \;\Leftrightarrow\; a \in N \;\Leftrightarrow\; \pi(a) = N.$$

Also ist $\operatorname{Kern}\psi = \{N\}$ und damit ψ injektiv nach Satz 5.7.4. □

[14] Man kann zeigen: Für $n > 4$ ist A_n der einzige nichttriviale Normalteiler von S_n. Im Falle $n = 4$ ist auch noch die Kleinsche Vierergruppe V_4 (siehe [Ü]) ein Normalteiler in S_4.

[15] Manchmal "erster Isomorphiesatz" genannt.

Bemerkung 5.21 Es sei H eine zyklische Gruppe. Ist x ein erzeugendes Element, so ist $\varphi : \mathbb{Z} \to H$, definiert durch $\varphi(a) := x^a$, ein surjektiver Morphismus. Also ist H isomorph zu $\mathbb{Z}/\operatorname{Kern}\varphi$.

Im Falle $\operatorname{ord}(H) = \infty$ ist $\operatorname{Kern}\varphi = \{0\}$ und im Falle $m := \operatorname{ord}(H) < \infty$ ist $\operatorname{Kern}\varphi = m\mathbb{Z}$ (siehe Satz 3.18). Damit ergibt sich wieder Satz 5.8 (beachte: $\mathbb{Z}_m = \mathbb{Z}/(m\mathbb{Z})$).

Beispiele 5.22

1. Es seien K ein Körper und $G = \mathrm{GL}_n(K)$. Dann ist $\det : G \to (K \setminus \{0\}, \cdot, 1)$ ein surjektiver Morphismus mit Kern $\det = \mathrm{SL}_n(K)$. Also ist $\mathrm{GL}_n(K)/\mathrm{SL}_n(K)$ isomorph zu $K \setminus \{0\}$.

2. Es seien $G := (\mathbb{R}^2, +, 0)$ und $H := (\mathbb{R}, +, 0)$. Dann ist durch

$$\varphi(x, y) \;:=\; x - y \quad \text{für } (x, y) \in \mathbb{R}^2$$

ein surjektiver Morphismus $\varphi : \mathbb{R}^2 \to \mathbb{R}$ definiert. Dabei gilt

$$\operatorname{Kern}\varphi \;=\; \{(x, x) : x \in \mathbb{R}\} \;=:\; N.$$

Nach dem Isomorphiesatz ist $\mathbb{R}^2/N$ isomorph zu $\mathbb{R}$.

3. In der Situation von Beispiel 5.19.2 ist S_n/A_n isomorph zu $(\{1, -1\}, \cdot, 1)$.

6 Diedergruppen und Gruppen kleiner Ordnung

Wir beschäftigen uns kurz mit dem Zusammenspiel von Geometrie und Gruppentheorie.

Definition 6.1 Es sei (X, d) ein metrischer Raum und $f : X \rightarrowtail$ eine Selbstabbildung[16] von X mit

$$d\Big(f(x), f(y)\Big) \;=\; d(x, y) \quad \text{für } x, y \in X.$$

Dann heißt f **Isometrie** von X.

Damit ergibt sich leicht:

Bemerkung 6.2 Es sei (X, d) ein metrischer Raum.

1. Jede Isometrie von X ist injektiv.

2. Die Menge aller surjektiven Isometrien von X ist eine Untergruppe der symmetrischen Gruppe $\Big(S(X), \circ, \mathrm{id}_X\Big)$, genannt **Isometriegruppe** von X.

Beispiel 6.3 Es sei $m \in \mathbb{N}$. Dann ist die Menge aller orthogonalen $m \times m$-Matrizen mit reellen Einträgen

$$\mathrm{O}_m \;:=\; \{A \in \mathrm{GL}_m(\mathbb{R}) : A^{-1} = A^\top\}$$

eine Untergruppe von $\mathrm{GL}_m(\mathbb{R})$, genannt **orthogonale Gruppe** des $\mathbb{R}^m$. Für $A \in \mathrm{O}_m$ und $b \in \mathbb{R}^m$ definiert dann

$$T(x) \;=\; Ax + b \quad \text{für } x \in \mathbb{R}^m \tag{6.1}$$

eine Isometrie des $\mathbb{R}^m$ bezüglich der von der Euklidnorm $|\cdot|$ erzeugten Metrik, denn für $x, y \in \mathbb{R}^m$ gilt

$$\begin{aligned} \Big|T(x) - T(y)\Big|^2 \;&=\; \Big|A(x-y)\Big|^2 \;=\; \Big(A(x-y)\Big)^T A(x-y) \\ &=\; (x-y)^T A^T A(x-y) = |x-y|^2. \end{aligned}$$

Umgekehrt kann man zeigen[17], dass jede euklidsche Isometrie des $\mathbb{R}^m$ von der Form (6.1) ist; wir behandeln unten in Satz 6.4 den Spezialfall $m = 2$. Eine euklidsche Isometrie des $\mathbb{R}^m$ nennt man auch eine **Bewegung** des $\mathbb{R}^m$.

Bewegungen des $\mathbb{R}^m$ sind surjektiv, was sich aus der Invertierbarkeit von A in der Darstellung (6.1) ergibt.

[16] Die Schreibweise $f : X \rightarrowtail$ soll also für $f : X \to X$ stehen.

[17] Siehe etwa Gawronski (1996), *Grundlagen der Linearen Algebra*, Satz 6.3.13.

Satz 6.4 *Eine Selbstabbildung $T : \mathbb{C} \to \mathbb{C}$ ist genau dann isometrisch bezüglich der vom Betragsmetrik auf $\mathbb{C}$, wenn $a, b \in \mathbb{C}$ existieren mit $|a| = 1$ und*

$$T(z) \;=\; az + b \quad \textit{für } z \in \mathbb{C}$$

oder

$$T(z) \;=\; a\overline{z} + b \quad \textit{für } z \in \mathbb{C}.$$

Beweis. Ist T von obiger Form, so ist T eine Isometrie (da $|T(z)-T(w)| = |a|\cdot|z-w| = |z-w|$ für alle $z, w \in \mathbb{C}$).

Es sei umgekehrt $T : \mathbb{C} \to \mathbb{C}$ eine Isometrie. Dann definiert auch

$$S(z) \;:=\; \frac{T(z) - T(0)}{T(1) - T(0)} \quad \text{für } z \in \mathbb{C}$$

eine Isometrie von $\mathbb{C}$, wegen $\Big|T(1) - T(0)\Big| = |1 - 0| = 1$.

Für $z = x + \mathrm{i}y$ und $S(z) = u + \mathrm{i}v$ mit $x, y, u, v \in \mathbb{R}$ gilt

$$x^2 + y^2 \;=\; |z - 0|^2 \;=\; \Big|S(z) - S(0)\Big|^2 \;=\; u^2 + v^2 \tag{6.2}$$

und damit

$$\begin{aligned} x^2 - 2x + 1 + y^2 \;&=\; |z - 1|^2 \;=\; |S(z) - S(1)|^2 \\ &=\; u^2 - 2u + 1 + v^2 \;=\; x^2 - 2u + 1 + y^2, \end{aligned}$$

also $u = x$, und wiederum mit (6.2) dann $|y| = |v|$, also $S(z) = z$ oder $S(z) = \overline{z}$.

Damit folgt

$$S(z) = z \quad \text{für } z \in \mathbb{C} \quad \text{oder} \quad S(z) = \overline{z} \quad \text{für } z \in \mathbb{C},$$

denn sonst gäbe es $z_1 = x_1 + \mathrm{i}y_1, z_2 = x_2 + \mathrm{i}y_2 \in \mathbb{C} \setminus \mathbb{R}$ mit $x_1, y_1, x_2, y_2 \in \mathbb{R}$ und $S(z_1) = z_1$ und $S(z_2) = \overline{z_2}$, was aber wegen

$$|z_1 - z_2|^2 \;=\; |S(z_1) - S(z_2)|^2 \;=\; |z_1 - \overline{z_2}|^2$$

auf den Widerspruch $y_1 y_2 = 0$ führen würde.

Mit $a := T(1) - T(0)$ und $b := T(0)$ ergibt sich die Behauptung. □

Bemerkung und Definition 6.5 Es seien $m \in \mathbb{N}$ und $F \subset \mathbb{R}^m$. Eine Bewegung $T : \mathbb{R}^m \to$ heißt **Symmetrie** von F falls $T(F) = F$ gilt. Wir setzen

$$\mathrm{Sym}(F) \;:=\; \{T : T \text{ Symmetrie von } F\}.$$

Wie man leicht sieht ist $\mathrm{Sym}(F)$ ist eine Untergruppe der Isometriegruppe des $\mathbb{R}^m$, die sogenannte **Symmetriegruppe** von F.

Beispiel 6.6 Es seien $n \in \mathbb{N}$ mit $n \geq 2$ und $\zeta := \zeta_n := \mathrm{e}^{2\pi \mathrm{i}/n}$. Dann ist mit $V_n := \{\zeta^0, \zeta, \ldots, \zeta^{n-1}\} = \langle\zeta\rangle$

$$R_n \;:=\; \mathrm{conv}(V_n) \;=\; \left\{ \sum_{k=0}^{n-1} \lambda_k \zeta^k : \lambda_0, \ldots, \lambda_{n-1} \in [0,1], \sum_{k=0}^{n-1} \lambda_k = 1 \right\} \;\subset\; \mathbb{C}$$

das reguläre n-Eck mit der Eckenmenge V_n. Die Gruppe

$$\mathrm{D}_n \;:=\; \mathrm{Sym}(R_n)$$

heißt n-te **Diedergruppe**. Wir untersuchen nun ihre Struktur:

Sind $\tau(z) := \tau_n(z) := \zeta z$ (Drehung um 0 mit Drehwinkel $2\pi/n$) und $\sigma(z) := \overline{z}$ (Spiegelung an $\mathbb{R}$), so sind $\sigma, \tau \in D_n$ nach Definition von R_n. Dabei gilt

$$\mathrm{ord}(\sigma) = 2, \quad \mathrm{ord}(\tau) = n, \quad \sigma \circ \tau \;=\; \tau^{-1} \circ \sigma.$$

Wir zeigen:

1. $\mathrm{D}_n = \langle\{\tau, \sigma\}\rangle = \langle\tau\rangle \cup \langle\tau\rangle\,\sigma = \{\tau^k \circ \sigma^j : k = 0, \ldots, n-1,\ j = 0, 1\}$.
2. $\mathrm{ord}(\mathrm{D}_n) = 2n$.
3. D_n ist für $n \geq 3$ nicht abelsch (und damit auch nicht zyklisch).
4. D_2 ist abelsch, aber nicht zyklisch.

(*Denn*:

1. $\supset$ an beiden Stellen ist klar, da $\mathrm{D_n}$ eine Gruppe ist, die σ und τ enthält. Zu zeigen ist also: Für $T \in \mathrm{D}_n$ gilt $T \in \langle\tau\rangle \cup \langle\tau\rangle\,\sigma$.

Zunächst ist $T(0) = 0$.

(Denn: Für $|w| = 1$ und $b \in \mathbb{C}$ gilt

$$|w + b|^2 = 1 + |b|^2 + 2\mathrm{Re}(wb).$$

Also ist $|a + b|^2 \geq 1 + |b|^2$ oder $|-a + b|^2 \geq 1 + |b|^2$ für jedes a mit $|a| = 1$. Ist n gerade und $T(z) = az + b$, so folgt aus $|T(\pm 1)| \leq 1$ damit $b = 0$. Entsprechendes gilt im Falle $T(z) = a\overline{z} + b$. Ist n ungerade, so ergibt sich die Behauptung durch eine kleine Zusatzüberlegung; [Ü])

Also ist nach Satz 6.4 mit $a := T(1)$

$$T(z) \;=\; az \quad \text{für } z \in \mathbb{C} \quad \text{oder} \quad T(z) \;=\; a\overline{z} \quad \text{für } z \in \mathbb{C}.$$

Aus $|T(z)| = |z|$ und der Tatsache, dass $V_n = R_n \cap \{|w| = 1\}$ gilt, folgt

$$T(V_n) \;=\; V_n, \tag{6.3}$$

mit $T(1) = \zeta^k$ für genau ein $k \in \{0, \dots, n-1\}$, also $T = \tau^k$ oder $T = \tau^k \circ \sigma$.

2. Wegen $\sigma \notin \langle \tau \rangle$ folgt 2. aus dem Satz von Lagrange (S. 3.21).

3. Es gilt $\tau^{-1} = \tau$ genau für $n = 2$. Also ist D_n genau dann abelsch, wenn $n = 2$ gilt. Schließlich rechnet man leicht nach, dass D_2 nicht zyklisch ist.)

Satz 6.7 *Es sei $n \in \mathbb{N} \setminus \{1\}$. Dann ist D_n bis auf Isomorphie die einzige Gruppe der Ordnung $2n$, die von zwei Elementen a und b mit*

$$\mathrm{ord}(a) \;=\; 2, \quad \mathrm{ord}(b) \;=\; n, \quad ab = b^{-1}a$$

erzeugt wird.

Beweis. Wie in Beispiel 6.6 gesehen, ist D_n eine solche Gruppe, mit $a = \sigma$ und $b = \tau$.

Es sei nun G eine weitere solche Gruppe. Dann gilt für $j, k, \ell, m \in \mathbb{Z}$

$$b^k a^j b^m a^\ell \;=\; \begin{cases} b^{k+m} a^{j+\ell} & \text{falls } j \text{ gerade,} \\ b^{k-m} a^{j+\ell} & \text{falls } j \text{ ungerade,} \end{cases} \tag{6.4}$$

denn im ersten Fall ist $a^j = e$, und im zweiten Fall ist $a^j = a$ und mit $m = qn + r$ (Division mit Rest) gilt

$$a^j b^m \;=\; ab^r \;=\; b^{-r}a \;=\; b^{-m}a^j$$

mit r-maliger Anwendung von $ab = b^{-1}a$ im zweiten Schritt. Also ist

$$U \;:=\; \left\{ b^k a^j : j, k \in \mathbb{Z} \right\}$$

eine Untergruppe von G, und mit $\{a, b\} \subset U$ folgt $G = \langle \{a, b\} \rangle \subset U$, also $G = U$. Weiter ist

$$U \;=\; \left\{ b^k a^j : k \in \{0, \dots, n-1\},\, j \in \{0, 1\} \right\},$$

und damit definiert

$$\varphi\left(\tau^k \circ \sigma^j\right) \;:=\; b^k a^j \quad \text{für } k \in \{0, \dots, n-1\},\, j \in \{0, 1\}$$

eine Surjektion φ von D_n auf G, die wegen $\#G = 2n = \#\mathrm{D}_n$ eine Bijektion ist. Wegen $\mathrm{ord}(\tau) = n = \mathrm{ord}(b)$ und $\mathrm{ord}(\sigma) = 2 = \mathrm{ord}(a)$ gilt auch

$$\varphi\left(\tau^k \circ \sigma^j\right) \;=\; b^k a^j \quad \text{für } k, j \in \mathbb{Z},$$

und mit (6.4) für D_n und für G folgt für $j,k,\ell,m \in \mathbb{Z}$ mit j gerade beziehungsweise ungerade

$$\varphi\Big(\tau^k \circ \sigma^j \circ \tau^m \circ \sigma^\ell\Big) \;=\; \left\{ \begin{array}{rcl} \varphi\Big(\tau^{k+m} \circ \sigma^{j+\ell}\Big) & = & b^{k+m}a^{j+\ell} \\ \varphi\Big(\tau^{k-m} \circ \sigma^{j+\ell}\Big) & = & b^{k-m}a^{j+\ell} \end{array} \right\} \;=\; b^k a^j b^m a^\ell$$
$$= \; \varphi\Big(\tau^k \circ \sigma^j\Big)\varphi\Big(\tau^m \circ \sigma^\ell\Big).$$

Also ist φ auch ein Gruppenmorphismus und damit sind D_n und G isomorph. □

Ein anderer Struktursatz ist:

Satz 6.8 *Es sei G eine Gruppe mit* $\operatorname{ord}(x) = 2$ *für $x \in G \setminus \{e\}$. Dann ist G abelsch und es ist* $\operatorname{ord} G \in \{2^m : m \in \mathbb{N}_0\} \cup \{\infty\}$.

Beweis. Für $a \in G$ gilt $a^2 = e$; also gilt für $x, y \in G$

$$xy \;=\; xey \;=\; x(xy)^2y \;=\; x^2yxy^2 \;=\; yx.$$

Es sei nun $\#G < \infty$. Dann existiert

$$m \;:=\; \min\{n \in \mathbb{N}_0 : \exists\, M \subset G,\, \#M = n,\, \langle M\rangle = G\},$$

und wir wählen $M \subset G$ mit $\#M = m$ und $\langle M\rangle = G$. Dann ist nach Satz 3.15.2

$$G \;=\; \left\{\prod_{a\in M} a^{k_a} : (k_a) \in \mathbb{Z}^M\right\} \;=\; \left\{\prod_{a\in F} a : F \subset M\right\}, \tag{6.5}$$

wobei im zweiten Schritt $a^{k_a} \in \{e, a\}$ benutzt wurde.

Für $F, F' \subset M$ mit $F \neq F'$ ist

$$\prod_{a\in F} a \;\neq\; \prod_{a\in F'} a,$$

denn sonst wäre mit o.E. einem $a_0 \in F \setminus F'$

$$a_0 \;=\; \left(\prod_{a\in F'} a\right)\left(\prod_{a\in F, a\neq a_0} a\right)^{-1} \;\in\; \langle F' \cup F \setminus \{a_0\}\rangle \;\subset\; \langle M \setminus \{a_0\}\rangle,$$

also $G = \langle M\rangle = \langle M \setminus \{a_0\}\rangle$ im Widerspruch zur Minimalität von m.

Mit (6.5) folgt $\#G = \#\{F : F \subset M\} = 2^m$. □

Damit können wir eine vollständige Charakterisierung der Gruppen von doppelter Primzahlordnung geben:

Satz 6.9 [18] *Es sei G eine Gruppe der Ordnung $2p$ mit $p \in \mathbb{P}$. Dann ist entweder G zyklisch, also isomorph zu $(\mathbb{Z}_{2p}, +)$, oder isomorph zu D_p.*

Beweis. Der "entweder"-Teil der Behauptung ergibt sich aus der Azyklizität der Diedergruppen; siehe Beispiel 6.6.

Nach Bemerkung 3.22 gilt $\mathrm{ord}(x) \in \{2, p, 2p\}$ für $x \in G \setminus \{e\}$. Ist ord $x = 2p$ für ein $x \in G$, so ist $G = \langle x \rangle$ und damit G zyklisch, also nach Satz 5.8 isomorph zu $(\mathbb{Z}_{2p}, +)$.

Es gelte nun also $\mathrm{ord}(x) \in \{2, p\}$ für $x \in G \setminus \{e\}$.

Ist $p = 2$, so gilt $\mathrm{ord}(x) = 2$ für $x \in= G \setminus \{e\}$, also ist G abelsch nach Satz 6.8. Für beliebig gewählte $a, b \in G \setminus \{e\}$ mit $a \neq b$ gilt dann

$$\mathrm{ord}(a) \;=\; 2, \quad \mathrm{ord}(b) \;=\; 2, \quad ab \;=\; ba \;=\; b^{-1}a$$

und $ab \neq e$ wegen $b = b^{-1} \neq a^{-1}$, sowie $ab \notin \{a, b\}$, und damit wegen $\mathrm{ord}(G) = 4$ also

$$G \;=\; \{e, a, b, ab\} \;=\; \langle \{a, b\} \rangle,$$

und folglich ist G isomorph zu D_2 nach Satz 6.7.

Es sei also $p \geq 3$. Dann ist $\mathrm{ord}(G) = 2p$ keine Zweierpotenz, also existiert nach Satz 6.8 ein $b \in G$ mit $\mathrm{ord}(b) > 2$, also $\mathrm{ord}(b) = p$. Weiter existiert wegen $\mathrm{ord}(G)$ gerade auch ein $a \in G$ mit $\mathrm{ord}(a) = 2$ ([Ü]). Dabei gilt $a \notin \langle b \rangle$ nach Bemerkung 3.22, da $\mathrm{ord}(a) = 2$ kein Teiler von $p = \#\langle b \rangle$ ist. Mit $H := \langle b \rangle$ folgt $H \cap Ha = \emptyset$ und $H \cap aH = \emptyset$, wegen $\mathrm{ord}(G) = 2p$ und $\mathrm{ord}(H) = p$ also

$$G \;=\; H \cup aH \quad \text{und} \quad G \;=\; H \cup Ha,$$

also insbesondere $G = \langle \{a, b\} \rangle$ und $aH = Ha$, d.h. $H \lhd G$ und folglich, under Verwendung von $a^2 = e$ im ersten Schritt und Bemerkung 5.14 im zweiten

$$aHa \;=\; aHa^{-1} \;=\; H.$$

Also existiert ein $k \in \{0, \ldots, p-1\}$ mit

$$ab^k a \;=\; b,$$

[18] In einer etwas ausführlicheren und systematischeren Darstellung der elementaren Gruppentheorie erhält man Satz 6.9 als eine von mehreren Anwendungen der sogenannten Sylow-Sätze. Siehe dazu etwa Meyberg, K. (1980), *Algebra 1*, 2. Auflage, Hanser. In diesem Buch wird auch gezeigt, dass es (bis auf Isomorphie) zu jeder Primzahl p genau zwei Gruppen der Ordnung p^2 gibt (dort Satz 2.2.12), und für jede Wahl zweier Primzahlen $p < q$ mit $q \notin \{1 + kp : k \in \mathbb{N}_0\}$ genau eine der Ordung pq (Beispiel 2.2.11 d)). Beispielsweise ist, bis auf Isomorphie, $(\mathbb{Z}_{15}, +)$ die einziger Gruppe der Ordnung 15.

Mehr über Symmetriegruppen als hier findet man zum Beispiel im Kapitel 5 von Artin, M. (1998), *Algebra*, Birkhäuser.

und damit wegen $a^2 = e$ auch

$$aba \;=\; a(ab^k a)a \;=\; b^k$$

und folglich mit $a^2 = e$

$$b^{k^2} = (b^k)^k = (aba)^k = ab^k a = b.$$

Also ist

$$b^{k^2-1} \;=\; e$$

und damit $p|(k^2-1)$ nach Satz 3.18. Wegen p prim und $k^2 - 1 = (k+1)(k-1)$ folgt $p|(k+1)$ oder $p|(k-1)$, wegen $k \in \{0, \ldots, p-1\}$ also $k = p-1$ oder $k = 1$.

Im Fall $k = 1$ wäre $aba = b$, also

$$ab \;=\; ba^{-1} \;=\; ba$$

und damit auch (wieder mit $a^2 = e$)

$$\begin{aligned}(ab)^2 &= b^2 \neq e,\\ (ab)^p &= ab^p = a \neq e,\end{aligned}$$

und wir erhielten den Widerspruch $\mathrm{ord}(ab) \notin \{1, 2, p\}$.

Also ist $k = p-1$, d. h. $aba = b^{p-1} = b^{-1}$, und damit

$$ab \;=\; b^{-1}a.$$

Wiederum mit Satz 6.7 folgt nun, dass G isomorph ist zu D_p. □

Satz 6.10 *Es gibt bis auf Isomorphie jeweils genau*

- *eine Gruppe der Ordnung $n \in \{1, 2, 3, 5, 7\}$, nämlich $(\mathbb{Z}_n, +)$,*
- *zwei Gruppen der Ordnung $n \in \{4, 6\}$, nämlich $(\mathbb{Z}_n, +)$ und $\mathrm{D}_{n/2}$.*

Insbesondere sind alle Gruppen der Ordnung ≤ 5 abelsch.

Beweis. Der erste Fall ist klar nach Satz 5.10, der zweite nach Satz 6.9 mit $p \in \{2, 3\}$. Der Zusatz ist klar wegen der Kommutativität von D_2 nach Beispiel 6.6. □

7 Polynome und Körpererweiterungen

Wir betrachten zunächst Ringe und Körper etwas genauer, zum Teil analog zu unseren Untersuchungen von Gruppen in den vorangegangenen Abschnitten.

Definition 7.1 Es sei $R = (R, +, \cdot)$ ein Ring und es sei U eine Untergruppe von $(R, +, 0)$.

1, Ist U ein Untermonoid von $(R, \cdot, 1)$, so heißt U **Unterring** von R.

2. Ist $U \cdot R \subset U$ und $R \cdot U \subset U$, so heißt U **(zweiseitiges) Ideal** in R.

3. Ist R ein Körper und ist $U \setminus \{0\}$ eine Untergruppe von $(R \setminus \{0\}, \cdot, 1)$, so heißt U **Unterkörper** (oder **Teilkörper**) von R.

Bemerkung 7.2 Es sei $R = (R, +, \cdot)$ ein Ring und es sei $U \subset R$.

1. Nach Kriterium 3.12(iii) ist $U \neq \emptyset$ Untergruppe von $(R, +, 0)$ genau dann, wenn $U - U \subset U$. Damit gilt dies in allen Fällen in Definition 7.1.

2. Man sieht leicht, dass U genau dann ein Untermonoid von $(R, \cdot, 1)$ ist, wenn $U \cdot U \subset U$ und $1 \in U$ gilt.

3. Ist U ein Ideal mit $1 \in U$, so ist schon $U = R$. Also ist lediglich R sowohl Unterring von R als auch Ideal in R.

Durch zu Bemerkung 3.14 analoge Argumentation erhält man mit Bemerkung 7.2 leicht: Beliebige Schnitte von Unterringen eines Rings sind Unterringe. Beliebige Schnitte von Idealen eines Rings sind Ideale. Beliebige Schnitte von Unterkörpern eines Körpers sind Unterkörper. Dies rechtfertigt die Namensgebungen in der folgenden

Definition 7.3 Es seien R ein Ring und $M \subset R$. Dann heißen

$$\langle M \rangle \;:=\; \langle M \rangle_{\text{Ring}} \;:=\; \bigcap_{U \supset M,\, U \text{ Unterring}} U$$

von M **erzeugter Unterring** und

$$\langle\langle M \rangle\rangle \;:=\; \bigcap_{I \supset M,\, I \text{ Ideal}} I$$

von M **erzeugtes Ideal**. Weiter heißt im Falle eines Körpers R

$$\langle M \rangle \;:=\; \langle M \rangle_{\text{Körper}} \;:=\; \bigcap_{U \supset M,\, U \text{ Unterkörper}} U$$

von M **erzeugter Unterkörper**.

Definition 7.4 Es seien $R = (R, +, \cdot)$ und $S = (S, +, \cdot)$ Ringe und es sei $\varphi : R \to S$. Ist $\varphi : (R, +, 0_R) \to (S, +, 0_S)$ ein Gruppenmorphismus und $\varphi : (R, \cdot, 1_R) \to (S, \cdot, 1_S)$ ein Monoidmorphismus, so heißt φ **(Ring-)morphismus** von R nach S, mit **Kern** $\mathrm{Kern}(\varphi) \coloneqq \varphi^{-1}(\{0_S\})$.

Dabei heißt wieder φ

$$\textbf{(Ring)-}\left\{\begin{array}{l}\textbf{Monomorphismus} \text{ oder } \textbf{Einbettung}\\ \textbf{Isomorphismus}\end{array}\right\} \text{ falls } \varphi \left\{\begin{array}{l}\text{injektiv}\\ \text{bijektiv}\end{array}\right\} \text{ ist.}$$

Existiert ein Isomorphismus $\varphi : R \to S$, so heißen R und S **isomorph**, in Zeichen $R \simeq S$.

Man sieht leicht: Verkettungen von Morphismen bzw. Monomorphismen bzw. Isomorphismen sind wieder solche. Inverse von Isomorphismen sind Isomorphismen.

Beispiel 7.5 Für $m \in \mathbb{N}_0$ ist die Funktion

$$\mathbb{Z} \ni x \;\mapsto\; [x]_m \in \mathbb{Z}_m$$

ist ein surjektiver Ringmorphismus, der nur im Trivialfall $m = 0$ injektiv und damit Isomorphismus ist.

Bemerkung 7.6 Für Ringmorphismen $\varphi : R \to S$ gelten zum Gruppenfall analoge Aussagen :

- Ist $U \subset R$ ein Unterring, so ist $\varphi(U) \subset S$ ein Unterring. Ist U ein Ideal in R, so ist $\varphi(U)$ ein Ideal in $\varphi(R)$.
- Ist $V \subset S$ ein Unterring bzw. Ideal, so ist $\varphi^{-1}(V) \subset R$ ein Unterring bzw. Ideal. Insbesondere ist $\mathrm{Kern}(\varphi)$ stets ein Ideal in R (aber kein Unterring, da $1 \notin \mathrm{Kern}(\varphi)$).
- φ ist genau dann injektiv, wenn $\mathrm{Kern}(\varphi) = \{0\}$ gilt.

Wir konzentrieren uns nun auf Untergruppen und Unterkörper.

Ist R ein kommutativer Ring und ist $\alpha \in \mathbb{N}_0^n$ ein n-dimensionaler **Multiindex**, so setzt man

$$x^\alpha \;\coloneqq\; \prod_{j=1}^{n} x_j^{\alpha_j} \quad \text{für } x = (x_1, \ldots, x_n) \in R^n.$$

Damit können wir nun erzeugte Unterringe beziehungsweise Unterkörper in einem wichtigen Spezialfall bequem hinschreiben:

Satz 7.7 *Es sei $n \in \mathbb{N}$.*

1. Sind R ein kommutativer Ring, $U \subset R$ ein Unterring und $x = (x_1, \ldots, x_n) \in R^n$, so gilt

$$U[x_1, \ldots, x_n] \;:=\; \langle U \cup \{x_1, \ldots, x_n\}\rangle_{\text{Ring}} = \left\{ \sum_{\alpha \in \mathbb{N}_0^n} a_\alpha x^\alpha : (a_\alpha) \in U^{(\mathbb{N}_0^n)} \right\}.$$

2. Sind K ein Körper, $U \subset K$ ein Unterring und $x = (x_1, \ldots, x_n) \in K^n$, so gilt

$$\begin{aligned} U(x_1, \ldots, x_n) \;&:=\; \langle U \cup \{x_1, \ldots, x_n\}\rangle_{\text{Körper}} \\ &=\; \left\{ \frac{\sum\limits_{\alpha \in \mathbb{N}_0^n} a_\alpha x^\alpha}{\sum\limits_{\alpha \in \mathbb{N}_0^n} b_\alpha x^\alpha} : (a_\alpha), (b_\alpha) \in U^{(\mathbb{N}_0^n)}, \sum_{\alpha \in \mathbb{N}_0^n} b_\alpha x^\alpha \neq 0 \right\}. \end{aligned}$$

Beweis. 1. Einerseits rechnet man nach, dass die rechte Seite ein Unterring ist, der U und $x_1, \ldots, x_n$ enthält (beachte: $x^0 = 1$ und $x^{\alpha+\beta} = x^\alpha x^\beta$). Andererseits enthält jeder Unterring, der U und $x_1, \ldots, x_n$ enthält, auch notwendigerweise die rechte Seite.

2. Analog. □

Im obigen Satz heißt $U[x_1, \ldots, x_n]$ der durch **adjungieren** von $x_1, \ldots, x_n$ zu U **im Ring-Sinne** entstandene Unterring, kurz gelesen als "U adjungiert x_1 bis x_n". Entsprechend heißt $U(x_1, \ldots, x_n)$ **im Körper-Sinne** entstandener Unterkörper.

Beispiel 7.8 1. Es sei $R := \mathbb{R}$ und $U := \mathbb{Z}$. Dann ist für $x \in \mathbb{R}$

$$\mathbb{Z}[x] \;=\; \Big\{ \sum_{j \in \mathbb{N}_0} a_j x^j : (a_j) \in \mathbb{Z}^{(\mathbb{N}_0)} \Big\} \;=\; \Big\{ \sum_{j=0}^{n} a_j x^j : a_j \in \mathbb{Z}, n \in \mathbb{N}_0 \Big\},$$

also etwa

$$\mathbb{Z}[\sqrt{2}] \;=\; \Big\{ \sum_{j=0}^{n} a_j \sqrt{2}^j : a_j \in \mathbb{Z}, n \in \mathbb{N}_0 \Big\} \;=\; \{a + \sqrt{2}\, b : a, b \in \mathbb{Z}\} \;=\; \mathbb{Z} + \sqrt{2}\,\mathbb{Z},$$

wobei im zweiten Schritt $(\sqrt{2})^j \in \mathbb{Z} \cup \sqrt{2}\,\mathbb{Z}$ für $j \in \mathbb{N}_0$ benutzt wurde.

2. Es sei $R := \mathbb{C}$ und $U := \mathbb{R}$. Dann gilt mit $\mathrm{i}^j \in \{\pm 1, \pm \mathrm{i}\}$ für $j \in \mathbb{Z}$

$$\mathbb{R}[\mathrm{i}] \;=\; \Big\{ \sum_{j=0}^{n} a_j \mathrm{i}^j : a_j \in \mathbb{R},\ n \in \mathbb{N}_0 \Big\} = \{a + \mathrm{i}\, b : a, b \in \mathbb{R}\} \;= \mathbb{R} + \mathrm{i}\mathbb{R} \;=\; \mathbb{C}.$$

Definition 7.9 Es sei R ein kommutativer Ring.

1. Ist $M \neq \emptyset$ eine beliebige Menge, so sind für $f, g \in R^M$ die Funktionen $f + g \in R^M$ und $f \cdot g \in R^M$ (wie üblich) definiert durch $(f + g)(x) := f(x) + g(x)$ und $(f \cdot g)(x) :=$

$f(x) \cdot g(x)$ für $x \in M$. Damit ist $R^M = (R^M, +, \cdot)$ ein kommutativer Ring mit der Nullfunktion als Nullelement und Einselement 1_{R^M}, definiert durch $1_{R^M}(x) := 1_R$ für $x \in M$. Weiter setzen wir noch $(\lambda f)(x) := \lambda f(x)$ für $\lambda \in R$ und $f \in R^M$.

2. Wir betrachten nun den Fall $M = \mathbb{N}_0$ und definieren für $(a_j), (b_j) \in R^{\mathbb{N}_0}$ (anders als im ersten Teil)

$$(a_j) \cdot (b_j) \quad := \quad (c_j) \text{ mit } c_j := \sum_{k=0}^{j} a_k b_{j-k}.$$

Dabei heißt (c_j) **Cauchy-Produkt** oder auch **Faltung**[19] von (a_j) und (b_j).

Bemerkung 7.10 Mit der Addition aus Definition 7.9.1 und der Multiplikation aus Definition 7.9.2 ist $(R^{\mathbb{N}_0}, +, \cdot)$ ein kommutativer Ring, mit dem Einselement $(1_R, 0, \ldots) = \left(\delta_{j0}\right)_{j=0}^{\infty}$ ([Ü]). Setzt man

$$X \quad := \quad (0, 1_R, 0, 0, \ldots) \quad = \quad \left(\delta_{j1}\right)_{j=0}^{\infty} \quad \in \quad R^{\mathbb{N}_0},$$

so gilt

$$X^k \quad = \quad \left(\delta_{jk}\right)_{j=0}^{\infty} \qquad \text{für } k \in \mathbb{N}_0.$$

Weiter ist

$$\tilde{R} \quad := \quad \{aX^0 : a \in R\} \quad = \quad \{(a, 0, \ldots) : a \in R\}$$

ein vermittels $R \ni a \mapsto aX^0 \in \tilde{R}$ zu R isomorpher Unterring von $R^{\mathbb{N}_0}$. Wir identifizieren im Weiteren $\tilde{R}$ und R und damit a mit aX^0 für $a \in R$.

Definition 7.11 In der Situation aus Bemerkung 7.10 heißt

$$R[X] := \tilde{R}[X] = \left\{ \sum_{j \in \mathbb{N}_0} a_j X^j : (a_j) \in R^{(\mathbb{N}_0)} \right\} \quad = \quad \left\{ \sum_{j=0}^{n} a_j X^j : a_j \in R, n \in \mathbb{N}_0 \right\}$$

Polynomring über R in der (einen) **Unbestimmten** X. Die Elemente von $R[X]$ heißen **Polynome** über R. Ist

$$P \quad = \quad \sum_{j=0}^{n} a_j X^j \quad \in \quad R[X]$$

ein Polynom, so heißt die Funktion $P(\cdot) : R \to R$, definiert durch

$$P(x) \quad := \quad \sum_{j=0}^{n} a_j x^j \qquad \text{für } x \in R$$

die **zugehörige Polynomfunktion**, und ein $x \in R$ mit $P(x) = 0$ heißt **Nullstelle** oder **Wurzel** des Polynoms P.

[19] In anderem Kontext oft mit $(a_j) * (b_j)$ bezeichnet.

Bemerkung 7.12 Für $(a_j) \in R^{(\mathbb{N}_0)}$ und jedes $n \in \mathbb{N}_0$ mit $a_j = 0$ für $j > n$ gilt

$$(a_j) \;=\; (a_0, \ldots, a_n, 0, \ldots) \;=\; \sum_{j=0}^{n} a_j X^j,$$

also $R[X] = R^{(\mathbb{N}_0)}$, und für $(b_j) \in R^{(\mathbb{N}_0)}$ und $m \in \mathbb{N}_0$ mit $b_j = 0$ für $j > m$ gilt dann

$$\begin{aligned} \sum_{j=0}^{n} a_j X^j + \sum_{j=0}^{m} b_j X^j &= \sum_{j=0}^{n \vee m} (a_j + b_j) X^j, \\ \left(\sum_{j=0}^{n} a_j X^j\right)\left(\sum_{j=0}^{m} b_j X^j\right) &= \sum_{j=0}^{n+m} \left(\sum_{k=0}^{j} a_k b_{j-k}\right) X^j. \end{aligned}$$

Beispiel 7.13 Es sei $R := (\mathbb{Z}_2, +, \cdot)$. Dann sind

$$P_1 := X^2 + X, \quad P_2 := X^7 + X^4 + X^3 + X, \quad P_3 := 0$$

drei paarweise verschiedene Polynome über R, mit identischen Polynomfunktionen $P_1(\cdot) = P_2(\cdot) = P_3(\cdot) =$ Nullfunktion.

Bemerkung 7.14 Es seien R ein kommutativer Ring, $x \in R$ und $U \subset R$ ein Unterring. Dann gilt $U[X] \subset R[X]$. Damit ist $P(x)$ auch für $P \in U[X]$ definiert.

1. Nach Satz 7.7 gilt

$$U[x] \;=\; \Big\{P(x) : P \in U[X]\Big\}$$

und, falls R ein Körper ist, auch

$$U(x) \;=\; \Big\{P(x)/Q(x) : P, Q \in U[X], Q(x) \neq 0\Big\}.$$

2. Die Funktion

$$U[X] \ni P \;\mapsto\; P(x) \in R$$

ist ein Ringmorphismus, genannt **Auswertungsmorphismus** auf $U[X]$ bezüglich x.

(*Denn*: Es ist $X^0(x) = x^0 = 1_R$ und für $P = \sum_{j=1}^{n} a_j X^j$, $Q = \sum_{j=1}^{m} b_j X^j \in R[X]$ gilt

$$\begin{aligned} \big(P+Q\big)(x) &= \left(\sum_{j=0}^{m \vee n} (a_j + b_j) X^j\right)(x) = \sum_{j=0}^{m \vee n} (a_j + b_j) x^j = \sum_{j=0}^{n} a_j x^j + \sum_{j=0}^{m} b_j x^j \\ &= P(x) + Q(x), \\ \big(PQ\big)(x) &= \left(\sum_{j=0}^{n+m} \left(\sum_{k=0}^{j} a_k b_{j-k}\right) X^j\right)(x) = \sum_{j=0}^{n+m} \left(\sum_{k=0}^{j} a_k b_{j-k}\right) x^j = P(x)Q(x)\ .) \end{aligned}$$

3. Die Funktion

$$R[X] \ni P \;\mapsto\; P(\cdot) \in R^R$$

ist ein Ringmorphismus, der im Allgemeinen nicht injektiv ist (etwa nach Beispiel 7.13).

Definition 7.15 Es seien R ein kommutativer Ring und $P = \sum_{j=0}^{n} a_j X^j \in R[X]$. Dann heißt (mit $\max \emptyset := -\infty$)

$$\deg P := \max\{j \in \mathbb{N}_0 : a_j \neq 0\}$$

der **Grad** von P. Im Fall $\deg P \in \{0, -\infty\}$ heißt P **konstant** und für $P \neq 0$ heißt $a_{\deg P}$ **führender Koeffizient** von P. Ist dabei $a_{\deg P} = 1$, so heißt P **normiert**.

Bemerkung 7.16 Es sei R ein kommutativer Ring. Dann gilt[20] für $P, Q \in R[X]$

$$\begin{aligned} \deg(P+Q) &\leq \max\{\deg P, \deg Q\}, \\ \deg(PQ) &\leq \deg P + \deg Q; \end{aligned}$$

ist R sogar Integritätsring, so gilt genauer

$$\deg(PQ) = \deg P + \deg Q.$$

Satz 7.17 (Division mit Rest) *Es sei K ein Körper und es seien $P, S \in K[X]$ mit $S \neq 0$. Dann existieren $Q, R \in K[X]$ mit* $\deg R < \deg S$ *und*

$$P = Q \cdot S + R.$$

Beweis. Im Trivialfall $\deg P < \deg S$ kann man $Q := 0$ und $R := P$ setzen. Damit reicht es, zu zeigen: Ist $n \in \mathbb{N}_0$ und sind $P, S \in K[X]$ mit $0 \leq \deg S \leq \deg P = n$, so existeren Q, R wie behauptet.

Ist $n = 0$, also $P = a_0$ und $S = b_0$ mit $a_0, b_0 \in R \setminus \{0\}$, so setzen wir $Q := a_0/b_0$ und $R := 0$.

Es sei nun $n \in \mathbb{N}$ und die Behauptung gelte für jedes $k \in \{0, \ldots, n-1\}$. Weiter seien

$$P = \sum_{j=0}^{n} a_j X^j, \quad S = \sum_{j=0}^{m} b_j X^j \in K[X]$$

mit $\deg P = n$ und $\deg S = m \leq n$. Mit

$$C := P - \frac{a_n}{b_m} X^{n-m} S \in K[X]$$

gilt dann $\deg C < n$.

[20] Man setzt natürlich $-\infty \leq a$ und $(-\infty) + a = a + (-\infty) := -\infty$ für $a \in \{-\infty\} \cup \mathbb{N}_0$, oder auch allgemeiner für $a \in [-\infty, \infty[$.

Ist dabei sogar $\deg C < m$, so können wir $Q := \frac{a_n}{b_m} X^{n-m}$ und $R := C$ setzen.

Ist $\deg C \geq m$, so liefert die Induktionsvoraussetzung (mit C statt P) Polynome $\widetilde{Q}, R \in K[X]$ mit $\deg R < \deg S$ und

$$C \;=\; \widetilde{Q}S + R,$$

also

$$P \;=\; C + \frac{a_n}{b_m} X^{n-m} S \;=\; QS + R.$$

mit $Q := \widetilde{Q} + \frac{a_n}{b_m} X^{n-m}$. □

Satz 7.18 *Es seien K ein Körper und $P \in K[X]$.*

1. (Polynomdivision) Ist $a \in K$ eine Wurzel von P, so existiert genau ein Polynom $Q \in K[X]$ mit $P = (X-a)Q$, und es gilt $\deg(Q) + 1 = \deg(P)$.

2. Ist $P \neq 0$, so hat P höchstens $\deg P$ Wurzeln.

Beweis. 1. Existenz: Wegen $\deg(X-a) = 1$ existiert nach Satz 7.17 ein $Q \in K[X]$ mit

$$P \;=\; (X-a)Q + R$$

mit $\deg R < 1$, also $R = r_0$ mit einem $r_0 \in K$. Damit gilt

$$0 \;=\; P(a) \;=\; (a-a)Q(a) + R(a) \;=\; r_0,$$

wobei im (nichttrivialen) zweiten Schritt Bemerkung 7.14.2 benutzt wurde, und folglich ist $R = 0$. Dabei gilt $\deg(P) = \deg((X-a)Q) = \deg(X-a) + \deg(Q) = 1 + \deg(Q)$, unter Verwendung von Bemerkung 7.16 im zweiten Schritt.

Eindeutigkeit: [Ü].

2. Sind $a_1, \ldots, a_m$ paarweise verschiedene Wurzeln von P, so liefert 1. induktiv ein $Q \in K[X]$ mit $P = \left(\prod_{j=1}^{m} (X - a_j)\right) Q$ und $\deg(Q) + m = \deg(P)$, und wegen $P \neq 0$ und damit auch $Q \neq 0$ folgt $m \leq \deg(P)$. □

Definition 7.19 Ist E ein Körper und ist K ein Teilkörper von E, so sagen wir im Weiteren kurz E sei eine **(Körper-)Erweiterung** von K. In diesem Fall ist E auch ein Vektorraum über K (die Abbildung

$$K \times E \ni (\lambda, x) \mapsto \lambda \cdot x \in E$$

ist eine Skalarmultiplikaton). Die Dimension des K-Vektorraums E heißt **Grad** der Erweiterung, in Zeichen

$$[E : K] \;:=\; \dim_K(E),$$

kurz gelesen als "Grad von E über K". Die Erweiterung heißt **endlich** falls $[E : K]$ endlich ist.

Beispiele 7.20

1. $[\mathbb{C} : \mathbb{R}] = 2$, denn $\{1, \mathrm{i}\}$ ist eine zweielementige Basis des $\mathbb{R}$-Vektorraumes $\mathbb{C}$.
2. $[\mathbb{R} : \mathbb{Q}] = \infty$, denn für jede endliche Menge $M \subset \mathbb{R}$ ist[21]

$$\mathrm{span}_{\mathbb{Q}}(M) = \Big\{ \sum_{x\in M} \lambda_x \cdot x : (\lambda_x) \in \mathbb{Q}^M \Big\}$$

abzählbar, also $\neq \mathbb{R}$. .

Satz 7.21 *Es seien E eine endliche Erweiterung von K und F eine endliche Erweiterung von E. Dann ist auch die Erweiterung F von K endlich und es gilt*

$$[F : E][E : K] \;=\; [F : K].$$

Beweis. Es sei B eine Basis von E als K-Vektorraum und C eine Basis von F als E-Vektorraum. Ist $z \in F$, so existieren Skalare $\mu_y \in E$ mit $z = \sum_{y\in C} \mu_y y$. Weiter existieren zu jeden $y \in C$ Skalare $\lambda_{xy} \in K$ mit $\mu_y = \sum_{x\in B} \lambda_{xy} x$. Also ist

$$z \;=\; \sum_{y\in C} \Big(\sum_{x\in B} \lambda_{xy} x \Big) y \;=\; \sum_{y\in C} \sum_{x\in B} \lambda_{xy} xy\,. \tag{7.1}$$

Damit ist $BC = \{xy : x \in B, y \in C\}$ ein Erzeugendensystem von F als K-Vektorraum.

Hat $z = 0$ die Darstellung (7.1), so folgt wegen der E-linearen Unabhängigkeit von $(y)_{y\in C}$ zunächst $\sum_{x\in B} \lambda_{xy} x = 0$ für $y \in C$, und mit der K-linearen Unabhängigkeit von $(x)_{x\in B}$ dann $\lambda_{xy} = 0$ für $x \in B$, $y \in C$. Damit ist BC eine Basis von F als K-Vektorraum. Wegen der linearen Unabhängigkeit von $(x)_{x\in B}$ gilt $b \neq 0$ für $b \in B$, und mit der E-linearen Unabhängigkeit von $(y)_{y\in C}$ folgt die Injektivität der Funktion $B \times C \ni (b, c) \mapsto bc$, also $\#(BC) = \#(B \times C)$, und damit

$$[F : K] \;=\; \#(BC) \;=\; \#(B \times C) \;=\; \#B \cdot \#C \;=\; [E : K][F : E].$$

□

[21] Sind V ein K-Vektorraum und $M \subset V$, so schreiben wir $\mathrm{span}(M)$ oder $\mathrm{span}_K(M)$ für den linearen Spann der Menge M in V, d. h. $\mathrm{span}(M)$ ist der Schnitt über alle linearen Unterräume von V, die M enthalten.

Definition 7.22 Es sei E eine Körpererweiterung von K.

Ist $x \in E$ Wurzel eines vom Nullpolynom verschiedenen $P \in K[X]$, so heißt x **algebraisch** über K. Ist x nicht algebraisch über K, so heißt x **transzendent** über K. Ist jedes $x \in E$ algebraisch über K, so heißt E **algebraisch** über K.

Beispiele 7.23

1. Es sei K ein Körper. Ist $a \in K$, so ist a Wurzel von $X - a \in K[X]$. Also ist K algebraisch über K.
2. $\sqrt{2}$ ist algebraisch über $\mathbb{Q}$, denn $P(\sqrt{2}) = 0$ zum Beipiel für $P := X^2 - 2 \in \mathbb{Q}[X]$.
3. $\mathbb{C}$ ist algebraisch über $\mathbb{R}$, denn für $z = x + \mathrm{i}y \in \mathbb{C}$ mit $x, y \in \mathbb{R}$ und

$$P \;:=\; (X - x)^2 + y^2 \;\in\; \mathbb{R}[X].$$

gilt $P(z) = (z - x)^2 + y^2 = (\mathrm{i}y)^2 + y^2 = 0$ mit Bemerkung 7.14.2.

4. Es sei $\mathbb{A}$ die Menge der reellen und über $\mathbb{Q}$ algebraischen Zahlen. Da $\mathbb{Q}[X]$ abzählbar ist und jedes Polynom $P \in \mathbb{Q}[X]\backslash\{0\}$ nur endlich viele Wurzeln hat, ist $\mathbb{A}$ abzählbar, also $\mathbb{R} \setminus \mathbb{A}$ überabzählbar. Insbesondere ist $\mathbb{R}$ nicht algebraisch über $\mathbb{Q}$.

Bemerkung 7.24 Es sei E eine Körpererweiterung von K.

1. Für $x \in E$ ist

$$K[x] \;=\; \{P(x) : P \in K[X]\} \;=\; \mathrm{span}_K\{x^j : j \in \mathbb{N}_0\},$$

also $K[x]$ insbesondere auch ein Untervektorraum des K-Vektorraumes E.

Bezeichnet $\varphi_x : K[X] \to E$ den Auswertungsmorphismus auf $K[X]$ bezüglich x, so ist φ_x auch eine K-lineare Abbildung (man beachte: $K[X]$ ist auch ein K-Vektorraum). Aus der Definition der Transzendenz ergibt sich unmittelbar, dass folgende Aussagen äquivalent sind:

(i) x ist transzendent über K.
(ii) $(x^j)_{j\in\mathbb{N}_0}$ ist linear unabhängig im K-Vektorraum E.
(iii) $\mathrm{kern}(\varphi_x) = \{0\}$ (also $\varphi_x : K[X] \to E$ injektiv).

2. Ist E eine endliche Erweiterung von K, so ist $(x^j)_{j=0}^{[E:K]}$ für alle $x \in E$ linear abhängig im K-Vektorraum E, also x algebraisch über E nach 1. Damit ist E algebraisch über K.

Satz 7.25 *Es sei E eine Körpererweiterung von K. Dann gilt: $x \in E$ ist genau dann algabraisch über K, wenn $K[x]$ ein Unterkörper von E ist, also $K[x] = K(x)$ gilt.*

Beweis. $\Leftarrow$: Es ist entweder $x = 0$, also x algebraisch, oder $x \neq 0$, also $1/x \in K[x]$. Nach Bemerkung 7.24.1 gibt es ein $P \in K[X]$ mit $1/x = P(x)$. Also ist $\deg P \geq 0$ und x Wurzel von $Q := 1 - X \cdot P \in K[X]$ mit $\deg Q \geq 1$, und damit x algebraisch über K.

$\Rightarrow$: Da $K[x]$ ein Unterring von E ist, ist nur zu zeigen: Für $y \in K[x] \setminus \{0\}$ ist $1/y \in K[x]$. Ist also $y \in K[x]$, so existiert nach Bemerkung 7.24.1 ein $P \in K[X] \setminus \{0\}$ mit $P(y) = 0$, $P = \sum_{j=r}^{d} a_j X^j$ mit $r, d \in \mathbb{N}_0$, $r \le d$, $a_r \neq 0$. Damit folgt

$$0 \;=\; \frac{1}{a_r y^{r+1}} P(y) \;=\; \sum_{j=r}^{d} \frac{a_j}{a_r}\, y^{j-r-1},$$

also

$$\frac{1}{y} \;=\; \sum_{j=r+1}^{d} \left(-\frac{a_j}{a_r}\right) y^{j-r-1} \;\in\; K[x].$$

□

Bemerkung 7.26 Es sei E eine endliche Körpererweiterung von K. Ist $x \in E$ algebraisch über K, so ist E auch eine endliche Körpererweiterung von $K[x]$ mit

$$[E : K] \;=\; \Big[E : K[x]\Big] \cdot \Big[K[x] : K\Big].$$

(*Denn*: Nach Satz 7.25 ist $K[x]$ ein Unterkörper von E. Wegen $[E : K] < \infty$ sind auch $\dim_K K[x] < \infty$ und $\dim_{K[x]} E < \infty$. Die Dimensionsformel folgt aus Satz 7.21.)

Definition 7.27 Es sei R ein kommutativer Ring. Für Polynome $P, S \in R[X]$ heißt P ein **Vielfaches** von S (oder auch S ein **Teiler** von P), falls es ein Polynom $Q \in R[X]$ mit $P = QS$ gibt.

Satz 7.28 *Es seien E eine Körpererweiterung von K und $x \in E$ algebraisch über K. Dann gibt es genau ein normiertes Polynom $P_x \in K[X]$ minimalen Grades mit $P_x(x) = 0$, und für dieses gelten die Aussagen:*

1. *Jedes Polynom $P \in K[X]$ mit $P(x) = 0$ ist Vielfaches von P_x.*
2. *$\{x^j : j = 0, \ldots, \deg(P_x) - 1\}$ ist eine Basis des K-Vektorraumes $K[x]$.*
3. *$K[x]$ ist Körpererweiterung von K vom Grad $[K[x] : K] = \deg P_x$.*
4. *$K[x]$ ist algebraisch über K.*

Beweis. 1. Es ist

$$n \;:=\; \min\{\deg(P) : P \in K[X] \setminus \{0\},\, P(x) = 0\} \;\in\; \mathbb{N},$$

und Wahl eines das Minimum annehmenden Polynoms und Division durch seinen führenden Koeffizienten liefert ein $P_x = \sum_{j=0}^{n} a_j X^j \in K[X]$ mit $\deg P_x = n$, $P_x(x) = 0$, und $a_n = 1$. Wäre $Q \in K[X] \setminus \{P\}$ auch normiert mit $\deg Q = n$ und $Q(x) = 0$, so wäre $P_x - Q \in K[X] \setminus \{0\}$ mit $\deg(P_x - Q) < n$ und $(P_x - Q)(x) = 0$, im Widerspruch zur Minimalität von n. Also existiert P_x eindeutig, wie behauptet.

Es sei $P \in K[X]$ mit $P(x) = 0$. Nach Satz 7.17 existieren $Q, R \in K[X]$ mit $P = QP_x + R$ und $\deg R < \deg P_x$. Aus

$$R(x) \;=\; P(x) - Q(x)P_x(x) \;=\; 0$$

und der Minimalität von n folgt $R = 0$ und damit $P = QP_x$.

2. Es sei $\varphi_x : K[X] \to E$ der Auswertungsmorphismus und es sei

$$K_{<n}[X] \;:=\; \{S \in K[X] : \deg S < n\}.$$

Mit 1. folgt für $S \in K_{<n}[X]$ die Äquivalenz von $\varphi_x(S) = 0$ mit $S = 0$. Also ist $\varphi_x|_{K_{<n}[X]}$ als Ringmorphismus mit trivialem Kern injektiv. Weiter gilt schon

$$\varphi_x(K_{<n}[X]) \;=\; K[x],$$

denn für $y \in K[x]$, also $y = \varphi_x(P)$ für ein $P \in K[X]$, also $P = QP_x + R$ mit Polynomen $Q, R \in K[X]$ mit $\deg R < \deg P_x$, ist $R \in K_{<n}[X]$ und

$$y \;=\; \varphi_x(P) \;=\; P(x) \;=\; Q(x)P_x(x) + R(x) \;=\; R(x) \;=\; \varphi_x(R).$$

Damit ist $\varphi_x : K_{<n}[X] \to K[x]$ ein K-Vektorraumisomorphismus.

Da $B := \{X^0, \ldots, X^{n-1}\}$ eine Basis von $K_{<n}[X]$ ist ([Ü]), ist also

$$\{x^0, \ldots, x^{n-1}\} = \varphi_x(B)$$

eine Basis von $K[x]$.

3. $K[x]$ ist Körper nach Satz 7.25, und es ist $\dim_K K[x] = n$ nach 2.

4. Ergibt sich aus 3. und Bemerkung 7.24.2. □

Satz 7.29 *Es sei E eine Körpererweiterung von K. Dann ist die Menge $A \subset E$ der über K algebraischen Elemente ein Unterkörper von E mit $K \subset A$.*

Beweis. Nach Beispiel 7.23.1 ist $K \subset A$. Daher reicht es, zu zeigen: Sind $x, y \in A$, so gilt $x - y, xy \in A$ und, falls $x \neq 0$, auch $1/x \in A$.

Seien also $x, y \in A$. Ist $x \neq 0$, so gilt, wegen $x \in K[x]$ und da $K[x]$ nach Satz 7.25 ein Körper ist, auch auch $1/x \in K[x]$, also $1/x \in A$ nach Satz 7.28.4.

Es seien weiter $x^0, \ldots, x^m$ und $y^0, \ldots, y^n$ Basen von $K[x]$ beziehungsweise $K[y]$ gemäß Satz 7.28.2. Für $M, N \in \mathbb{N}_0$ existieren dann $a_\mu, b_\nu \in K$ mit

$$x^M = \sum_{\mu=0}^{m} a_\mu x^\mu, \qquad y^N = \sum_{\nu=0}^{n} b_\nu y^\nu$$

und folglich

$$x^M y^N = \sum_{\mu=0}^{m} \sum_{\nu=0}^{n} a_\mu b_\nu x^\mu y^\nu.$$

Also ist $\{x^\mu y^\nu : \mu = 0, \ldots, m;\ \nu = 0, \ldots, n\}$ ein Erzeugendensystem des Untervektorraumes $U := \operatorname{span}\{x^N y^M : M, N \in \mathbb{N}_0\}$ und damit $\dim_K U \leq mn < \infty$. Wegen

$$K[xy] = \operatorname{span}\{(xy)^j : j \in \mathbb{N}_0\} \subset U \quad \text{und} \quad K[x-y] = \operatorname{span}\{(x-y)^j : j \in \mathbb{N}_0\} \subset U$$

(binomische Formel!) sind $((xy)^j)_{j\in\mathbb{N}_0}$ und $((x-y)^j)_{j\in\mathbb{N}_0}$ linear abhängig, und mit Bemerkung 7.24.1 folgt $x - y, xy \in A$. □

Bemerkung und Definition 7.30 Sei E eine Körpererweiterung von K und sei $x \in E$ algebraisch über K. Dann heißt das Polynom P_x aus Satz 7.28 das **Minimalpolynom** von x über K, und x heißt vom **Grad** $\deg P_x$ über K.

Aus der Definition ergibt sich sofort: x ist genau dann vom Grad 1 über K, wenn $x \in K$ gilt, und dann ist $X - a \in K[X]$ das Minimalpolynom.

Beispiel 7.31 1. Das Minimalpolynom von i über $\mathbb{R}$ ist $P_{\mathrm{i}} = X^2 + 1$, denn $P_{\mathrm{i}}(\mathrm{i}) = 0$ und $\mathrm{i} \notin \mathbb{R}$. Also ist i vom Grad 2 über $\mathbb{R}$. Mit Beispiel 7.23.3 folgt analog: Jedes $z \in \mathbb{C}\setminus\mathbb{R}$ ist vom Grad 2 über $\mathbb{R}$.

2. Das Minimalpolynom von $\sqrt{2}$ über $\mathbb{Q}$ ist $P_{\sqrt{2}} = X^2 - 2$, wegen $\sqrt{2} \notin \mathbb{Q}$. Also ist $\sqrt{2}$ vom Grad 2 über $\mathbb{Q}$. Nach Satz 7.28 und Satz 7.25 ist $\{1, \sqrt{2}\}$ eine Basis von $\mathbb{Q}[\sqrt{2}]$ und $\mathbb{Q}[\sqrt{2}] = \mathbb{Q} + \sqrt{2} \cdot \mathbb{Q} = \mathbb{Q}(\sqrt{2})$ ein Unterkörper von $\mathbb{R}$.

Mit dem nächsten Resultat kann man manchmal entscheiden ob ein gegebenes Polynom ein Minimalpolynom ist. Ein Polynom $P \in K[X] \setminus \{0\}$ heißt **irreduzibel** wenn die folgende Implikation gilt

$$P = QS \text{ mit } Q, S \in K[X] \quad \Rightarrow \quad \deg Q = 0 \text{ oder } \deg S = 0.$$

Satz 7.32 *Es seien E eine Körpererweiterung von K, $x \in E$ algebraisch und P_x das zugehörige Minimalpolynom. Für $P \in K[X]$ sind die folgenden Aussagen äquivalent:*

(i) $P = P_x$.

(ii) $P(x) = 0$ *und P ist normiert und irreduzibel.*

Beweis. (i) $\Rightarrow$ (ii): Nach Definition ist $P_x(x) = 0$ und P_x normiert. Ist nun $P_x = QS$ mit $Q, S \in K[X]$, so folgt $0 = P_x(x) = Q(x)S(x)$, also $Q(x) = 0$ oder $S(x) = 0$, also wegen der Minimalität des Grades von P_x dann $\deg Q = \deg P_x$ oder $\deg S = \deg P_x$, und wegen $\deg Q + \deg S = \deg P_x$ dann $\deg S = 0$ oder $\deg Q = 0$.

(ii) $\Rightarrow$ (i): Es gelte (ii). Nach Satz 7.28.1 existiert ein $Q \in K[X]$ mit $P = QP_x$, und mit der Irreduzibilität von P folgt $\deg Q = 0$, also, wegen der Normiertheit von P_x und P, schon $Q = 1$. □

8 Konstruktionen mit Zirkel und Lineal

Ungefähr ab dem Jahre 430 v.d.Z. beschäftigten sich griechische Mathematiker mit dem **Würfelverdopplungsproblem**, auch **Delisches Problem** genannt, bei dem aus einem gegebenen Würfel nur mit Zirkel und Lineal ein Würfel des doppelten Volumens konstruiert werden soll[22]. Erst 1837 publizierte Pierre-Laurent Wantzel den ersten Beweis der Unmöglichkeit einer solchen Konstruktion. Zumindest in der heute üblichen und im Folgenden dargestellten Beweisführung handelt es sich um eine Anwendung der elementaren Körpererweiterungstheorie des vorherigen Abschnitts.

Wir beschränken uns hier auf Konstruktionen in einer Ebene und schreiben wieder $|\cdot|$ für die übliche Euklidnorm auf dem $\mathbb{R}$-Vektorraum $\mathbb{R}^2 = \mathbb{C}$. Weiter sei in diesem Abschnitt für $P, Q \in \mathbb{R}^2$ mit $P \neq Q$ und $0 < r < \infty$

$$\begin{aligned} g_{P,Q} &:= \{tP + (1-t)Q : t \in \mathbb{R}\}, && \textbf{Gerade} \text{ durch } P \text{ und } Q, \\ k_{P,r} &:= \{P + re^{it} : t \in \mathbb{R}\}, && \textbf{Kreis(linie)} \text{ um } P \text{ mit Radius } r. \end{aligned}$$

Definition 8.1 1. Es sei $M \subset \mathbb{R}^2$. Ein Punkt $P \in \mathbb{R}^2$ heißt **direkt konstruierbar** (mit Zirkel und Lineal) aus M falls es Punkte $A, B, C, D, E, F \in M$ mit $A \neq B$ und $D \neq E$ gibt für die eine der folgenden drei Bedingungen erfüllt ist:

(gg) $g_{A,B} \neq g_{D,E}$ und $P \in g_{A,B} \cap g_{D,E}$.

(gk) $P \in g_{A,B} \cap k_{F,|D-E|}$.

(kk) $k_{C,|A-B|} \neq k_{F,|D-E|}$ und $P \in k_{C,|A-B|} \cap k_{F,|D-E|}$.

Es sei $M_0 := M$ und induktiv

$$M_n := \{P \in \mathbb{R}^2 : P \text{ direkt konstruierbar aus } M_{n-1}\} \quad \text{für } n \in \mathbb{N}.$$

Ein Punkt $P \in \mathbb{R}^2$ heißt **konstruierbar** (mit Zirkel und Lineal) aus M falls $P \in \bigcup_{n \in \mathbb{N}_0} M_n$.

2. Es sei $M \subset \mathbb{R}$. Eine Zahl $x \in \mathbb{R}$ heißt **konstruierbar** aus M falls der Punkt $(x, 0) \in \mathbb{R}^2$ aus $M \times \{0\}$ im Sinne von 1. konstruierbar ist, und wir setzen

$$\mathrm{kon}(M) := \{x \in \mathbb{R} : x \text{ konstruierbar aus } M\}.$$

Dabei gilt offenbar $M \subset \mathrm{kon}(M) = \mathrm{kon}(\mathrm{kon}(M))$.

[22] Die zweite Namensgebung erklärt sich aus einer Legende nach der dieses Problem den Bewohnern der Insel Delos vom dortigen Orakel in Form einer Textaufgabe gestellt wurde als sie es angesichts einer Pest um Rat fragten. Zur Historie siehe http://www-history.mcs.st-and.ac.uk/HistTopics/Doubling_the_cube.html

Satz 8.2 *Es sei* $\{0,1\} \subset M \subset \mathbb{R}$.

1. *Für* $(a,b) \in \mathbb{R}^2$ *gilt die Äquivalenz*

$$(a,b) \text{ konstruierbar aus } M \times \{0\} \quad \Leftrightarrow \quad a,b \in \mathrm{kon}(M).$$

2. $\mathrm{con}(M)$ *ist ein Unterkörper von* $\mathbb{R}$ *mit und es gilt die Implikation*

$$a \in \mathrm{kon}(M),\ a \geq 0 \quad \Rightarrow \quad \sqrt{a} \in \mathrm{kon}(M).$$

Beweis. Wir setzen $K := \mathrm{kon}(M)$. Der Beweis ergibt sich aus den folgenden fünf in der Vorlesung näher ausgeführten Schritten:

(α) $a,b \in K \Rightarrow a+b, a-b \in K$.

(β) (a,b) konstruierbar aus $M \times \{0\} \Rightarrow a,b \in K$.

(γ) $a,b \in K \Rightarrow (a,b)$ konstruierbar aus $M \times \{0\}$.

(δ) $a,b \in K,\ b \neq 0 \Rightarrow \frac{a}{b} \in K$.

(ϵ) $0 < a \in K \Rightarrow \sqrt{a} \in K$. □

Bemerkung 8.3 Jeder Unterkörper von $\mathbb{R}$ enthält schon $\mathbb{Q}$. In Satz 8.2 gilt damit $\mathrm{kon}(M) \supset \mathbb{Q}$, also $\mathrm{kon}(M) = \mathrm{kon}(\mathrm{kon}(M)) \supset \mathrm{kon}(\mathbb{Q})$, und im Fall von $M \subset \mathbb{Q}$ folglich $\mathrm{kon}(M) = \mathrm{kon}(\mathbb{Q})$.

Wir wollen Satz 8.2 präzisieren. Dazu benötigen wir:

Satz 8.4 *Es seien* K *ein Körper mit* $2 = 1+1 \neq 0$ *und* E *eine Körpererweiterung von* K *mit* $[E:K] = 2$. *Dann existiert ein* $a \in E \setminus K$ *mit* $a^2 \in K$ *und* $E = K + Ka$.

Beweis. Es sei $x \in E \setminus K$. Dann ist $\{1,x\}$ eine Basis des K-Vektorraumes E, nach Satz 7.28 oder auch einfach wegen der linearen Unabhängigkeit von $(1,x)$ über K. Also existieren $p,q \in K$ mit

$$x^2 + px + q \quad = \quad 0,$$

also, $1+1 \neq 0$ ausnutzend,

$$\left(x + \frac{p}{2}\right)^2 \quad = \quad \frac{p^2}{4} - q \quad \in \quad K.$$

Mit $a := x + \frac{p}{2}$ gilt also $a^2 \in K$ und $a \in E \setminus K$, also ist $(1,a)$ linear unabhängig und damit eine Basis von E. □

Satz 8.5 *Es sei K ein Unterkörper von $\mathbb{R}$ und es sei $x \in \mathbb{R}$. Dann sind folgende zwei Aussagen äquivalent:*

(i) $x \in \mathrm{kon}(K)$.

(ii) *Es existieren ein $n \in \mathbb{N}_0$ und Unterkörper*

$$K = K_0 \subset K_1 \subset \ldots \subset K_n \subset \mathbb{R}$$

mit $x \in K_n$ und $[K_j : K_{j-1}] = 2$ für $j \in \{1, \ldots, n\}$.

Beweis. (i) $\Rightarrow$ (ii):

1. Wir zeigen: Ist U ein Unterkörper von $\mathbb{R}$ und ist ein Punkt $(x, y) \in \mathbb{R}^2$ direkt konstruierbar aus $U \times U$, so gilt $x, y \in U[\sqrt{\delta}]$ für ein $\delta \in U$ mit $\delta \geq 0$.

Wir beweisen die Behauptung durch Fallunterscheidung nach den drei Konstruktionsarten (gg), (gk) und (kk):

(gg): Geraden $g_{A,B}$ mit $A, B \in U^2$ und $A \neq B$ sind auch durch Gleichungen der Form

$$ax + by + c = 0 \tag{8.1}$$

mit $a, b, c \in U$ und $(a, b) \neq (0, 0)$ beschreibbar (Normalenform). Ein Schnittpunkt $(x, y) \in \mathbb{R}^2$ zweier solcher Geraden ist Lösung eines linearen Gleichungssystems über U, liegt also in U^2.

(gk): Kreise $k_{F,|D-E|}$ mit $D, E, F \in U^2$ und $D \neq E$ sind auch durch Gleichungen der Form

$$(x - d)^2 + (y - e)^2 = f \tag{8.2}$$

mit $d, e, f \in U$ und $f \neq 0$ beschreibbar. Auflösen von (8.1), o.E. nach y, und einsetzen in (8.2) liefert eine quadratische Gleichung für x mit Koeffizienten in U. Auflösen dieser über $\mathbb{R}$, falls möglich, liefert $x \in U[\sqrt{\delta}]$ für ein $\delta \in U$ mit $\delta \geq 0$ (genauer ist δ die Diskriminante der quadratischen Gleichung). Mit (8.1) ist dann auch $y \in U[\sqrt{\delta}]$.

(kk): Zwei Kreisgleichungen sind durch Subtraktion auf den Fall (gk) zurückführbar.

2. In Beweisschritt 1. ist entweder $\sqrt{\delta} \in U$, und dann $U = U[\sqrt{\delta}]$, oder $\sqrt{\delta} \notin U$, und dann $\sqrt{\delta}$ als Wurzel von $X^2 - \delta \in U[X]$ algebraisch vom Grad 2 über U. Nach Satz 7.28 ist dann $U[\sqrt{\delta}]$ ein Unterkörper von $\mathbb{R}$ mit $[U[\sqrt{\delta}] : U] = 2$.

3. Ist $x \in \mathrm{kon}(K)$, also $(x, 0)$ in $m \in \mathbb{N}$ Schritten aus $K \times \{0\}$ und damit auch aus $K \times K$ konstruierbar, so liefert die m-fache Anwendung von 1. und 2., startend mit $U := K$, die Behauptung (ii).

(ii) $\Rightarrow$ (i): Es reicht zu zeigen: Für $j \in \{1, \ldots, n\}$ gilt

$$K_j \subset \mathrm{kon}(K_{j-1}).$$

Es sei also $j \in \{1, \ldots, n\}$. Wegen $[K_j : K_{j-1}] = 2$ existiert nach Satz 8.4 ein $a \in K_j \setminus K_{j-1}$ mit $a^2 \in K_{j-1}$ und $K_j = K_{j-1} + K_{j-1}a$. Nach Satz 8.2.2 ist dann

$$K_j \subset K_{j-1} + K_{j-1}\mathrm{kon}(K_{j-1}) \subset \mathrm{kon}(K_{j-1}).$$

□

Satz 8.6 *Es sei K ein Unterkörper von $\mathbb{R}$ und sei $x \in \mathrm{kon}(K)$. Dann ist x algebraisch über K vom Grad 2^m für ein $m \in \mathbb{N}_0$.*

Beweis. Es sei $K = K_0 \subset \ldots \subset K_n$ wie in Satz 8.5 mit $x \in K_n$. Dann liefert Satz 7.21

$$[K_n : K] \;=\; [K_n : K_{n-1}][K_{n-1} : K] \;=\; \ldots \;=\; \prod_{j=1}^{n} [K_j : K_{j-1}] \;=\; 2^n.$$

Nach Bemerkung 7.26, angewandt auf $E := K_n$, ist $[K[x] : K]$ ein Teiler von $[K_n : K]$, also $[K[x] : K] = 2^m$ für ein $m \in \mathbb{N}_0$. Mit Satz 7.28 ergibt sich die Behauptung. □

Bemerkung 8.7 Es seien K ein Körper und $P \in K[X]$. Dann gilt ([Ü])

1. Ist $\deg P \geq 2$ und hat P eine Wurzel $a \in K$, so ist P reduzibel.
2. Ist $\deg P \in \{2, 3\}$ und ist P reduzibel, so hat P eine Wurzel in K.

Bemerkung 8.8

1. Ist $P \in \mathbb{Z}[X]$ normiert und ist $x \in \mathbb{Q}$ eine Wurzel von P, so ist $x \in \mathbb{Z}$ ([Ü]).
2. Es sei $a \in \mathbb{N}$. Dann ist entweder $\sqrt[3]{a} \in \mathbb{N}$ oder $\sqrt[3]{a}$ vom Grad 3 über $\mathbb{Q}$ ([Ü]).

Bemerkung 8.9 (Unlösbarkeit des Delischen Problems)

Es ist $\sqrt[3]{2} \notin \mathrm{kon}(\mathbb{Q})$.

(*Denn*: Nach Bemerkung 8.8 ist $\sqrt[3]{2}$ ($\notin \mathbb{N}$) vom Grad 3 über $\mathbb{Q}$ und damit nicht vom Grad 2^m für ein $m \in \mathbb{N}_0$, also $\notin \mathrm{kon}(\mathbb{Q})$ nach Satz 8.6.)

Wir betrachten das Problem der **Winkeldreiteilung**: Ein "Winkel" $\alpha \in \mathbb{R}$ heißt **dreiteilbar (mit Zirkel und Lineal)** falls $\cos(\alpha/3) \in \mathrm{kon}(\{0, 1, \cos(\alpha)\})$. Wegen Satz 8.2 gilt dabei auch $\sin(\alpha/3) \in \left\{ \pm\sqrt{1 - \cos^2(\alpha/3)} \right\} \subset \mathrm{kon}(\{0, 1, \cos(\alpha)\})$ und außerdem

$$\mathrm{kon}(\{0, 1, \cos(\alpha)\}) \;=\; \mathrm{kon}(\mathbb{Q} \cup \{\cos(\alpha)\}) \;=\; \mathrm{kon}(\mathbb{Q}(\cos\alpha)).$$

Satz 8.10

1. Für $\alpha \in \mathbb{R}$ und $K_\alpha := \mathbb{Q}(\cos\alpha)$ sind äquivalent:

(i) $\cos(\alpha/3) \in \mathrm{kon}(K_\alpha)$.

(ii) $P := X^3 - 3X - 2\cos\alpha \in K_\alpha[X]$ *hat eine Wurzel in* K_α.

2. $\alpha := \pi/3$ ist nicht dreiteilbar.

Beweis. 1. Wir zeigen die Äquivalenz für $x := 2\cos(\alpha/3)$. Wegen

$$\cos(3t) \quad = \quad 4\cos^3 t - 3\cos t \qquad \text{für } t \in \mathbb{R} \tag{8.3}$$

gilt

$$0 \quad = \quad 8\cos^3(\alpha/3) - 6\cos(\alpha/3) - 2\cos(\alpha)$$

und folglich ist x eine Wurzel von $P \in K_\alpha[X]$, also x vom Grad ≤ 3 über K_α. Damit ergibt sich die Äquivalenzkette

$$\begin{aligned} x \in \mathrm{kon}(K_\alpha) \quad &\Leftrightarrow \quad x \text{ vom Grad } < 3 \text{ über } K_\alpha \\ &\Leftrightarrow \quad P \text{ reduzibel in } K_\alpha[X] \\ &\Leftrightarrow \quad P \text{ hat eine Wurzel in } K_\alpha; \end{aligned}$$

dabei wurden im ersten Schritt Bemerkung 8.6 sowie Satz 8.5 (mit $n = 1$ und $K_1 = K_\alpha[x]$), im zweiten Schritt Satz 7.32, und im letzten Bemerkung 8.7 verwendet.

2. Es gilt $\cos(\alpha) = 1/2$ (folgt etwa aus (8.3)), also ist hier $K_\alpha = \mathbb{Q}$ und

$$P = X^3 - 3X - 1 \in \mathbb{Z}[X] \subset \mathbb{R}[X].$$

Ist $f = P(\cdot) : \mathbb{R} \to \mathbb{R}$ die zugehörige Polynomfunktion, so hat f wegen

$$f(-2) = -3,\ f(-1) = 1,\ f(0) = -1,\ f(1) = -3,\ f(2) = 1$$

nach dem Zwischenwertsatz drei Nullstellen in $\mathbb{R} \setminus \mathbb{Z}$. Also hat P keine Wurzel in $\mathbb{Z}$ und folglich nach Bemerkung 8.8.1 keine Wurzel in $\mathbb{Q} = K_\alpha$. Damit folgt die Behauptung aus 1. □

Wir haben im letzten Abschnitt gesehen, dass die Menge der (über $\mathbb{Q}$) transzendenten reellen Zahlen überabzählbar ist. Wir haben allerdings bisher keine „konkrete“ Zahl als transzendent ausmachen können. Wir beweisen nun:

Satz 8.11 e *ist transzendent.*

Beweis. Angenommen, e ist algebraisch (vom Grad m). Dann existiert ein $q \in \mathbb{N}$ mit

$$P := \sum_{j=0}^{m} a_j X^j = qP_{\mathrm{e}} \in \mathbb{Z}[X].$$

Für $p \in \mathbb{P}$ betrachten wir

$$X^{p-1}(X-1)^p \cdots (X-m)^p = \sum_{j=p-1}^{mp+p-1} c_j X^j \in \mathbb{Z}[X] \subset \mathbb{R}[X]$$

und die zugehörige Polynomfunktion $f = f_{m,p} : \mathbb{R} \to \mathbb{R}$. Mit $c_{p-1} = (-1)^p \cdots (-m)^p$ gilt (siehe Analysis, Potenzreihenentwicklung um 0)

$$f^{(k)}(0) = k!c_k = \begin{cases} (p-1)!(-1)^p \cdots (-m)^p, & \text{falls } k = p-1 \\ 0, & \text{falls } k < p-1 \text{ oder } k > np+p-1 \\ \in (p!)\mathbb{Z}, & \text{sonst} \end{cases}.$$

Mit einer entsprechenden Überlegung (Potenzreihenentwicklung um j) ergibt sich

$$f^{(k)}(j) \in (p!)\mathbb{Z} \quad \text{für } k \in \mathbb{N}_0,\ j = 1, \ldots, m.$$

Für

$$F := \sum_{k=0}^{mp+p-1} f^{(k)} : \mathbb{R} \to \mathbb{R}$$

gilt (da $f^{(mp+p)} \equiv 0$)

$$\Big(\mathrm{e}^{-x}F(x)\Big)' = \mathrm{e}^{-x}\Big(F'(x) - F(x)\Big) = -\mathrm{e}^{-x}f(x) \qquad (x \in \mathbb{R}),$$

also für $j = 1, \ldots, m$

$$\int_0^j \mathrm{e}^{-x}f(x)dx = -\mathrm{e}^{-x}F(x)\Big|_0^j = F(0) - \mathrm{e}^{-j}F(j).$$

Mit $a_0, \ldots, a_m \in \mathbb{Z}$ folgt

$$D := \sum_{j=1}^{m}\Big(a_j\mathrm{e}^j \int_0^j \mathrm{e}^{-x}f(x)dx\Big) = F(0)\underbrace{\sum_{j=1}^{m} a_j\mathrm{e}^j}_{=-a_0} - \sum_{j=1}^{m} a_j F(j)$$

$$f^{(p-1)}(0)(-a_0) + \underbrace{(F(0) - f^{(p-1)}(0))}_{\in(p!)\mathbb{Z}}(-a_0) + \sum_{j=1}^{m} a_j \underbrace{F(j)}_{\in(p!)\mathbb{Z}}$$

$$\equiv (p-1)!(-1)^p \cdots (-m)^p(-a_0) =: b \mod p.$$

Da P_e (und damit auch P) irreduzibel über $\mathbb{Q}$ ist, gilt $a_0 = P(0) \neq 0$. Für $p > \max\left(m, |a_0|\right)$ ist p kein Teiler von b ist (sonst müsste p nach Satz 2.6.1 einen der Faktoren teilen, was nicht der Fall ist). Also ist $D \neq 0$. Aus $f^{(p-1)}(0) \in ((p-1)!)\mathbb{Z}$ folgt $D \in ((p-1)!)\mathbb{Z}$ und damit

$$|D| \geq (p-1)! \,.$$

Andererseits gilt (mit $\left|f(x)\right| \leq m^{mp+p-1}$ für $0 \leq x \leq m$)

$$\begin{aligned} |D| &\leq \sum_{j=1}^{m} \left(|a_j| \mathrm{e}^j \int_0^j \mathrm{e}^{-x} \left|f(x)\right| dx \right) \leq m^{mp+p-1} \sum_{j=1}^{m} |a_j| \mathrm{e}^j j \\ &\leq \left(m^{m+1}\right)^p \mathrm{e}^m \sum_{j=1}^{m} |a_j| < (p-1)! \end{aligned}$$

für p genügend groß. Widerspruch! □

Bemerkung 8.12 Mit ähnlichen Methoden wie im vorangegangenen Beweis (aber mit mehr Aufwand[23]) kann man zeigen, dass auch π transzendent ist. Zusammen mit obigen Resultaten ergibt sich daraus die Unmöglichkeit der **Quadratur des Kreises** mit Zirkel und Lineal, d.h. der Konstruktion von $\sqrt{\pi}$ aus $\{0,1\}$ bzw. $\mathbb{Q}$: Wäre nämlich $\sqrt{\pi} \in \mathrm{kon}(\mathbb{Q})$, so wäre nach Satz 8.2.2 auch $\pi = \sqrt{\pi}^2 \in \mathrm{kon}(\mathbb{Q})$, und damit wäre π nach Satz 8.6 algebraisch über $\mathbb{Q}$.

[23] Einen Beweis findet man etwa in Müller, T., *Irrationalitätsbeweise*, Heldermann Verlag (2014)

9 Isomorphiesatz für Ringe und Quotientenkörper

Wir arbeiten zunächst die Rolle der Ideale in der Ringtheorie etwas genauer heraus.

Satz 9.1 *Es seien R ein kommutativer Ring und $M \subset R$ endlich. Dann ist*

$$\langle\langle M\rangle\rangle = \sum_{x\in M} Rx \,(= \sum_{x\in M} xR).$$

Beweis. Es sei U die rechte Seite. Dann gilt $U - U = \sum\limits_{x\in M}(R-R)x \subset U$ und $RU = \sum\limits_{x\in M}(RR)x \subset U$, also ist U ein Ideal. Weiter ist $y = \sum\limits_{x\in M}\delta_{xy}x \in I$ für $y \in M$, also $\langle\langle M\rangle\rangle \subset U$.

Ist umgekehrt $I \supset M$ ein Ideal, so ist schon $I \supset U$, also gilt nach Definition des erzeugten Ideals $\langle\langle M\rangle\rangle \supset U$. □

Bemerkung und Definition 9.2 Ein Ideal $I \subset R$ heißt **Hauptideal** falls es ein $x \in R$ mit $I = \langle\langle x\rangle\rangle$ gibt. Ist R kommutativ, so sind die Hauptideale nach Satz 9.1 genau die Ideale der Form $Rx(= xR)$

Beispiel 9.3 Es sei $R = \mathbb{Z}$. Für $x, y \in \mathbb{Z}$ ist $\langle\langle x\rangle\rangle = x\mathbb{Z}$ und

$$\langle\langle\{x, y\}\rangle\rangle \;=\; x\mathbb{Z} + y\mathbb{Z} = \mathrm{ggT}(x, y)\mathbb{Z}$$

nach Satz 9.1 und Satz 2.4, also auch $\langle\langle\{x, y\}\rangle\rangle$ ein Hauptideal.

Bemerkung 9.4 Es seien R ein Ring und $I \subset R$ ein Ideal. Da I ein Normalteiler in $(R, +, 0)$ ist, definiert $\pi(x) := \pi_I(x) := x + I$ für $x \in R$ nach Bemerkung 5.17 einen surjektiven Gruppenmorphismus $\pi_I : R \to R/I$, wobei $R/I = \{x + I : x \in R\}$, mit $\mathrm{Kern}(\pi_I) = I$. Darüber hinaus wird durch

$$(x + I) \cdot (y + I) \;:=\; (xy) + I \quad \text{für } x, y \in R \tag{9.1}$$

eine Verknüpfung $\cdot$ auf R/I wohldefiniert.

(Für $x, x', y, y' \in R$ mit $x + I = x' + I$ und $y + I = y' + I$, also $x - x' \in I$ und $y - y' \in I$, gilt

$$xy - x'y' \;=\; x(y - y') + (x - x')y' \;\in\; RI + IR \;\subset\; I + I \;=\; I,$$

also $xy + I = x'y' + I$.)

Weiter ist $\cdot$ assoziativ sowie distributiv über $+$, denn für $x, y, z \in R$ gilt

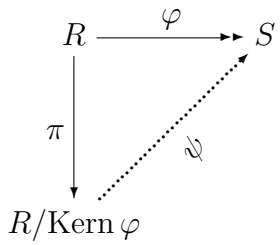
$$\begin{aligned}
\Big((x+I)(y+I)\Big)(z+I) &= (xy+I)(z+I) = \Big((xy)z+I\Big) = \Big(x(yz)+I\Big) \\
&= (x+I)(yz+I) = (x+I)\Big((y+I)(z+I)\Big), \\
\Big((x+I)+(y+I)\Big)(z+I) &= \ldots = (x+I)(z+I)+(y+I)(z+I), \\
(z+I)\Big((x+I)+(y+I)\Big) &= \ldots = (z+I)(x+I)+(z+I)(y+I).
\end{aligned}$$

Also ist $(R/I, +, \cdot)$ ein Ring mit Einselement $1_R + I$. Aus (9.1) ergibt sich zudem, dass π_I ein Ringmorphismus ist.

Analog zum Gruppenfall sind damit und nach Bemerkung 7.6 die Ideale genau die Kerne von Ringmorphismen.

Beispiel 9.5 Als Standardbeispiel dient wieder $R = \mathbb{Z}$, $I = m\mathbb{Z}$. Dann ist $\mathbb{Z}_m = \mathbb{Z}/(m\mathbb{Z})$; vgl. Beispiel 5.19.1.

Bemerkung 9.6 Sind R, S Ringe, so gilt der Isomorphiesatz der Gruppentheorie (Satz 5.20) natürlich für die additiven Gruppen R und S. Da die dort auftretenden Funktionen φ und π auch multiplikativ sind, gilt der Satz auch mit "Ring" statt "Gruppe":



Isomorphiesatz der Ringtheorie *Es seien $\varphi : R \to S$ ein surjektiver Ringmorphismus und $\pi := \pi_{\operatorname{Kern}\varphi}$. Dann existiert genau eine Funktion $\psi : R/\operatorname{Kern}\varphi \to S$ mit $\psi \circ \pi = \varphi$, und diese ist ein Ringisomorphismus; insbesondere sind also $R/\operatorname{Kern}\varphi$ und S isomorph.*

Wir wollen nun zeigen, dass jeder Ring eine ,,Kopie" von $\mathbb{Z}_q$ für ein geeignetes $q \in \mathbb{N}_0$ enthält.

Satz 9.7 *Es seien R ein Ring und $\mathbb{Z}1_R := \{m1_R : m \in \mathbb{Z}\}$. Dann gilt:*

1. $\mathbb{Z}1_R$ ist Unterring von R und isomorph zu $(\mathbb{Z}_q, +, \cdot)$ mit

$$q := \begin{cases} 0 & \text{falls } n1_R \neq 0_R \text{ für } n \in \mathbb{N}, \\ \min\{n \in \mathbb{N} : n1_R = 0_R\} & \text{sonst.} \end{cases}$$

2. $\mathbb{Z}1_R$ ist genau dann nullteilerfrei, wenn $q \in \{0, 1\} \cup \mathbb{P}$.

Beweis. 1. Durch $\varphi(m) := m1_R$ für $m \in \mathbb{Z}$ wird, wie man leicht nachrechnet, ein Ringmorphismus φ von $\mathbb{Z}$ in R definiert, mit $\mathrm{Kern}(\varphi) = q\mathbb{Z}$. Also ist sein Bild $\varphi(R) = \mathbb{Z}1_R$ nach Bemerkung 7.6 ein Unterring von R, und mit dem Isomorphisatz aus Bemerkung 9.6 folgt $\mathbb{Z}1_R \simeq \mathbb{Z}/(q\mathbb{Z}) = \mathbb{Z}_q$.

2. Wegen der Isomorphie aus 1. ist $\mathbb{Z}1_R$ genau dann nullteilerfrei, wenn $\mathbb{Z}_q$ nullteilerfrei ist. Für $q \neq \{0,1\} \cup \mathbb{P}$ ist $\mathbb{Z}_q$ nicht nullteilerfrei ([Ü]) und für $q \in \mathbb{P}$ ist $\mathbb{Z}_q$ sogar ein Körper nach Satz 3.9. Schließlich sind $\mathbb{Z}_0 \simeq \mathbb{Z}$ und $\mathbb{Z}_1 = \{[0]_1\}$ nullteilerfrei. □

Definition 9.8 Die Zahl q aus Satz 9.7 heißt **Charakteristik** von R.

Insbesondere ist die Charakteristik q eines Körpers entweder Null oder eine Primzahl, denn Körper sind nullteilerfrei und mit $0 \neq 1$, also $q \neq 1$.

Jeder Ring mit Primzahlcharakteristik q, also erst recht jeder Körper mit Primzahlcharakteristik q, enthält nach Satz 9.7 eine Kopie des Körpers $\mathbb{Z}_q$. Wir zeigen nun, dass jeder Körper der Charakteristik Null eine Kopie des Körpers $\mathbb{Q}$ enthält. Zur Vorbereitung beweisen wir, dass jeder Integritätsring durch "Quotientenbildung", analog zur Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$, in einen Körper eingebettet werden kann.

Satz 9.9 (Quotientenkörper) *Es sei R ein Integritätsring. Dann wird auf $M := R \times (R \setminus \{0\})$ durch*

$$(a,b) \sim (a',b') \quad :\Leftrightarrow \quad ab' = a'b \qquad \text{für } (a,b),(a',b') \in M$$

eine Äquivalenzrelation $\sim$ definiert, und auf $Q := M/_\sim$ werden mit der Notation

$$\frac{a}{b} \quad := \quad [(a,b)]_\sim \qquad \text{für } (a,b) \in M$$

für die zugehörigen Äquivalenzklassen durch

$$\frac{a}{b} + \frac{c}{d} \quad := \quad \frac{ad+cb}{bd} \qquad \text{und} \qquad \frac{a}{b} \cdot \frac{c}{d} \quad := \quad \frac{ac}{bd} \qquad \text{für} \quad \frac{a}{b}, \frac{c}{d} \in Q$$

zwei Verknüpfungen $+$ und $\cdot$ wohldefiniert, mit denen $(Q,+,\cdot)$ ein Körper ist. Außerdem ist $j : R \to Q$ mit

$$j(a) := \frac{a}{1} \qquad \text{für } a \in R \tag{9.2}$$

eine Ringeinbettung.

Beweis. Die Reflexivität und die Symmetrie von $\sim$ sind offensichtlich. Gilt weiter $(a,b) \sim (a',b')$ und $(a',b') \sim (a'',b'')$, also $ab' = a'b$ und $a'b'' = a''b'$, so folgt

$$b''b'a \;=\; b''a'b \;=\; a''b'b,$$

und daraus mit der Kommutativität sowie der Kürzungsregel aus Bemerkung 3.3.2 schon $ab'' = b''a = a''b$, also $(a,b) \sim (a'',b'')$. Damit ist $\sim$ auch transitiv.

Durch einfaches aber insgesamt nicht ganz kurzes Nachrechnen überzeugt man sich, dass die Verknüpfungen tatsächlich wohldefiniert sind und dass $(Q,+,\cdot)$ ein Körper mit $0_Q = \frac{0}{1}$ und $1_Q = \frac{1}{1}$ ist; zu $\frac{a}{b} \neq 0_Q$ multiplikativ invers ist dabei $\frac{b}{a}$. Die Morphismuseigenschaft von j und die Injektivität sind klar nach Definition von $\sim$. □

Bemerkung 9.10 Es seien K und E Körper. Ist $\varphi : K \to E$ ein Ringmorphismus, so ist φ schon injektiv (also eine Einbettung) und $\varphi(K)$ ein Unterkörper von E. Außerdem gilt dann

$$\varphi\left(\frac{x}{y}\right) \;=\; \frac{\varphi(x)}{\varphi(y)} \quad \text{für } x,y \in K \text{ mit } y \neq 0.$$

(*Denn*: Wäre φ nicht injektiv, so existierte ein $x \in K \setminus \{0\}$ mit $\varphi(x) = 0$, also

$$1_E = \varphi(1_K) \;=\; \varphi(xx^{-1}) \;=\; \varphi(x)\varphi(x^{-1}) \;=\; 0_E,$$

Widerspruch. Damit ist φ injektiv. Für $x,y \in K$ mit $y \neq 0$ gilt also $\varphi(y) \neq 0$ und

$$\varphi(x) \;=\; \varphi\left(\frac{x}{y}y\right) \;=\; \varphi\left(\frac{x}{y}\right)\varphi(y),$$

und folglich $\varphi(x/y) = \varphi(x)/\varphi(y)$. Dies zeigt auch, dass $\varphi(K)$ ein Körper ist.)

Bemerkung und Definition 9.11 Es seien Q und $j : R \to Q$ wie in Satz 9.9. Wir nennen Q den **Quotientenkörper** von R und schreiben $\mathrm{Quot}(R) := Q$.

Ist dann E ein weiterer Körper und $f : R \to E$ eine Ringeinbettung, so gibt es genau einen Ringmorphismus $F : Q \to E$ mit $F \circ j = f$, und dieser erfüllt

$$F\left(\frac{a}{b}\right) \;=\; \frac{f(a)}{f(b)} \quad \text{für } a \in R,\ b \in R \setminus \{0\}.$$

F heißt die **kanonische Fortsetzung** von f. Nach Bemerkung 9.10 ist F eine Einbettung und damit $F(\mathrm{Quot}(R))$ ein zu $\mathrm{Quot}(R)$ isomorpher Unterkörper von E.

(*Denn*: Es seien E und f wie angegeben. Ist $F : Q \to E$ ein Ringmorphismus mit $F \circ j = f$, so gilt für $a, b \in R$, $b \neq 0$, mit Bemerkung 9.10 angewandt auf F im zweiten Schritt,

$$F\left(\widetilde{\frac{a}{b}}\right) \;=\; F\left(\widetilde{\frac{a}{1}} \,/\, \widetilde{\frac{b}{1}}\right) \;=\; \frac{F\left(\widetilde{\frac{a}{1}}\right)}{F\left(\widetilde{\frac{b}{1}}\right)} \;=\; \frac{F(j(a))}{F(j(b))} \;=\; \frac{f(a)}{f(b)}.$$

Umgekehrt rechnet man nach, dass durch $F\left(\widetilde{\frac{a}{b}}\right) := \frac{f(a)}{f(b)}$ für $\widetilde{\frac{a}{b}} \in Q$ ein Ringmorphismus von Q nach E mit $F \circ j = f$ wohldefiniert wird.)

Beispiel 9.12 Ist K ein Körper, so ist $K[X]$ ein Integritätsring. Also ist

$$\mathrm{Quot}(K[X]) = \left\{ \widetilde{\frac{P}{Q}} \;: P, Q \in K[X],\, Q \neq 0 \right\}$$

mit den oben definierten Verknüpfungen ein Körper. Sind E eine Erweiterung von K, x transzendent über K und $f_x : K[X] \to E$ der Auswertungsmorphismus bezüglich x, so ist f_x nach Bemerkung 7.24 eine Einbettung. Ist $F_x : \mathrm{Quot}(K[X]) \to E$ die kanonische Fortsetzung von f_x, so gilt

$$F_x\left(\widetilde{\frac{P}{Q}}\right) = \frac{P(x)}{Q(x)} \quad \text{für } P, Q \in K[X],\, Q \neq 0.$$

Im Falle $K = \mathbb{Q}$, $E = \mathbb{R}$ ist die rechte Seite $P(x)/Q(x)$ für alle $x \in \mathbb{R} \setminus \mathbb{A}$ definiert und $P/Q : \mathbb{R} \setminus \mathbb{A} \to \mathbb{R}$ eine rationale Funktion.

Bemerkung 9.13 Es seien E ein Körper und $R \subset E$ ein Unterring. Dann ist

$$\mathrm{Quot}(R) \;\simeq\; \left\{ \frac{a}{b} : a, b \in R,\; b \neq 0 \right\}.$$

(*Denn*: Ist $f : R \to E$ mit $f(a) := a$ für $a \in R$ und ist F die kanonische Erweiterung von f, so gilt

$$F\left(\widetilde{\frac{a}{b}}\right) = \frac{a}{b} \quad \text{für } a \in R,\, b \in R \setminus \{0\}.$$

und nach Bemerkung/Definition 9.11 ist $\mathrm{Quot}(R)$ isomorph zu $F(\mathrm{Quot}(R))$.)

Definition 9.14 Es sei E ein Körper. Dann heißt, unter Verwendung der Notation aus Definition 7.3,

$$P(E) \;:=\; \bigcap_{U \subset E \text{ Unterkörper}} U \;=\; \langle \{1_E\} \rangle_{\text{Körper}}$$

Primkörper von E. Damit ist $P(E)$ offenbar der kleinste Unterkörper von E.

Bemerkung 9.15 Ist E ein Körper, so ist

$$P(E) = \langle\{1_E\}\rangle_{\text{Körper}} \supset \left\{\frac{a}{b} : a, b \in \mathbb{Z}1_E,\ b \neq 0\right\} =: Q.$$

Da Q (etwa nach Bemerkung 9.13) ein Unterkörper von E ist, der 1_E enthält, ist schon $P(E) = Q$. Speziell für $E = \mathbb{Q}$ gilt also $P(\mathbb{Q}) = \mathbb{Q}$.

Satz 9.16 *Es sei E ein Körper mit Charakteristik q. Dann gilt*

$$P(E) \simeq \begin{cases} \mathbb{Z}_q & \text{falls } q \in \mathbb{P}, \\ \mathbb{Q} & \text{falls } q = 0. \end{cases}$$

Beweis. Im Fall $q \in \mathbb{P}$ ist $\mathbb{Z}_q$ ein Körper. Nach Satz 9.7 ist dann auch $\mathbb{Z}1_E$ ein Körper (da isomorph zu $\mathbb{Z}_q$). Aus $P(E) \supset \mathbb{Z}1_E$ folgt $P(E) = \mathbb{Z}1_E$.

Im Fall $q = 0$ ist $\mathbb{Z}1_E \simeq \mathbb{Z}$ und $f : \mathbb{Z} \to \mathbb{Z}1_E$ mit $f(m) := m1_E$ ein Isomorphismus, also $f : \mathbb{Z} \to E$ eine Ringeinbettung. Für die kanonische Fortsetzung $F : \mathbb{Q} = \text{Quot}(\mathbb{Z}) \to E$ gilt dann

$$F\left(\frac{m}{n}\right) = \frac{m1_E}{n1_E} \quad \text{für } m, n \in \mathbb{Z}, n \neq 0$$

und damit $F(\mathbb{Q}) = P(E)$ mit Bemerkung 9.15. Nach Bemerkung/Definition 9.11 ist $P(E)$ isomorph zu $\mathbb{Q}$. □

Satz 9.17 *Es sei E ein endlicher Körper. Dann hat E eine Primzahlcharakteristik q und mit $d := [E : P(E)]$ gilt $\#E = q^d$.*

Beweis. Nach Satz 9.16 ist $P(E) \simeq \mathbb{Z}_q$ für ein $q \in \mathbb{P}$ und damit $\#P(E) = \#\mathbb{Z}_q = q$. Aus $d < \infty$ folgt, dass E isomorph zu $(P(E))^d$ ist (Lineare Algebra), also insbesondere $\#E = q^d$. □

Index