Jürgen Müller

Elementare Zahlentheorie und Algebra

Skriptum zur Vorlesung
Wintersemester 2017/2018

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

Universität Trier
Fachbereich IV
Mathematik/Analysis

Inhaltsverzeichnis

1 Der Ring der ganzen Zahlen

Wir gehen zunächst kurz auf das "Wesen" natürlicher bzw. ganzer Zahlen ein.

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.

Bei assoziativen Verknüpfungen lässt man die Klammern meist weg, setzt also zum Beispiel $xyz \coloneqq (xy)z = x(yz)$. 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 $(M, \cdot, e)$. Eine Halbgruppe M mit kommutativer Verknüpfung $\cdot$ heißt **kommutativ** oder auch **abelsch**.

Bemerkung 1.3 Die **natürlichen Zahlen** können axiomatisch beschrieben werden als ein Tripel $(\mathbb{N}, 1, \nu)$ mit den drei Eigenschaften (**Peano-Axiome**):

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

(N2) $\nu : \mathbb{N} \to \mathbb{N}$ ist eine injektive Funktion mit $1 \notin \nu(\mathbb{N})$.

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

Die Zahl $\nu(n)$ nennt man Nachfolger von n. Damit kann man die arabischen Ziffern definieren durch $2 := \nu(1)$, $3 := \nu(2)$, $4 := \nu(3)$, $5 := \nu(4)$, $6 := \nu(5)$, $7 := \nu(6)$, $8 := \nu(7)$ und $9 := \nu(8)$. Weiter kann man – mit viel Aufwand – zeigen:

Auf $\mathbb{N}$ existiert genau eine assoziative und kommutative Verknüpfung $+$ mit $n+1 = \nu(n)$ und $n + \nu(m) = \nu(n+m)$ für $n, m \in \mathbb{N}$. Unter Verwendung der Addition ist eine Ordnungsrelation $<$ auf $\mathbb{N}$ definiert durch $n < m$ genau dann, wenn $m = n + k$ für ein $k \in \mathbb{N}$. Weiter kann man zeigen: Auf $\mathbb{N}$ existiert genau eine assoziative und kommutative Verknüpfung $\cdot$ so, dass $n \cdot 1 = 1$ ist und dass $m(n+1) = mn + m$ für $n, m \in \mathbb{N}$ gilt. Damit sind $(\mathbb{N}, \cdot)$ eine abelsche Halbgruppe und $(\mathbb{N}, \cdot, 1)$ ein abelsches Monoid.

Erweitert man $\mathbb{N}$ um ein Element 0 zu $\mathbb{N}_0$ mit $0 < n$ für alle $n \in \mathbb{N}$ und so, dass $n+0 := 0+n := n$ und $n \cdot 0 := 0 \cdot n := 0$ für alle $n \in \mathbb{N}_0$, so sind $(\mathbb{N}_0, +, 0)$ und $(\mathbb{N}_0, \cdot, 1)$ abelsche Monoide mit den **Kürzungsregeln**

$$n + m = n + k \;\Rightarrow\; m = k \quad \text{und} \quad n \cdot m = n \cdot k,\, n \neq 0 \;\Rightarrow\; m = k\,.$$

Schließlich folgt aus dem Prinzip der vollständigen Induktion die wichtige **Wohlordnungseigenschaft** von $\mathbb{N}$: *Jede nichtleere Menge $M \subset \mathbb{N}$ hat ein Minimum.*

Beispiel 1.4 Es sei X eine Menge. Dann heißt

$$\mathscr{P}(X) := \{A : A \subset X\}$$

die **Potenzmenge** von X. Ist $(X, \cdot)$ eine Halbguppe, so definiert das **Komplexprodukt**

$$A \cdot B := \{xy : x \in A,\, y \in B\} \qquad (A, B \subset X)$$

eine assoziative Verknüpfung $\cdot$ auf $\mathscr{P}(X)$, also ist $(\mathscr{P}(X), \cdot)$ eine Halbgruppe. Ist $(X, \cdot, e)$ ein Monoid, so ist auch $(\mathscr{P}(X), \cdot, \{e\})$ ein Monoid. Im Falle einer einpunktigen Menge $A = \{x\}$ schreibt man meist kurz xB statt $\{x\} \cdot B$ und im Falle des Pluszeichens als Verknüpfung auf X natürlich auch $A + B$ statt $A \cdot B$ und $x + B$ statt xB. Die Menge $A + B$ heißt dann auch **Minkowski-Summe** von A und B.

Definition 1.5 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 1.6 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

$$y_1 \;=\; y_1 e \;=\; y_1(xy_2) \;=\; (y_1x)y_2 \;=\; ey_2 \;=\; y_2.$$

Für invertierbare x bezeichnet man 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

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

da $x^{-1}x = xx^{-1} = e$ 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 $e \in M^*$ und es gilt $xy \in M^*$ sowie $x^{-1} \in M^*$ für $x, y \in M^*$. Damit ist $(M^*, \cdot, e)$ eine Gruppe.

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 1.7 Es sei $X \neq \emptyset$ ein Menge. Dann ist [1]

$$S(X) \;:=\; \{f \in \mathrm{Abb}(X) : f \text{ bijektiv}\}$$

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

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

[1] Sind X, Y nichtleere Mengen, so setzen wir $Y^X := \mathrm{Abb}(X, Y) := \{f : X \to Y\}$ und $\mathrm{Abb}(X) := \mathrm{Abb}(X, X)$.

(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 heißen $(R, +, \cdot)$ **Ring**, das neutrale Element 0 bezüglich $+$ **Null(element)** und das neutrale Element 1 bezüglich $\cdot$ **Eins(element)**. Ist $(R, \cdot)$ 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 1.9 Das Monoid $(\mathbb{N}_0, +, 0)$ lässt sich durch Äquivalenzklassenbildung in $\mathbb{N}_0 \times \mathbb{N}_0$ 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 $1 = 1_{\mathbb{Z}}$. Zudem 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 $z > 0$). Man setzt $|a| := \operatorname{sign}(a) \cdot a$, wobei

$$\operatorname{sign}(a) := \begin{cases} 1, & \text{falls } a > 0 \\ 0, & \text{falls } a = 0 \\ -1, & \text{falls } a < 0 \end{cases}.$$

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.

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

Bemerkung 1.10 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 $(x - y)z = xz - yz$.

Satz 1.11 (**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]. □

Bemerkung 1.12 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 $\prod_{\ell=1}^{0} x_\ell := e$ und $\prod_{\ell=1}^{k} x_\ell := (\prod_{\ell=1}^{k-1} x_\ell) \cdot x_k$ für $k = 1, \ldots, N$. Außerdem schreiben wir $x^k := \prod_{\ell=1}^{k} x$ (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 $\prod_{j\in J} x_j$ (wohl-)definiert durch $\prod_{j\in J} x_j := \prod_{\ell=1}^{k} x_{j_\ell}$, 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

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

auch kurz $\prod_{j\in J} x_j := \prod_{j\in J,\, x_j \neq e} x_j$. Tupel $x \in M^{(J)}$ nennt man auch **abbrechend**. Schließlich setzen wir für $A \subset M$ noch

$$A^{(J)} := A^{(J,e)} := \{x \in M^{(J)} : x_j \in A \ (j \in J)\}.$$

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

Im Weiteren betrachten wir allgemeine Summen in $(\mathbb{Z}, +, 0)$ und Produkte in $(\mathbb{Z}, \cdot, 1)$. Als Anwendung der Division mit Rest beweisen wir ein Ergebnis über die Darstellung natürlicher Zahlen.

Satz 1.13 *Es sei $q \in \mathbb{N}$ mit $q \geq 2$ und $A := \{0, \ldots, q-1\}$. Dann existiert für jedes $n \in \mathbb{N}_0$ genau eine Folge $a = (a_j) = \big(a_j(n)\big) \in A^{(\mathbb{N}_0)} = A^{(\mathbb{N}_0,0)}$ mit*

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

Beweis. 1. Eindeutigkeit: Angenommen, es existieren $a, b \in A^{(\mathbb{N}_0)}$ mit $a \neq b$ und $\sum\limits_{j \in \mathbb{N}_0} a_j q^j = \sum\limits_{j \in \mathbb{N}_0} b_j q^j$. Dann gilt für $m := \max\{j : a_j \neq b_j\}$ (ohne Einschränkung $a_m > b_m$)

$$0 = (a_m - b_m) q^m + \sum_{j=0}^{m-1} (a_j - b_j) q^j \geq q^m - (q-1) \sum_{j=0}^{m-1} q^j = 1.$$

Widerspruch.

2. Wir zeigen die Existenz per Induktion nach n.
Für $n = 0$ ist $a_j(0) \coloneqq 0$ für $j \in \mathbb{N}_0$ passend.
Induktionsschritt $n-1$ auf n: Es sei $k \in \mathbb{N}_0$ mit $q^k \leq n < q^{k+1}$. Division mit Rest ergibt

$$n = m q^k + n'$$

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 $\big(a_j(n')\big) \in A^{(\mathbb{N}_0)}$ 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

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

□

Für jedes q ist die durch Satz 1.13 wohldefinierte Abbildung

$$\mathbb{N}_0 \ni n \mapsto \big(a_j(n)\big)_{j \in \mathbb{N}_0} \in A^{(\mathbb{N}_0)}$$

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 $a_r \dots a_0$ statt $(a_r \dots a_0)_{\text{Zehn}}$, also zum Beispiel Zehn $= 10$.

Definition 1.14 Ein Ring R heißt **nullteilerfrei** wenn für beliebige $x, y \in R$ aus $xy = 0$ schon $x = 0$ oder $y = 0$ folgt. Ein kommutativer Ring R mit $1 \neq 0$ heißt **Integritätsring** oder **Integritätsbereich**, falls er nullteilerfrei ist, und **Körper**, falls $R^* = R \setminus \{0\}$ gilt (also jedes $x \neq 0$ invertierbar bezüglich $\cdot$ ist).

Bemerkung 1.15 1. Jeder Körper ist ein Integritätsbereich (sind $x, y \in R^*$, so ist auch $xy \in R^*$).

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

- Aus $xy = xz$ folgt $x = 0$ oder $y = z$.
- Aus $yx = zx$ folgt $x = 0$ 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 1.16 $(\mathbb{Z}, +, \cdot)$ ist ein Integritätsring, aber kein Körper; $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$ sind Körper.

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 andernfalls $a \nmid b$. Ist dabei $a \neq 0$, so ist q eindeutig bestimmt. Wir setzen dann $b/a := q$. 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 $|a| \leq |b|$.

Es sei R ein kommutativer Ring. Wir verwenden im Weiteren Rechenregeln für Minkowskisummen und Komplexprodukte in $\mathscr{P}(R)$. Zu beachten ist dabei, dass das Komplexprodukt nicht distributiv über der Minkowskisumme ist, d. h. im Allgemeinen gilt *nicht* $A(B+C) = AB+AC$ ([Ü]). Allerdings gilt immerhin stets $A(B+C) \subset AB+AC$ und $a(B + C) = aB + aC$ für $A, B, C \subset R$ und $a \in R$.

Sind speziell $a, b \in \mathbb{Z}$, so ist $(a\mathbb{Z})(b\mathbb{Z}) = (ab)(\mathbb{Z}\mathbb{Z}) = (ab)\mathbb{Z}$. Wir wollen nun die wesentlich interessantere Frage beantworten, wie $a\mathbb{Z} + b\mathbb{Z}$ dargestellt werden kann.

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** oder auch **relativ prim**. 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 (**Lemma von Bézout**)
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

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

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

Es sei $a = qm + r$ wie in Satz 1.11. 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**[2]: Sind $a, b \in \mathbb{Z} \setminus \{0\}$, so wendet man sukzessive Division mit Rest an, startend mit $r_0 = b, r_1 = |a|$:

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

Da nach Satz 1.11 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

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

Denn: Es sei $d := \mathrm{ggT}(a, b)$. Durch Nachverfolgen des Gleichungssystems von unten nach oben sieht man

$$r_{n-1} \in r_n\mathbb{Z},\ r_{n-2} = q_{n-1}r_{n-1} + r_n \in r_n\mathbb{Z}, \ldots, r_1 \in r_n\mathbb{Z},\ r_0 \in r_n\mathbb{Z},$$

[2]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.

also $r_n|a$ und $r_n|b$ und damit insbesondere $r_n \leq d$.

Andererseits sieht man durch Lesen des Gleichungssystems von oben nach unten und mit Satz 2.4

$$r_2 \in a\mathbb{Z} + b\mathbb{Z}, \ldots, r_n \in a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z} .$$

Aus $r_n \geq 1$ folgt $r_n \geq d$.

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 Folgerung 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

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

3. 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

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

Wichtig für alles Weitere ist folgender Fakt:

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

Denn: Gilt $p|bc$ 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 $b \in B$.

Wir zeigen nun, 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 bezüglich der Multiplikation angesehen werden.

Satz 2.8 (**Primfaktorzerlegung, Fundamentalsatz der Arithmetik**)
Für jedes $n \in \mathbb{N}$ existiert genau ein Tupel $(\alpha_p(n))_{p\in\mathbb{P}} \in \mathbb{N}_0^{(\mathbb{P})} = \mathbb{N}_0^{(\mathbb{P},0)}$ mit

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

Beweis. 1. Eindeutigkeit: Wir zeigen: Ist $n \in \mathbb{N}$ und sind $\nu := (\nu_p), \mu := (\mu_p) \in \mathbb{N}_0^{(\mathbb{P})}$ mit

$$n = \prod_{p\in\mathbb{P}} p^{\nu_p} = \prod_{p\in\mathbb{P}} p^{\mu_p}\ ,$$

so gilt $\mu_p = \nu_p$ für alle $p \in \mathbb{P}$ (also $\mu = \nu$).

Angenommen, dies ist nicht der Fall. Dann sei $n \in \mathbb{N}$ die minimale natürliche Zahl, für die zwei solche Darstellungen existieren, also $\nu \neq \mu$ mit $n = \prod\limits_{p\in\mathbb{P}} p^{\nu_p} = \prod\limits_{p\in\mathbb{P}} p^{\mu_p}$. Dabei ist $n > 1$, also $\nu \neq 0$. Wir wählen ein $q \in \mathbb{P}$ mit $\nu_q \neq 0$. Dann folgt aus $q \Big| \prod\limits_{p\in\mathbb{P}} p^{\mu_p}$ mit B/D 2.7 die Existenz eines $q' \in \mathbb{P}$ mit $\mu_{q'} > 0$ und $q|q'$. Da q' eine Primzahl ist, gilt schon $q = q'$. Durch Kürzen ergibt sich, dass n/q die zwei Darstellungen

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

hat. Dies widerspricht der Minimalität von n.

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

Es sei also $n \in \mathbb{N} \setminus \{1\}$. Dann ist $p_1 := \min\{k > 1 : k|n\}$ 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

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

□

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

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

wohldefiniert 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

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

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. Für $(a_j)_{j \in J} \in [0, \infty)^J$ (also hier (a_j) nicht abbrechend) setzen wir

$$\sum_{j \in J} a_j := \sup_{E \subset J \text{ endlich}} \sum_{j \in E} a_j \in [0, \infty].$$

Ist $\sum_{j \in J} a_j < \infty$, so sprechen wir von Konvergenz und im Falle $\sum_{j \in J} a_j = \infty$ von Divergenz der Reihe. Zunächst gilt

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

Beweis. Angenommen, $\mathbb{P}$ sei endlich. Dann ist $n := 1 + \prod_{p\in\mathbb{P}} p \in \mathbb{N}$ und $n > 1$. Ist $q \in \mathbb{P}$ mit $q|n$, so folgt aus $q|\prod_{p\in\mathbb{P}} p$ auch $q|(n - \prod_{p\in\mathbb{P}} p = 1)$. Widerspruch. □

Bekanntlich divergiert die harmonische Reihe $\sum_{n\in\mathbb{N}} 1/n$. Dies kann man so interpretieren, dass die Folge $(n)_{n\in\mathbb{N}}$ nicht sehr schnell wächst. Andererseits konvergiert die Reihe $\sum_{n\in\mathbb{N}} 1/n^2$ über die Reziproken der Quadratzahlen. Also wächst die Folge $(n^2)_{n\in\mathbb{N}}$ der Quadratzahlen viel schneller als die Folge der natürlichen Zahlen – Quadratzahlen sind in diesem Sinne „relativ selten“ unter den natürlichen Zahlen. Wir zeigen, dass andererseits in diesem Sinne „relativ viele“ natürliche Zahlen Primzahlen sind:

Satz 2.11 (**Euler**)
Die Reihe über die Reziproken der Primzahlen divergiert, d. h. $\sum_{p\in\mathbb{P}} 1/p = \infty$.

Beweis. Für $E \subset \mathbb{P}$ endlich sei $M_E := \{n = \prod_{p\in E} p^{\nu_p} : (\nu_p) \in \mathbb{N}_0^E\}$. Für $0 \le x \le 1/2$ gilt $\dfrac{1}{1-x} \le \mathrm{e}^{2x}$. Also folgt

$$\prod_{p\in E} \frac{1}{1-1/p} \le \exp\left(2\sum_{p\in E}\frac{1}{p}\right).$$

Aus der Eindeutigkeitsaussage des Fundamentalsatzes der Arithmetik ergibt sich

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

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

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

und damit

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

□

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

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

(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. Ein Hilfsmittel ist folgender Satz (wobei $\lfloor \cdot \rfloor$ = die Gaußklammer bezeichnet).

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

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

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

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

Außerdem ist $\alpha_p(k) = \#\{\nu \in \mathbb{N} : p^\nu | k\}$ für $k \in \mathbb{N}$. Damit erhalten wir

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

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

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

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

Beweis. 1. Für $n \in \mathbb{N}$ gilt

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

und daher

$$n \ln 2 \;\le\; s_n := \ln \binom{2n}{n} \;\le\; 2n \ln 2.$$

2. Für $n \in \mathbb{N}$ ist unter Verwendung von Satz 2.12

$$\begin{aligned} s_n &= \ln\Big((2n)!\Big) - 2\ln(n!) \\ &= \sum_{p\in\mathbb{P}} \ln p \cdot \alpha_p\Big((2n)!\Big) - 2\sum_{p\in\mathbb{P}} \ln p \cdot \alpha_p(n!) \\ &= \sum_{(\mathbb{P}\ni)p\le 2n} \ln p \sum_{\nu=1}^{\lfloor \frac{\ln 2n}{\ln p}\rfloor} \left(\left\lfloor \frac{2n}{p^\nu} \right\rfloor - 2\left\lfloor \frac{n}{p^\nu} \right\rfloor \right). \end{aligned}$$

Weiter gilt für $x \in \mathbb{R}$

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

Damit ergibt sich einerseits

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

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

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

3. Beweis von "$\ldots \le \pi(n)$": Für $n \in \mathbb{N}$ gilt mit 1. und (2.2)

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

Aus $\ln 2 > 5/8$ und der Monotonie von $x \mapsto x/\ln(x)$ auf $[\mathrm{e}, \infty)$[3] folgt

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

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

[3] Ist $\alpha > 0$ und $\varphi(x) := x^{-\alpha}\ln(x)$ für $x > 0$, so gilt $\varphi'(x) > 0$ für $0 < x < \mathrm{e}^{1/\alpha}$ und $\varphi'(x) < 0$ für $x > \mathrm{e}^{1/\alpha}$.

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

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

Für $n \in \mathbb{N}$ erhalten wir mit (2.3) und 1.

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

Damit folgt für $k \in \mathbb{N}_0$

$$\vartheta(2^{k+1}) - \vartheta(2^k) \;\leq\; 2^{k+1} \ln 2,$$

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

$$\vartheta(2^{k+1}) \;=\; \sum_{\ell=0}^{k} \Big(\vartheta(2^{\ell+1}) - \vartheta(2^\ell)\Big) \;\leq\; \sum_{\ell=0}^{k} 2^{\ell+1} \ln 2 \;=\; 2(2^{k+1} - 1) \ln 2 \;\leq\; 2^{k+2} \ln 2.$$

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

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

speziell für $y = n^{2/3}$ also

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

und damit

$$\pi(n) \;\leq\; n^{2/3} + \frac{3}{2}\, \frac{4n \ln 2}{\ln n} \;=\; \frac{n}{\ln n} \left(\frac{\ln n}{n^{1/3}} + 6 \ln 2 \right).$$

Da $x \mapsto x^{-1/3} \ln(x)$ an $x = \mathrm{e}^3$ maximal wird, folgt

$$\pi(n) \;\leq\; \frac{n}{\ln n} \left(\frac{3}{\mathrm{e}} + 6 \ln 2 \right) \;<\; 6\, \frac{n}{\ln n}.$$

□

Bemerkung 2.14 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 $x^m + 1 = -((-x)^m - 1)$).

Bemerkung 2.15 Ein schwieriges Problem liegt in der konkreten Bestimmung großer Primzahlen. Ein möglicher Ansatz besteht 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 $k \in \mathbb{P}$.

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

   Denn: Es sei $k \neq 2^n$ 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 $p \in \{2, 3, 5, 7, 13, 17, 19\}$. Derzeit (Stand 11/2017) sind 49 Mersenne-Zahlen als prim erkannt, die größte davon (im Jahr 2016 identifiziert) ist

$$2^{74.207.281} - 1,$$

mit 22.338.618 Stellen im Dezimalsystem; siehe dazu die Webseite https://primes.utm.edu/mersenne/index.html#known von C. 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 $n \in \{0, 1, 2, 3, 4\}$. Andererseits ist $F_5 = 2^{2^5} + 1 = 2^{32} + 1$ keine Primzahl.

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

$$(5^4 + 2^4) | (5^4 2^{28} + 2^{32}).$$

   Aus $(a + 1) | (a + 1)(a - 1)(a^2 + 1) = a^4 - 1$ folgt außerdem

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

   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 $\mathbb{Z}_m := \mathbb{Z}/_{\equiv_m} = \{[a]_m : a \in \mathbb{Z}\}$ für die Quotientenmenge. 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 1.11 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 $(\mathbb{Z}, +, \cdot)$.

Beispiel 3.2 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 3.3 *Es sei $n \in \mathbb{N}$ mit der Dezimaldarstellung $n = a_r a_{r-1} \ldots a_0$. Dann gilt:*

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

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

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

$$[n]_m \;=\; \sum_{j=0}^{r} [a_j]_m \;=\; \Big[\sum_{j=0}^{r} a_j\Big]_m$$

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)

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

und wir erhalten die dritte Aussage. □

Zurück zur allgemeinen Theorie der Ringe $\mathbb{Z}_m$: Wir haben in Beispiel 3.2.2 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 3.4 *Für $m \in \mathbb{N}$ und $a \in \mathbb{Z}$ gilt: Genau dann existiert ein $x \in \mathbb{Z}$ mit $ax \equiv 1 \mod m$, 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 3.5 Es sei $m \in \mathbb{N}$. Ist $a \in \mathbb{Z}$ teilerfremd zu m, so heißt $[a]_m$ **prime Restklasse modulo** m. 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 1.6.2 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 3.4.

Beispiel 3.6 $\mathbb{Z}_4^* = \big\{[1]_4, [3]\big\}$ ist eine zweielementige Gruppe (bezüglich $\cdot$).

Satz 3.7 *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 3.5. 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 3.8 Ist $1 < m \in \mathbb{N} \setminus \mathbb{P}$, so ist der Ring $(\mathbb{Z}_m, +, \cdot)$ nicht nullteilerfrei, denn dann existieren $r, s \in \{2, \ldots, m-1\}$ mit $m = rs$ und damit $[0]_m = [r]_m[s]_m$.

Definition 3.9 Es seien $(M, \cdot)$ eine Halbgruppe und $U \subset M$. Dann heißt U eine **Unterhalbgruppe**, falls $(U, \cdot_U)$ mit $x \cdot_U y := xy$ für $x, y \in U$ 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 $(U, \cdot_U, e)$ Gruppen, so heißt U **Untergruppe** von M.

Man schreibt in den obigen Fällen jeweils wieder $\cdot$ statt $\cdot_U$.

Wir konzentrieren uns nun auf Gruppen.

Bemerkung 3.10 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) ⇒ (ii): Nach Definition ist $e \in U$. Sind $a, b \in U$, so ist $ab \in U$ da $\cdot_U$ eine Verknüpfung auf U ist. Außerdem ist $a^{-1} \in U$ aufgrund der Eindeutigkeit der Inversen (in G). Folglich gilt (ii).
(ii) ⇒ (i): Klar.
(ii) ⇒ (iii): Klar.

(iii) $\Rightarrow$ (ii): 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

$$U \ni x \mapsto ax \in aU$$

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 3.11 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 3.12 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[4], 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 $\langle a \rangle$.

Satz 3.13 *Es seien G eine Gruppe und $M \subset G$, $M \neq \emptyset$. Dann gilt*

1. $\langle M \rangle = \bigcup_{n \in \mathbb{N}} \Big\{ \prod_{j=1}^{n} a_j^{\varepsilon_j} : a_j \in M,\, \varepsilon_j \in \{-1, 1\}\ (j = 1, \ldots, n) \Big\}$.

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

2. Ist $\langle M\rangle$ abelsch, so ist

$$\langle M\rangle = \Big\{ \prod_{a\in M} a^{\nu_a} : (\nu_a)_{a\in M} \in \mathbb{Z}^{(M)} \Big\}.$$

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

$\langle M\rangle \subset U$: Es gilt $M \subset U$ und U ist eine Untergruppe von G nach Kriterium 3.10.(iii), denn mit $a, b \in U$, 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

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

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

$U \subset \langle M\rangle$: Ist W eine Untergruppe von G mit $M \subset W$, so gilt $U \subset W$ nach dem Kriterium 3.10(ii); also ist $U \subset \langle M\rangle$.

2. Nun sei $\langle M\rangle$ abelsch und V die rechte Seite in 2.

$V \subset \langle M\rangle$: Genauso wie $U \subset \langle M\rangle$.

$U \subset V$: Sind $a_1, \dots a_n \in M$ sowie $\varepsilon_1, \dots, \varepsilon_n \in \{-1, 1\}$ und setzt man $\nu_a := \sum_{j:a_j=a} \varepsilon_j$ $(a \in M)$, so gilt $a_1^{\varepsilon_1} \cdot \ldots \cdot a_n^{\varepsilon_n} \;=\; \prod_{a\in M} a^{\nu_a} \;\in\; V$. □

Bemerkung und Definition 3.14 Es sei G eine Gruppe.

1. Für $a \in G$ ist nach Satz 3.13

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

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 3.15 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 ist insbesondere

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

und damit $\mathbb{Z}_m$ 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 3.4 überlegt.

Satz 3.16 *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*

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

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 1.11 (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 3.17 Es seien G eine Gruppe und $U \subset G$ eine Untergruppe. Setzt man für $a, a' \in G$

$$a \sim a' :\Leftrightarrow a^{-1}a' \in U \quad (\Leftrightarrow a' \in aU)\,,$$

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

Durch Betrachtung von $a'a^{-1}$ anstelle von $a^{-1}a'$ erhält man entsprechend die **Rechtsnebenklassen** Ua von U. Für abelsche Gruppen gilt natürlich $aU = Ua$ für $a \in G$.

Stets (also auch im nichtabelschen Fall) ist für $a \in G$ wegen der Injektivität von $U \ni x \mapsto ax$ und von $U \ni x \mapsto xa$

$$\#(aU) \;=\; \operatorname{ord} U \;=\; \#(Ua).$$

Weiter setzen wir

$$G/U := G/_U \;:=\; \{aU : a \in G\} \quad \text{und} \quad {}_U\backslash G \;:=\; \{Ua : a \in G\}\,.$$

Man sieht leicht, dass die Abbildung $G/_U \ni aU \mapsto U(a^{-1}) \in {}_U\backslash G$ (wohldefiniert und) bijektiv ist. Also gilt $\#(G/_U) = \#({}_U\backslash G)$ und der gemeinsame Wert

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

heißt **Index** von U (in G).

Beispiel 3.18 Es seien $G = (\mathbb{Z}, +, 0)$, $m \in \mathbb{N}$ und $U := m\mathbb{Z}$. Dann gilt (beachte $aU = a + U$ und $Ua = U + a$ hier)

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

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

Satz 3.19 (**Lagrange**).
Es seien G eine endliche Gruppe und U eine Untergruppe. Dann gilt

$$\operatorname{ord} G = \operatorname{ord} U \cdot (G : U)$$

und insbesondere $\operatorname{ord} U \,|\, \operatorname{ord} G$.

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

$$\operatorname{ord} G = \sum_{aU \in G/_U} \#(aU) = \sum_{aU \in G/_U} \operatorname{ord} U = \operatorname{ord} U \cdot (G : U).$$

□

Bemerkung 3.20 Sind G eine endliche Gruppe und $x \in G$, so ergibt sich $\operatorname{ord}(x) | \operatorname{ord}(G)$ aus dem Satz von Lagrange (angewandt auf $U := \langle x \rangle$) und mit Satz 3.16 dann auch $x^{\operatorname{ord}(G)} = e$.

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

Definition 3.21 Die durch

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

definierte Funktion $\varphi : \mathbb{N} \to \mathbb{N}$ heißt **Eulersche φ-Funktion**. Dabei gilt $\varphi(1) = 1$ und $\varphi(p) = p - 1$ für $p \in \mathbb{P}$ nach Satz 3.7.

Satz 3.22 *Es sei $a \in \mathbb{Z}$.*
1. (**Euler**) *Ist $m \in \mathbb{N}$ mit $\operatorname{ggT}(a,m) = 1$, so gilt*

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

2. (**kleiner Satz von Fermat**) *Ist $p \in \mathbb{P}$ kein Teiler von a, so gilt*

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

Beweis. 1. Bemerkung 3.20 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

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

□

Wir betrachten jetzt Kongruenzen der Form $[a]_m[x]_m = [b]_m$ im Restklassenring $\mathbb{Z}_m$, genannt **lineare Kongruenzen**.

Satz 3.23 *Es seien $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$ und $d := \operatorname{ggT}(a,m)$.*
1. Die Gleichung

$$ax \;\equiv\; b \mod m, \tag{3.1}$$

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 (3.1) genau dann, wenn

$$\frac{a}{d}x \;\equiv\; \frac{b}{d} \mod \frac{m}{d}. \tag{3.2}$$

gilt.

2. Ist $x \in \mathbb{Z}$ eine Lösung von (3.2), so ist $L_x := x + (m/d)(\{0,\dots,d-1\}$ eine d-elementige Menge paarweise modulo m inkongruenter Lösungen von (3.1) und die Lösungsmenge von (3.1) ist $L_x + m\mathbb{Z}$.

Beweis. 1. Die Gleichung (3.1) 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

$$x \text{ löst (3.1)} \quad \Leftrightarrow \quad m|(ax-b) \quad \Leftrightarrow \quad \frac{m}{d}\Big|\Big(\frac{a}{d}\,x - \frac{b}{d}\Big) \quad \Leftrightarrow \quad x \text{ löst (3.2)}.$$

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 3.5, hat also ein Inverses $[c]_{m/d}$, und für $x \in \mathbb{Z}$ gilt die Äquivalenzkette

$$x \text{ löst (3.2)} \quad \Leftrightarrow \quad \Big[\frac{a}{d}\Big]_{\frac{m}{d}}\,[x]_{\frac{m}{d}} = \Big[\frac{b}{d}\Big]_{\frac{m}{d}} \quad \Leftrightarrow \quad [x]_{\frac{m}{d}} = \Big[\frac{cb}{d}\Big]_{\frac{m}{d}}.$$

Sind nun x Lösung von (3.2) und $y \in \mathbb{Z}$, so ergibt sich mit Division mit Rest

$$y \text{ löst (3.2)} \Leftrightarrow [y]_{\frac{m}{d}} = [x]_{\frac{m}{d}} \Leftrightarrow y \in x + \frac{m}{d}\mathbb{Z} = x + m\mathbb{Z} + \frac{m}{d}\{0, \ldots, d-1\} = L_x + m\mathbb{Z}\,.$$

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

Beispiele 3.24 1. Wir betrachten die Kongruenz

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

In der Notation von Satz 3.23 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 (3.2), also

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

Eine Lösung ist $x = 5$. Also ist hier $L_x = \{5, 14, 23\}$ und $\{5, 14, 23\} + 27 \cdot \mathbb{Z}$ die Lösungsmenge von (3.1).

2. Die Kongruenz

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

hat nach Satz 3.23 wegen $\mathrm{ggT}(6, 27) = 3 \not| 2$ keine Lösung.

Von grundlegender Bedeutung ist das folgende Ergebnis über simultane Kongruenzen.

Satz 3.25 *Es seien $m_1, \ldots, m_N \in \mathbb{N}$ 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 $j \in \{1, \ldots, N\}$ gilt.

2. Durch

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

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

3. (**Chinesischer Restsatz**)[5] *Sind $b_1, \ldots, b_N \in \mathbb{Z}$, so existiert ein $x \in \mathbb{Z}$ mit*

$$x \;\equiv\; b_j \mod m_j \quad \text{für } j \in \{1, \ldots, N\}, \tag{3.3}$$

und mit jedem solchen x ist die Lösungsmenge von (3.3) dann $[x]_m = x + m\mathbb{Z}$.

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 (3.3), und ein $y \in \mathbb{Z}$ ist genau dann Lösung von (3.3) wenn $y \in [x]_m$ gilt. □

Bemerkung 3.26 Die Berechnung einer Lösung von (3.3) lässt sich wie folgt auf die Berechnung je einer Lösung von N Gleichungen des Typs (3.1) zurückführen:

Mit der Notation und den Voraussetzungen von Satz 3.25 sei für $j \in \{1, \ldots, N\}$

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

[5] 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 3.27.

und damit $\mathrm{ggT}(a_j, m_j) = 1$ nach Satz 2.6.3 (induktiv angewandt), so dass nach Satz 3.23 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 (3.3), 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 3.27 Wir betrachten das System simultaner Kongruenzen

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

In der Notation von Bemerkung 3.26 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 linearen (und nicht simultanen) 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

$$x := a_1 x_1 + a_2 x_2 + a_3 x_3 = 35 \cdot 1 + 21 \cdot 3 + 15 \cdot 2 = 128$$

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.

Bemerkung und Definition 3.28 Nach dem Fermatschen Satz 3.22.2 gilt für $n \in \mathbb{N}$:

Existiert ein $a \in \mathbb{N}$ *mit* $\mathrm{ggT}(a, n) = 1$ *und* $a^{n-1} \not\equiv 1 \mod n$, *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. Ist n pseudoprim zur Basis a für jedes a mit $\mathrm{ggT}(a, n) = 1$, so heißt n eine **Carmichaelzahl**. Wir werden nun zeigen, dass es Carmichaelzahlen gibt. 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.

Definition 3.29 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 $n = \prod\limits_{p|n} p$ gilt ([Ü]).

Satz 3.30 *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.*[7]

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 3.22.2

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

Wegen der Quadratfreiheit von n liefert nun Satz 3.25.1

$$a^{n-1} \equiv 1 \mod n.$$ □

Beispiel 3.31 Es ist $561 = 3 \cdot 11 \cdot 17$ quadratfrei, und es gilt $2|560, 10|560$ und $16|560$. Also ist 561 nach Satz 3.30 eine Carmichael-Zahl (und genauer die kleinste).[8]

Wir betrachten noch einmal die Eulersche φ-Funktion. Mit f aus Satz 3.25 gilt

Satz 3.32 *Es seien $m_1, \ldots, m_N \in \mathbb{N}$ paarweise teilerfremd und $m := \prod\limits_{j=1}^{N} m_j$.*

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

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

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

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

[7] Es gilt auch die Umkehrung, d. h. jede Carmichaelzahl n ist quadratfrei und $(p-1)$ ist Teiler von $n-1$ für alle Primteiler p; siehe etwa O. Forster, Algorithmische Zahlentheorie, Springer, Wiesbaden, 2015.

[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.

wegen Bemerkung/Definition 3.5 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. für die zweite Gleichheit erhalten wir

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

□

Satz 3.33 *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

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

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

Ist nun $n \in \mathbb{N}$, so gilt $n = \prod\limits_{p|n} p^{\alpha_p(n)}$. 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 3.32 im ersten Schritt

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

□

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

Bemerkung 3.34 Es seien $p, q \in \mathbb{P}$ mit $p \neq q$ und

$$n := pq \qquad \text{sowie} \qquad m := (p-1)(q-1)(= \varphi(n)).$$

Ist $a \in \mathbb{N}$ teilerfremd zu m, so existiert nach Satz 3.4 ein (modulo m eindeutig bestimmtes) $b \in \mathbb{N}$ mit $ab \equiv 1 \mod m$. Mit diesen a, b gilt

$$(x^a)^b \;\equiv\; x \mod n \qquad \text{für } x \in \mathbb{Z}. \tag{3.4}$$

Denn: Wegen $m = (p-1)(q-1)$ 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 3.22.2 im ersten Fall des dritten Schrittes,

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

Analog erhalten wir

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

Mit Satz 3.25.1 und der Teilerfremdheit von p, q folgt (3.4).

Bemerkung 3.35 (Prinzip der RSA-Kryptographie)

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

- Der Empfänger E wählt p, q, a, b wie im Bemerkung 3.34 und stellt dem Sender S (oder auch mehreren Sendern) den öffentlichen Schlüssel (n, a) zur Verfügung
- S erstellt eine Nachricht x in Form eines Tupels

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

  und berechnet und sendet

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

- E berechnet daraus

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

  also x wegen (3.4)

Wesentlich dabei: Für große p, q ist $\varphi(n)$ und damit auch b aus der Kenntnis von n und a mit derzeit bekannten Verfahren praktisch nicht berechenbar. Weitere Informationen und Beispiele findet man etwa unter https://www.scai.fraunhofer.de/de/mediathek/material-fuer-mathematik-unterricht.html.

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

4 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 4.1 Es seien $(G,\cdot)$, $(H,\cdot_H)$ Halbgruppen und $\varphi : G \to H$ eine Funktion.

1. Gilt

$$\varphi(ab) = \varphi(a) \cdot_H \varphi(b) \quad \text{für } a,b \in G, \tag{4.1}$$

so heißt φ **(Halbgruppen-)Morphismus** (von G nach H).

2. Sind $(G,\cdot,e)$ und $(H,\cdot_H,e_H)$ Monoide und erfüllt φ neben (4.1) auch

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

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

Sind G und H Gruppen, so spricht man auch von einem **Gruppenmorphismus**. Einen injektiven Gruppenmorphismus φ nennt man auch **Monomorphismus** oder manchmal auch **Einbettung**, und einen surjektiven auch **Epimorphismus**. Ist φ bijektiv, so spricht man von einem **Isomorphismus**.

3. Um deulich zu machen, dass φ ein Morphismus ist, schreiben wir manchmal auch $\varphi : (G,\cdot) \to (H,\cdot_H)$ beziehungsweise $\varphi : (G,\cdot,e) \to (H,\cdot_H,e_H)$. Außerdem schreiben wir meist kurz $(H,\cdot)$ statt $(H,\cdot_H)$ beziehungsweise $(H,\cdot,e)$ statt $(H,\cdot_H,e_H)$, wenn sich der Bezug aus dem Zusammenhang ergibt.

Bemerkung 4.2 Es seien F,G,H Gruppen.

1. $\mathrm{id}_G : G \to G$ ist ein Isomorphismus.
2. Sind $\psi : F \to G$, $\varphi : G \to H$ Morphismen, so ist auch $\varphi\circ\psi : F \to H$ ein Morphismus.
3. Ist $\varphi : G \to H$ ein Isomorphismus, so ist auch $\varphi^{-1} : H \to G$ ein Isomorphismus.

   Denn: Es seien $u,v \in H$. Da φ surjektiv ist, existieren $a,b \in G$ mit $u = \varphi(a), v = \varphi(b)$, 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.

[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.

Satz 4.3 *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*

$$\varphi(a^{-1}) = \varphi(a)^{-1} \quad \text{für } a \in G. \tag{4.2}$$

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

Beweis. Es seien $u, v \in \varphi(G)$ und $a, b \in G$ mit $u = \varphi(a)$, $v = \varphi(b)$. Nach (4.1) ist dann $u \cdot v = \varphi(ab) \in \varphi(G)$. Damit $\varphi(G)$ eine Unterhalbgruppe von H.

Weiter gilt

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

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

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

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

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

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

□

Beispiele 4.4 1. Es sei $m \in \mathbb{N}$. Dann ist durch

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

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

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

φ ist ein Epimorphismus, aber kein Monomorphismus, da etwa $\varphi(0) = [0] = \varphi(m)$.

2. Durch

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

ist eine Gruppeneinbettung $\varphi : (\mathbb{R}, +, 0) \to (\mathbb{C}, +, 0)$ definiert.

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 $(K^*, \cdot, 1)$.

Bemerkung und Definition 4.5 Sind $(G, \cdot, e)$ und $(H, \cdot, e_H)$ Gruppen und ist $\varphi : G \to H$ ein Morphismus, so heißt $\operatorname{Kern}\varphi := \varphi^{-1}(\{e_H\}$ der **Kern** von φ. Dann ist $e \in \operatorname{Kern}\varphi$ und φ ein Monomorphismus genau dann, wenn $\operatorname{Kern}\varphi = \{e\}$ gilt.

Denn: Ist φ injektiv, so ist $\operatorname{Kern}\varphi$ einpunktig, also $\operatorname{Kern}\varphi = \{e\}$. Gilt umgekehrt $\operatorname{Kern}\varphi = \{e\}$, so folgt für $a, b \in G$ mit $\varphi(a) = \varphi(b)$ nach (4.2)

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

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

Beispiel 4.6 In Beispiel 4.4.1 ist $\operatorname{Kern}\varphi = \{x \in \mathbb{Z} : [x] = [0]\} = m\mathbb{Z}$, in 2. ist $\operatorname{Kern}\varphi = \{0\}$ und in 3. gilt

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

Man nennt $\mathrm{SL}_n(K)$ **spezielle lineare Gruppe**.

Satz 4.7 *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. *Ist $M \subset G$, so gilt $\varphi(\langle M\rangle) = \langle\varphi(M)\rangle$.*
5. *Ist G zyklisch, so ist auch $\varphi(G)$ zyklisch.*

Beweis. 1. ergibt sich unmittelbar aus Satz 4.3.

2. Es seien $a, b \in \varphi^{-1}(V)$. Dann gilt mit Kriterium 3.10(iii)

$$\varphi(a^{-1}b) = \varphi(a^{-1})\varphi(b) = \varphi(a)^{-1}\varphi(b) \in V,$$

also $a^{-1}b \in \varphi^{-1}(V)$. Wieder mit Kriterium 3.10(iii) ist $\varphi^{-1}(V) \subset G$ eine Untergruppe.

3. folgt aus 2.

4. und 5. als [Ü] □

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

Satz 4.8 *Es sei G eine Gruppe.*

1. 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.

2. Ist $p \in \mathbb{P}$, so gilt $\operatorname{ord}(G) = p$ genau dann, wenn G isomorph zu $(\mathbb{Z}_p, +, [0])$ ist.

Beweis. 1. "⇐": Die Gruppen $\mathbb{Z}$ und $\mathbb{Z}_m$ sind zyklisch nach Beispiel 3.15. Nach Satz 4.7.5 ist G zyklisch.

"⇒": Es sei G eine zyklische Gruppe und es sei $x \in G$ mit $G = \langle x \rangle$, also insbesondere $\mathrm{ord}(x) = \mathrm{ord}(G)$. Dann definiert

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

einen Epimorphismus 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: $\mathrm{ord}(G) = \infty$. 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 $\mathrm{ord}(G) = \mathrm{ord}(x) < \infty$ nach Satz 3.16.

2. Fall: $\mathrm{ord}(G) = m \in \mathbb{N}$. Nach Satz 3.16 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 $\mathrm{ord}(G) = m$ 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

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

2. "⇒": Ist $x \in G \setminus \{e\}$, so ist $\mathrm{ord}(x) > 1$ und nach dem Satz 3.19 von Lagrange $\mathrm{ord}(x) | \mathrm{ord}(G)$, also $\mathrm{ord}(x) = p = \mathrm{ord}(G)$. Damit ist $G = \langle x \rangle$ zyklisch, und folglich nach 1. isomorph zu $\mathbb{Z}_p$.

"⇐": ist klar. □

Beispiel 4.9 Für $m \in \mathbb{N}$ hat die zyklische Untergruppe $\langle \mathrm{e}^{2\pi \mathrm{i}/m} \rangle$ von $(\mathbb{C}^*, \cdot, 1)$ 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 $(\mathbb{Z}_m, +, 0)$.

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

Satz 4.10 *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

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

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

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

Die dadurch definierte Abbildung $\sigma_a : \{1, \ldots, n\} \to \{1, \ldots, n\}$ 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

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

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

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

und damit

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

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

Ist nun $a \in \operatorname{Kern} \varphi$, d.h. ist $\sigma_a = \mathrm{id}_{\{1,\ldots,n\}}$, so gilt $ax_j = x_{\sigma_a(j)} = x_j$ für $j \in \{1, \ldots, n\}$, und speziell für $x_j = e$ folgt $a = e$. Also ist φ nach Bemerkung/Definition 4.5 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 3.17 eingeführten Links- und Rechtsnebenklassen übereinstimmen:

Definition 4.11 Es seien G eine Gruppe und $U \subset G$ eine Untergruppe mit

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

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

$$U \quad \lhd \quad G.$$

Beispiele 4.12 1. Ist G abelsch, so ist jede Untergruppe $U \subset G$ Normalteiler von G.

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

3. Es seien $G = (S_3, \circ, \mathrm{id})$ und $U := \{\mathrm{id}, (1;2)\}$.[11] Dann ist U eine Untergruppe und hat nach dem Satz 3.19 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 ist U kein Normalteiler von G.

Bemerkung und Definition 4.13 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. Für $g \in G$ gilt

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

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

Also ist $U \lhd G$ genau dann, wenn $U^g = U$ für $g \in G$ gilt. Außerdem ist dies schon dann der Fall, wenn nur $U^g \subset U$ für $g \in G$ gilt ([Ü]).

Satz 4.14 *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. *$\mathrm{Kern}\,\varphi$ ist ein Normalteiler von G.*

[11] 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**.

Beweis. 1. Wir setzen $U := \varphi^{-1}(N)$. Dann ist $\varphi(U) \subset N$. Für $g \in G$ gilt mit (4.1) und (4.2)

$$\varphi(U^g) = \varphi\left(gUg^{-1}\right) = \varphi(g)\varphi(U)(\varphi(g))^{-1} \subset \varphi(g)N(\varphi(g))^{-1} = N^{\varphi(g)} = N$$

und damit

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

Also gilt $U \lhd G$ nach Bemerkung/Definition 4.13.

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

Beispiel 4.15 Es sei K ein Körper und $G := \mathrm{GL}_n(K)$ die allgemeine lineare Gruppe.

1. Nach Satz 4.14 ist die spezielle lineare Gruppe $\mathrm{SL}_n(K)$ ein Normalteiler von G.
2. Für $n = 2$ ist durch

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

ist ein Gruppenmorphismus $(K, +, 0) \ni t \mapsto B_t \in \mathrm{GL}_2(K)$ definiert, denn für $s, t \in K$ gilt $B_t \in \mathrm{GL}_2(K)$ und

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

Damit ist nach Satz 4.7.1

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

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

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 $\mathrm{GL}_2(K)$ nach Bemerkung/Definition 4.13.

Bemerkung und Definition 4.16 Ist $(G, \cdot)$ eine Halbgruppe, so ist nach Beispiel 1.4 auch $\mathrm{Pot}(G)$ mit dem Komplexprodukt eine Halbgruppe. Ist dabei $(G, \cdot, e)$ eine Gruppe 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

$$\pi_N(a) \;:=\; aN \quad \text{für } a \in G,$$

ein Halbgruppenmorphismus mit $\pi_N(e) = eN = N$ ist. Nach Satz 4.3 ist $(G/N, \cdot, N) = (\pi_N(G), \cdot, \pi_N(e))$ eine Gruppe, genannt **Faktorgruppe** oder **Quotientengruppe** von G nach N, und π_N ein surjektiver Gruppenmorphismus nach $(G/N, \cdot, N)$, der sogenannte **kanonische Morphismus**. Dabei ist $\mathrm{Kern}\,\pi_N = N$, denn für $a \in G$ gilt die Äquivalenzkette

$$a \in \mathrm{Kern}\,\pi_N \Leftrightarrow aN = N \Leftrightarrow a \in N.$$

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 4.14.2).

Beispiele 4.17 1. Es seien $G := (\mathbb{Z}, +, 0)$, $m \in \mathbb{N}$, und $N := m\mathbb{Z}$. Dann ist $\mathbb{Z}/(m\mathbb{Z}) = \mathbb{Z}_m$ und $\pi_{m\mathbb{Z}}(a) = a + m\mathbb{Z} = [a]_m$ für $a \in \mathbb{Z}$ sowie $\mathrm{Kern}\,\pi_{m\mathbb{Z}} = m\mathbb{Z}$; vgl. Beispiel 3.18 und Beispiel 4.4.1.

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

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

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

$$A_n \;:=\; \mathrm{Kern}\,\mathrm{sign} \;=\; \{\sigma \in S_n : \mathrm{sign}(\sigma) = 1\}$$

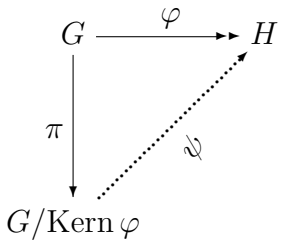
heißt n-te **alternierende Gruppe**[12]. Hier gilt, wie man sich leicht überlegt,

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

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

[12]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.

Der folgende Satz ist von zentraler Bedeutung für die Gruppentheorie.



Satz 4.18 *(Isomorphiesatz[13] 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_H das neutrale Element in H, so gilt für $a, b \in G$ die Äquivalenzkette

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

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

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

Also ist $\operatorname{Kern}\psi = \{N\}$ und damit ψ injektiv nach Bemerkung/Definition 4.5. □

Beispiele 4.19 1. Es seien $G := (\mathbb{R}^2, +, 0)$ und $H := (\mathbb{R}, +, 0)$. Dann ist durch

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

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

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

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

2. Es seien K ein Körper und $n \in \mathbb{N}$. Dann ist $\det : \mathrm{GL}_n(K) \to (K^*, \cdot, 1)$ ein surjektiver Morphismus mit Kern $\det = \mathrm{SL}_n(K)$. Also ist $\mathrm{GL}_n(K)/\mathrm{SL}_n(K)$ isomorph zu K^*.

3. In der Situation von Beispiel 4.17.2 ist S_n/A_n isomorph zu $(\{1, -1\}, \cdot, 1)$.

[13] Manchmal "erster Isomorphiesatz" genannt.

Bemerkung 4.20 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 $\mathbb{Z}/\mathrm{Kern}\,\varphi$.

Im Falle $\mathrm{ord}(H) = \infty$ ist $\mathrm{Kern}\,\varphi = \{0\}$ und im Falle $m := \mathrm{ord}(H) < \infty$ ist $\mathrm{Kern}\,\varphi = m\mathbb{Z}$ (siehe Satz 3.16). Damit ergibt sich wieder Satz 4.8 (beachte: $\mathbb{Z}_m = \mathbb{Z}/(m\mathbb{Z})$).

5 Diedergruppen und Gruppen kleiner Ordnung

Wir beschäftigen uns mit dem Zusammenspiel von Geometrie und Gruppentheorie.

Definition 5.1 Es sei (X, d) ein metrischer Raum und $f : X \to$ eine Selbstabbildung[14] 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. Im Falle der von der Euklidnorm $|\cdot|$ erzeugten euklischen Metrik auf $X = \mathbb{R}^m$ nennt man eine Isometrie auch **Bewegung** des $\mathbb{R}^m$.

Bemerkung 5.2 Es sei (X, d) ein metrischer Raum. Man sieht leicht:

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.

Bemerkung 5.3 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 $\mathrm{GL}_m(\mathbb{R})$ ([Ü]), genannt **orthogonale Gruppe** des $\mathbb{R}^m$. Für $A \in \mathrm{O}_m$ und $b \in \mathbb{R}^m$ definiert dann

$$T(x) \;=\; Ax + b \quad \text{für } x \in \mathbb{R}^m \tag{5.1}$$

eine Bewegung des $\mathbb{R}^m$, 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[15], dass jede Bewegung des $\mathbb{R}^m$ von der Form (5.1) ist; wir behandeln unten in Satz 5.4 den Spezialfall $m = 2$. Bewegungen des $\mathbb{R}^m$ sind stets surjektiv, was sich aus der Invertierbarkeit von A in der Darstellung (5.1) ergibt.

Satz 5.4 *Eine Selbstabbildung $T : \mathbb{C} \to$ ist genau dann isometrisch bezüglich der Betragsmetrik auf $\mathbb{C}$, wenn $\theta \in \mathbb{R}$ und $b \in \mathbb{C}$ existieren mit*

$$T(z) \;=\; \mathrm{e}^{\mathrm{i}\theta} z + b \quad \textit{für } z \in \mathbb{C}$$

oder

$$T(z) \;=\; \mathrm{e}^{\mathrm{i}\theta} \overline{z} + b \quad \textit{für } z \in \mathbb{C}.$$

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

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

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 $T : \mathbb{C} \xrightarrow{\sim}$ 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

$$x^2+y^2 \;=\; |z-0|^2 \;=\; \Big|S(z)-S(0)\Big|^2 \;=\; u^2+v^2 \tag{5.2}$$

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 (5.2) 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.

Wegen $|T(1)-T(0)| = 1$ ist $T(1)-T(0) = \mathrm{e}^{\mathrm{i}\theta}$ für ein $\theta \in \mathbb{R}$. Mit $b := T(0)$ ergibt sich die Behauptung. □

Bemerkung und Definition 5.5 1. Es seien $m \in \mathbb{N}$ und $F \subset \mathbb{R}^m$. Eine Bewegung $T : \mathbb{R}^m \xrightarrow{\sim}$ 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.

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

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

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

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

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

$$\tau \circ \sigma = \sigma \circ \tau^{-1}.$$

Satz 5.6 *Es gilt*

1. $\mathrm{D}_n = \langle\{\tau, \sigma\}\rangle = \langle\tau\rangle \cup \langle\tau\rangle\,\sigma \Big(= \{\tau^k \circ \sigma^j : k = 0, \ldots, n-1,\ j = 0, 1\}\Big)$.
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.*

Beweis.

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

Es sei $T \in \mathrm{D}_n$. Nach Satz 5.4 ist T von der Form $T = a \cdot \mathrm{id}_{\mathbb{C}} + b$ oder $T = a \cdot \sigma + b$ mit $a, b \in \mathbb{C}$, $|a| = 1$. Ist n gerade, so gilt $\pm 1 \in R_n$ und damit $T(\pm 1) \in R_n$, also $|T(\pm 1)| \leq 1$. Außerdem ist

$$|T(\pm 1)|^2 = |b \pm a|^2 = 1 + |b|^2 \pm 2\mathrm{Re}(ab),$$

also $|T(1)|^2 \geq 1 + |b|^2$ oder $|T(-1)|^2 \geq 1 + |b|^2$. Damit ist $b = 0$. Ist n ungerade, so ergibt sich ebenfalls $b = 0$ durch eine kleine Zusatzüberlegung; [Ü].

Aus $b = 0$ folgt $|T(z)| = |z|$ für alle z. Mit $V_n = R_n \cap \{|w| = 1\}$ ergibt sich

$$T(V_n) \;=\; V_n, \tag{5.3}$$

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

2. Wegen $\sigma \notin \langle\tau\rangle$ folgt 2. aus dem Satz von Lagrange (S. 3.19).

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 5.7 *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*

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

erzeugt wird.

Beweis. Wie in Satz 5.6 gesehen, ist D_n eine solche Gruppe, mit $a = \sigma$ und $b = \tau$.

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

$$(b^k a^j)^{-1} b^m a^\ell = a^{-j} b^{m-k} a^\ell = \begin{cases} b^{m-k} a^\ell & \text{falls } j \text{ gerade} \\ b^{k-m} a^{\ell+1} & \text{falls } j \text{ gerade} \end{cases}, \tag{5.4}$$

denn für gerade j ist $a^{-j} = e$, und für ungerade j ist $a^{-j} = a$ und mit $k - m = qn + r$ (Division mit Rest) gilt

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

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

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

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

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

eine surjektive Abbildung $\varphi : \mathrm{D}_n \to G$ (wohl-)definiert. Wegen $\#G = 2n = \#\mathrm{D}_n$ ist φ dann auch schon bijketiv. Aus $\mathrm{ord}(\tau) = n = \mathrm{ord}(b)$ und $\mathrm{ord}(\sigma) = 2 = \mathrm{ord}(a)$ folgt

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

und mit (5.4) für D_n und für G ergibt sich für $j, k, \ell, m \in \mathbb{Z}$ mit j gerade beziehungsweise ungerade

$$\varphi\Big((\tau^k \circ \sigma^j)^{-1} \circ \tau^m \circ \sigma^\ell\Big) = \left\{ \begin{array}{ccc} \varphi(\tau^{m-k} \circ \sigma^\ell) & = & b^{m-k} a^\ell \\ \varphi(\tau^{k-m} \circ \sigma^{\ell+1}) & = & b^{k-m} a^{\ell+1} \end{array} \right\} = \varphi(\tau^k \circ \sigma^j)^{-1} \varphi(\tau^m \circ \sigma^\ell).$$

Damit ist φ auch ein Gruppenmorphismus ([Ü]) und folglich sind D_n und G isomorph. □

Ein anderer Struktursatz ist:

Satz 5.8 *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 $a \in G$ ist $a^2 = e$, also folgt für $x, y \in G$

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

Es sei nun G endlich. Dann existiert

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

Wir wählen $M \subset G$ mit $\#M = m$ und $\langle M\rangle = G$ (also ein minimales Erzeugendensystem von G). Nach Satz 3.13.2 ist

$$G \;=\; \left\{\prod_{a\in M} a^{k_a} :\, (k_a) \in \mathbb{Z}^M\right\} \;=\; \left\{\prod_{a\in F} a : F \subset M\right\}, \tag{5.5}$$

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 $a' \in F' \setminus F$

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

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

Mit (5.5) folgt $\#G = \#\{F : F \subset M\} = 2^m$. □

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

Satz 5.9 [16] *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.*

[16] In einer etwas ausführlicheren und systematischeren Darstellung der elementaren Gruppentheorie erhält man Satz 5.9 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.

Beweis. Der "entweder"-Teil der Behauptung ergibt sich aus der Azyklizität der Diedergruppen; siehe Satz 5.6.

Nach Bemerkung 3.20 gilt $\operatorname{ord}(x) \in \{2, p, 2p\}$ 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 4.8 isomorph zu $(\mathbb{Z}_{2p}, +)$.

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

Ist $p = 2$, so gilt $\operatorname{ord}(x) = 2$ für $x \in G \setminus \{e\}$, also ist G abelsch nach Satz 5.8. Für beliebig gewählte $a, b \in G \setminus \{e\}$ mit $a \neq b$ gilt dann $ab \neq e$ wegen $b = b^{-1} \neq a^{-1}$ sowie $ab \notin \{a, b\}$ und

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

Wegen $\operatorname{ord}(G) = 4$ ist also

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

und folglich G isomorph zu D_2 nach Satz 5.7.

Es sei also $p \geq 3$. Dann ist $\operatorname{ord}(G) = 2p$ keine Zweierpotenz, also existiert nach Satz 5.8 ein $b \in G$ mit $\operatorname{ord}(b) > 2$, also $\operatorname{ord}(b) = p$. Weiter existiert wegen $\operatorname{ord}(G)$ gerade auch ein $a \in G$ mit $\operatorname{ord}(a) = 2$ ([Ü]). Dabei gilt $a \notin \langle b \rangle$ nach Bemerkung 3.20, da $\operatorname{ord}(a) = 2$ kein Teiler von $p = \#\langle b \rangle$ ist. Mit $U := \langle b \rangle$ folgt $U \cap Ua = \emptyset$ und $U \cap aU = \emptyset$, wegen $\operatorname{ord}(G) = 2p$ und $\operatorname{ord}(U) = p$ also

$$G \;=\; U \cup aU \quad \text{und} \quad G \;=\; U \cup Ua.$$

Insbesondere ist $G = \langle \{a, b\} \rangle$ und $aU = Ua$, d. h. $U \lhd G$ und folglich, under Verwendung von $a^2 = e$ im ersten Schritt und Bemerkung 4.13 im zweiten

$$aUa \;=\; aUa^{-1} \;=\; U.$$

Also existiert ein $k \in \{0, \ldots, p-1\}$ mit $ab^k a = b$. Wegen $a^2 = e$ ergibt sich

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

und folglich, wieder 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 3.16. 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 $a^2 = e$)

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

im Widerspruch zu $\operatorname{ord}(ab) \in \{1, 2, p\}$.

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

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

Wiederum mit Satz 5.7 folgt nun, dass G isomorph zu D_p ist. □

Satz 5.10 *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 4.8, der zweite nach Satz 5.9 mit $p \in \{2, 3\}$. Der Zusatz ist klar wegen der Kommutativität von D_2 nach Satz 5.6. □

6 Polynomringe und Körpererweiterungen

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

Definition 6.1 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 $(R^*, \cdot, 1)$, so heißt U **Unterkörper** (oder **Teilkörper**) von R.

Bemerkung 6.2 Es sei $R = (R, +, \cdot)$ ein Ring und es sei $U \subset R$.

1. Nach Kriterium 3.10(iii) ist $U \neq \emptyset$ Untergruppe von $(R, +, 0)$ genau dann, wenn $U - U \subset U$. Damit gilt dies in allen Fällen in Definition 6.1.

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 3.12 analoge Argumentation erhält man mit Bemerkung 6.2 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 6.3 Es seien R ein Ring und $M \subset R$. Dann heißen

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

von M **erzeugter Unterring** und

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

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

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

von M **erzeugter Unterkörper**.

Bemerkung und Definition 6.4 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 heißen φ ein **(Ring-)morphismus** von R nach S und $\mathrm{Kern}(\varphi) := \varphi^{-1}(\{0_S\})$ der **Kern** von φ.

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 $R \simeq S$. Nach Bemerkung/Definition 4.5 ist ein Morphismus φ genau dann ein Monomorphismus, wenn $\mathrm{Kern}(\varphi) = \{0\}$ gilt. Weiter sieht leicht: Verkettungen von Morphismen bzw. Monomorphismen bzw. Isomorphismen sind wieder solche. Inverse von Isomorphismen sind Isomorphismen.

Beispiel 6.5 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 6.6 Für Ringmorphismen $\varphi : R \to S$ gelten zum Gruppenfall analoge Aussagen ([Ü]):

- 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 im Falle $S \neq \{0_S\}$ kein Unterring (da $0_S \neq 1_S = \varphi(1_R)$ und damit $1 \notin \mathrm{Kern}(\varphi)$).
- Ist $U \subset R$ ein Unterring, so ist $\varphi(U) \subset S$ ein Unterring.
- Ist I ein Ideal in R, so ist $\varphi(I)$ ein Ideal in $\varphi(R)$ (aber nicht stets in S).

Bemerkung 6.7 Es seien K ein Körper und $S \neq \{0_S\}$ ein Ring. Ist $\varphi : K \to S$ ein Ringmorphismus, so ist φ schon injektiv, also eine Einbettung.

Denn: Wäre φ nicht injektiv, so existierte ein $x \in K^*$ mit $\varphi(x) = 0$, also

$$1_S = \varphi(1_K) \;=\; \varphi(xx^{-1}) \;=\; \varphi(x)\varphi(x^{-1}) \;=\; 0_S,$$

Widerspruch. Damit ist φ injektiv.

Außerdem ist $\varphi(K)$ nach Satz 4.3 ein Körper und es gilt $\varphi(x/y) = \varphi(x)/\varphi(y)$ für $x, y \in K$ mit $y \neq 0$.

Bemerkung und Definition 6.8 Sind R ein kommutativer Ring, $U \subset R$ ein Unterring und $x \in R$, so gilt

$$U[x] \;:=\; \langle U \cup \{x\}\rangle_{\text{Ring}} = \left\{ \sum_{j\in\mathbb{N}_0} a_j x^j : (a_j) \in U^{(\mathbb{N}_0)} \right\}.$$

Denn: Einerseits rechnet man nach, dass die rechte Seite ein Unterring ist, der U und x enthält (beachte: $x^0 = 1$ und $x^{j+k} = x^j x^k$). Andererseits enthält jeder Unterring, der U und x enthält, auch notwendigerweise die rechte Seite.

Entsprechend sieht man: Sind K ein Körper, $U \subset K$ ein Unterring und $x \in K$, so gilt

$$U(x) \;:=\; \langle U \cup \{x\}\rangle_{\text{Körper}} = \left\{ \frac{\sum\limits_{j\in\mathbb{N}_0} a_j x^j}{\sum\limits_{k\in\mathbb{N}_0} b_k x^k} : (a_j), (b_k) \in U^{(\mathbb{N}_0)}, \sum_{k\in\mathbb{N}_0} b_k x^k \neq 0 \right\}.$$

Damit heißt $U[x]$ der durch **adjungieren** von x zu U **im Ring-Sinne** entstandene Unterring, kurz gelesen als "U adjungiert x". Entsprechend heißt $U(x)$ **im Körper-Sinne** entstandener Unterkörper.

Beispiel 6.9 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 $j \in \mathbb{Z}$

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

Bemerkung 6.10 Es sei R ein Ring. 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 Ring mit der Nullfunktion als Nullelement und Einselement 1_{R^M}, definiert durch $1_{R^M}(x) := 1_R$ für $x \in M$. Ist R kommutativ, so ist auch R^M kommutativ. Weiter setzen wir noch $(\lambda f)(x) := \lambda f(x)$ für $\lambda \in R$ und $f \in R^M$.

Bemerkung 6.11 Wir betrachten nun einen kommutativen Ring R und den Fall $M = \mathbb{N}_0$. Anders als in Bemerkung 6.10 definieren für $(a_j), (b_j) \in R^{\mathbb{N}_0}$

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

Dabei heißt (c_j) **Faltung** oder auch **Cauchy-Produkt** [17] von (a_j) und (b_j). Mit der Addition aus Definition 6.10 und obiger Multiplikation ist $(R^{\mathbb{N}_0}, +, \cdot)$ ein kommutativer Ring mit 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

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

Für $(a_j) \in R^{(\mathbb{N}_0)}$ und jedes $n \in \mathbb{N}_0$ mit $a_j = 0$ für $j > n$ ergibt sich damit

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

Weiter ist

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

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

Definition 6.12 In der Situation aus Bemerkung 6.11 heißt

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

Polynomring über R in der **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** der Polynomfunktion oder **Wurzel** des Polynoms P.

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

Bemerkung 6.13 Für $(a_j), (b_j) \in R^{(\mathbb{N}_0)}$ und $n, m \in \mathbb{N}_0$ mit $a_j = 0$ für $j > n$ sowie $b_j = 0$ für $j > m$ gilt

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

Beispiel 6.14 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 und Definition 6.15 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 Bemerkung/Definition 6.8 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 gilt $X^0(x) = x^0 = 1_R$ und für $P = \sum_{j=1}^{n} a_j X^j$, $Q = \sum_{j=1}^{m} b_j X^j \in R[X]$

$$\begin{aligned} \Big(P + Q\Big)(x) &= \left(\sum_{j=0}^{m \vee n} (a_j + b_j) X^j \right)(x) \\ &= \sum_{j=0}^{m \vee n} (a_j + b_j) x^j = \sum_{j=0}^{n} a_j x^j + \sum_{j=0}^{m} b_j x^j = P(x) + Q(x) \end{aligned}$$

sowie

$$\Big(PQ\Big)(x) = \left(\sum_{j=0}^{n+m} \left(\sum_{k=0}^{j} a_k b_{j-k} \right) X^j \right)(x) = \sum_{j=0}^{n+m} \left(\sum_{k=0}^{j} a_k b_{j-k} \right) x^j = P(x)Q(x)\,.$$

3. Die Funktion

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

ist ein Ringmorphismus, der im Allgemeinen nicht injektiv ist (etwa nach Beispiel 6.14).

Definition 6.16 Es seien R ein kommutativer Ring und $P = \sum_{j=0}^{n} a_j X^j \in R[X]$. Dann heißt (mit $\max \emptyset := -\infty$)

$$\deg P := \max\{j \in \mathbb{N}_0 : a_j \neq 0\} \in \mathbb{N}_0 \cup \{-\infty\}$$

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 6.17 Es sei R ein kommutativer Ring. Dann gilt[18] 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 ([Ü])

$$\deg(PQ) = \deg P + \deg Q.$$

Satz 6.18 (Division mit Rest) *Es sei K ein Körper und es seien $P, S \in K[X]$ mit $S \neq 0$. Dann existiert genau ein Polynompaar (Q, R) in $K[X] \times K[X]$ mit $\deg R < \deg S$ und*

$$P = Q \cdot S + R.$$

Beweis. 1. Existenz: 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

$$P = \sum_{j=0}^{n} a_j X^j, \quad S = \sum_{j=0}^{m} b_j X^j \in K[X]$$

[18] Man setzt natürlich $-\infty \leq a$ und $(-\infty) + a = a + (-\infty) := -\infty$ für $a \in \{-\infty\} \cup \mathbb{N}_0$, oder auch allgemeiner für $a \in [-\infty, \infty[$.

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 $\deg C < n$. Ist dabei sogar $\deg C < m$, so können wir $Q := (a_n/b_m)X^{n-m}$ und $R := C$ setzen. Ist dagegen $\deg C \geq m$, so liefert die Induktionsvoraussetzung (mit C statt P) Polynome $\widetilde{Q}, R \in K[X]$ mit $\deg R < \deg S$ und

$$C \;=\; \widetilde{Q}S + R,$$

mit $Q := \widetilde{Q} + (a_n/b_m)X^{n-m}$ also

$$P \;=\; C + \frac{a_n}{b_m} X^{n-m} S \;=\; QS + R.$$

2. Eindeutigkeit: [Ü]. □

Satz 6.19 *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. Es sei $S := X - a$. Wegen $\deg S = 1$ existiert nach Satz 6.18 genau ein Paar (Q, R) in $K[X] \times K[X]$ mit $P = SQ + R$ und $\deg R < 1$, also $R = r_0$ mit einem $r_0 \in K$. Mit Bemerkung 6.15.2 folgt

$$0 \;=\; P(a) \;=\; S(a)Q(a) + R(a) \;=\; r_0\,.$$

Damit ist $R = 0$. Außerdem gilt $\deg(P) = \deg(SQ) = \deg(S) + \deg(Q) = 1 + \deg(Q)$, unter Verwendung von Bemerkung 6.17 im zweiten Schritt.

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 6.20 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

$$[E : K] \quad := \quad \dim_K(E),$$

kurz gelesen als „Grad von E über K“. Die Erweiterung heißt **endlich** falls $[E : K]$ endlich ist.

Beispiele 6.21 [19]

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

$$\mathrm{span}_{\mathbb{Q}}(M) = \left\{ \sum_{x \in M} \lambda_x \cdot x : (\lambda_x) \in \mathbb{Q}^M \right\}$$

abzählbar, also $\neq \mathbb{R}$.

Satz 6.22 *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*

$$[F : E][E : K] \quad = \quad [F : K].$$

Beweis. Es sei B eine Basis von E als K-Vektorraum und C eine Basis von F als E-Vektorraum. Dann ist die Funktion $B \times C \ni (x, y) \mapsto xy \in F$ injektiv, denn sind $(x, y), (x', y') \in B \times C$, so folgt aus $xy = x'y'$, also $xy - x'y' = 0$, wegen $x, x' \neq 0$ und der E-linearen Unabhängigkeit von $(y)_{y \in C}$ schon $y = y'$ und dann auch $x - x' = 0$.

Ist $z \in F$, so existieren Skalare $\mu_y \in E$ mit $z = \sum\limits_{y \in C} \mu_y y$. Weiter existieren zu jeden $y \in C$ Skalare $\lambda_{x,y} \in K$ mit $\mu_y = \sum\limits_{x \in B} \lambda_{x,y} x$. Also ist

$$z \quad = \quad \sum_{y \in C} \Big(\sum_{x \in B} \lambda_{x,y} x \Big) y \quad = \quad \sum_{y \in C} \sum_{x \in B} \lambda_{x,y} xy \,. \tag{6.1}$$

Damit ist BC ein Erzeugendensystem von F als K-Vektorraum.

Hat $z = 0$ die Darstellung (6.1), so folgt wegen der E-linearen Unabhängigkeit von $(y)_{y \in C}$ zunächst $\sum\limits_{x \in B} \lambda_{x,y} x = 0$ für $y \in C$, und mit der K-linearen Unabhängigkeit

[19] 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. Damit heißt M Erzeugendensystem von V, falls $\mathrm{span}(M) = V$ gilt und Basis von V, falls zusätzlich die Familie $(x)_{x \in M}$ linear unabhängig ist.

von $(x)_{x\in B}$ dann $\lambda_{x,y} = 0$ für $x \in B$, $y \in C$. Damit ist BC eine Basis von F als K-Vektorraum und folglich

$$[F : K] \;=\; \#(BC) \;=\; \#(B \times C) \;=\; \#B \cdot \#C \;=\; [E : K][F : E].$$

□

Definition 6.23 Es seien E eine Körpererweiterung von K und $x \in E$. Dann heißt x **algebraisch** über K, falls x Wurzel eines Polynoms $P \in K[X] \setminus \{0\}$ ist. 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 6.24

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 $x = a + \mathrm{i}b \in \mathbb{C}$ mit $a, b \in \mathbb{R}$ und

$$P \;:=\; (X - a)^2 + b^2 \;\in\; \mathbb{R}[X].$$

gilt $P(x) = (x - a)^2 + b^2 = (\mathrm{i}b)^2 + b^2 = 0$ mit Bemerkung 6.15.2.

4. Es sei $\mathbb{A}$ die Menge der reellen und über $\mathbb{Q}$ algebraischen Zahlen. Da $\mathbb{Q}[X]$ abzählbar ist und jedes Polynom $P \in \mathbb{Q}[X]\setminus\{0\}$ 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 6.25 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.

2. Aus der Definition der Transzendenz ergibt sich unmittelbar, dass für $x \in E$ 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).

3. 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 nach 2. algebraisch über K. Damit ist E algebraisch über K.

Satz 6.26 *Es seien E eine Körpererweiterung von K und $x \in E$.*

1. *Ist x algebraisch über K, so gibt es genau ein normiertes Polynom $P_x \in K[X]$ minimalen Grades mit $P_x(x) = 0$. Außerdem ist $\{x^j : j = 0, \ldots, \deg(P_x) - 1\}$ eine Basis des K-Vektorraumes $K[x]$.*

2. *Genau dann ist x algabraisch über K, wenn $K[x]$ ein Unterkörper von E ist, also $K[x] = K(x)$ gilt.*

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 $a_n = 1$. Ist $Q \in K[X]$ ebenfalls normiert mit $\deg Q = n$ und $Q(x) = 0$, so ist $\deg(P_x - Q) < n$ und $(P_x - Q)(x) = 0$. Nach Definition von n ist $P_x - Q = 0$. Also existiert P_x eindeutig, wie behauptet.

Es sei $\varphi_x : K[X] \to E$ der Auswertungsmorphismus und es sei

$$K_{<n}[X] \;:=\; \{S \in K[X] : \deg S < n\}.$$

Aus der Definition von n 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 $Q, R \in K[X]$ und $\deg R < \deg P_x$ nach Satz 6.18, 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 $K[x]$.

2. $\Leftarrow$: Ist $x = 0$, so ist x algebraisch über K. Es sei also $x \neq 0$. Dann ist $1/x \in K[x]$. Nach Bemerkung 6.25.1 gibt es ein $P \in K[X]$ mit $1/x = P(x)$. Also ist x Wurzel von $Q := 1 - X \cdot P \in K[X] \setminus \{0\}$ 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 $0 \neq y \in K[x]$, so ist $y^j \in K[x]$ für alle $j \in \mathbb{N}_0$ und damit y nach 1. und Bemerkung 6.25.2 algebraisch über K. Also existiert nach Bemerkung 6.25.1 ein $P \in K[X] \setminus \{0\}$ mit $P(y) = 0$, $P = \sum_{j=r}^{d} a_j X^j$ mit $r, d \in \mathbb{N}_0$, $r \leq d$, $a_r \neq 0$. 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 $1/y = \sum_{j=r+1}^{d} (-a_j/a_r) y^{j-r-1} \in K[y] \subset K[x]$. □

Bemerkung 6.27 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 6.26 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 6.22.

Definition 6.28 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.

Bemerkung und Definition 6.29 Ist E eine Körpererweiterung von K und ist $x \in E$ algebraisch über K, so heißt das Polynom P_x aus Satz 6.26 das **Minimalpolynom** von x über K, und x heißt vom **Grad** $\deg P_x$ über K. Jedes Polynom $P \in K[X]$ mit $P(x) = 0$ ist Vielfaches von P_x.

Denn: Es sei $P \in K[X]$ mit $P(x) = 0$. Nach Satz 6.18 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 $\deg P_x$ folgt wieder $R = 0$ und damit $P = QP_x$.

Weiter gilt mit Satz 6.26 und Bemerkung 6.25.3

- $K[x]$ ist eine Körpererweiterung von K vom Grad $[K[x] : K] = \deg P_x$.
- $K[x]$ ist algebraisch über K.

Beispiel 6.30 1. Es sei E ein Erweiterung von K. Aus der Definition ergibt sich sofort: $x \in E$ ist genau dann vom Grad 1 über K, wenn $x \in K$ gilt, und dann ist $X - x \in K[X]$ das Minimalpolynom.

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 6.26 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 $\mathbb{R}$.

3. Das Minimalpolynom von i über $\mathbb{R}$ (und über $\mathbb{Q}$) 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 $\mathbb{R}$ (und über $\mathbb{Q}$). Mit Beispiel 6.24.3 folgt analog: Jedes $x \in \mathbb{C} \setminus \mathbb{R}$ ist vom Grad 2 über $\mathbb{R}$.

Mithilfe des nächsten Resultats kann man manchmal entscheiden, ob ein gegebenes Polynom ein Minimalpolynom ist. Ein nichtkonstantes Polynom $P \in K[X]$ heißt **irreduzibel** (über K) wenn gilt: Ist $P = QS$ mit $Q, S \in K[X]$, so ist Q konstant oder S konstant.

Satz 6.31 *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 $S(x) = 0$. Ohne Einschränkung sei $Q(x) = 0$. Wegen der Minimalität des Grades von P_x ist dann $\deg Q = \deg P_x$ und wegen $\deg Q + \deg S = \deg P_x$ dann $\deg S = 0$.

(ii) $\Rightarrow$ (i): Nach Bemerkung 6.29 existiert ein $Q \in K[X]$ mit $P = QP_x$. Aufgrund der Irreduzibilität von P ist Q konstant, also $Q = 1$ wegen der Normiertheit von P_x und P. □

Ist E eine Körpererweiterung von K, so schreiben wir $A_E(K)$ für die Menge der über K algebraischen Elemente in E. Dann gilt $K \subset A_E(K)$ nach Beispiel 6.24.1. Wir zeigen abschließend

Satz 6.32 *Ist E eine Körpererweiterung von K, so ist $A_E(K)$ ein Unterkörper von E.*

Beweis. Wir schreiben kurz $A := A_E(K)$. Es reicht zu zeigen: Sind $x, y \in A$, so gilt $x - y, xy \in A$ und, falls $x \neq 0$, auch $1/x \in A$.

Es seien also $x, y \in A$. Ist $x \neq 0$, so gilt, wegen $x \in K[x]$ und da $K[x]$ nach Satz 6.26.2. ein Körper ist, auch auch $1/x \in K[x]$, also $1/x \in A$ nach Bemerkung 6.29. Wir setzen $m := \deg(P_x) - 1$ und $n := \deg(P_y) - 1$. Sind $M, N \in \mathbb{N}_0$, so existieren nach Satz 6.26.1 Skalare $a_\mu, b_\nu \in K$ 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 von

$$U := \operatorname{span}_K \{x^N y^M : M, N \in \mathbb{N}_0\}$$

und damit $\dim_K U \leq (m+1)(n+1) < \infty$. Wegen $(xy)^j \in U$ und $(x-y)^j \in U$ für alle $j \in \mathbb{N}_0$ (binomische Formel!) sind $((xy)^j)_{j \in \mathbb{N}_0}$ und $((x-y)^j)_{j \in \mathbb{N}_0}$ linear abhängig. Mit Bemerkung 6.25.2 folgt $x - y, xy \in A$. □

7 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[20]. 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 $0 < r < \infty$

$$\begin{aligned} g_{P,Q} &:= \{tP + (1-t)Q : t \in \mathbb{R}\}, && \textbf{Gerade} \text{ durch } P \text{ und } Q, \\ k_{P,r} &:= \{P + re^{it} : t \in \mathbb{R}\}, && \textbf{Kreis(linie)} \text{ um } P \text{ mit Radius } r. \end{aligned}$$

Bemerkung und Definition 7.1 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

$$M_n := \{P \in \mathbb{R}^2 : P \text{ direkt konstruierbar aus } M_{n-1}\} \qquad (n \in \mathbb{N}).$$

Dann ist $M_{n-1} \subset M_n$ für $n \in \mathbb{N}$. Ein Punkt $P \in \mathbb{R}^2$ heißt **konstruierbar** (mit Zirkel und Lineal) aus M falls ein n existiert mit $P \in M_n$.

2. Es sei $\{0, 1\} \subset M \subset \mathbb{R}$. 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. Wir setzen

$$\mathrm{kon}(M) := \{x \in \mathbb{R} : x \text{ konstruierbar aus } M\}.$$

Damit ist $M \subset \mathrm{kon}(M) = \mathrm{kon}(\mathrm{kon}(M))$. Weiter kann sich überlegen ([Ü]):

[20] 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

1. Mit $x, y \in \mathrm{kon}(M)$ sind auch $x+y \in \mathrm{kon}(M)$ und $-x \in \mathrm{kon}(M)$ (also ist $\mathrm{kon}(M)$ eine Untergruppe von $(\mathbb{R}, +, 0)$).

2. $(x, y) \in \mathbb{R}^2$ ist konstruierbar aus $M \times \{0\}$ genau dann, wenn $\{x, y\} \subset \mathrm{kon}(M)$ gilt.

Satz 7.2 *Es sei* $\{0, 1\} \subset M \subset \mathbb{R}$. *Dann ist* $\mathrm{kon}(M)$ *ein Unterkörper von* $\mathbb{R}$ *und mit* $0 \leq x \in \mathrm{kon}(M)$ *ist auch* $\sqrt{x} \in \mathrm{kon}(M)$.

Beweis. Es sei $K := \mathrm{kon}(M)$. Nach Bemerkung/Definition 7.1 ist noch zu zeigen: Sind $x, y \in K$ mit $x > 0$, so sind xy, $1/x$, $\sqrt{x} \in K$. Die drei Eigenschaften ergeben sich mit Bemerkung/Definition 7.1 durch geeignete Konstruktionen, die in der Vorlesung genauer erläutert werden. Für die erste Aussage verwendet man einen passenden Strahlensatz und für die zweite den Höhensatz von Euklid. □

Bemerkung 7.3 Jeder Unterkörper von $\mathbb{R}$ enthält schon $\mathbb{Q}$. In Satz 7.2 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 $\mathrm{kon}(M) = \mathrm{kon}(\mathbb{Q})$.

Bemerkung 7.4 1. 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 $E = K + Ka$.

> Denn: Es sei $x \in E \setminus K$. Dann ist $\{1, x\}$ eine Basis des K-Vektorraumes E, nach Satz 6.26 oder auch einfach wegen der linearen Unabhängigkeit von $(1, x)$ über K. Also existieren $p, q \in K$ mit $x^2 + px + q = 0$, also, $1 + 1 \neq 0$ ausnutzend,
>
> $$\left(x + \frac{p}{2}\right)^2 \;=\; \frac{p^2}{2^2} - q \;\in\; K.$$
>
> Mit $a := x + p/2$ gilt also $a^2 \in K$ und $a \in E \setminus K$, also ist $(1, a)$ linear unabhängig und damit eine Basis von E.

2. Es seien $K \subset \mathbb{R}$ ein Körper und $x \in \mathbb{R}$ vom Grad 2 über K. Mit $E := K(x)$ und a wie in 1. ist $x \in K + Ka$ und $K + Ka \subset K(\sqrt{a^2}) \subset \mathrm{kon}(K)$ nach Satz 7.2, also $x \in \mathrm{kon}(K)$.

Wir setzen für einen Unterkörper U von $\mathbb{R}$ und $x_0, \ldots, x_n \in \mathbb{R}$

$$U(x_0, \ldots, x_j) := \Big(U(x_0, \ldots, x_{j-1})\Big)(x_j) \qquad (j = 1, \ldots, n).$$

Satz 7.5 *Es seien K ein Unterkörper von $\mathbb{R}$ und $x \in \mathbb{R}$. Mit $\delta_0 := 1$ ist $x \in \mathrm{kon}(K)$ genau dann, wenn ein $n \in \mathbb{N}$ und $\delta_1, \ldots, \delta_n \geq 0$ existieren mit $\delta_j \in K(\sqrt{\delta_0}, \ldots, \sqrt{\delta_{j-1}})$ für $j = 1, \ldots, n$ und $x \in K(\sqrt{\delta_0}, \ldots, \sqrt{\delta_n})$.*

Beweis.

$\Rightarrow$: Es genügt, zu 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 $\delta \geq 0$. Mehrfache Anwendung, startend mit $U = K = K(1)$, ergibt dann die Behauptung.

Wir beweisen die Aussage 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

$$ax + by + c \;=\; 0 \tag{7.1}$$

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

$$(x - d)^2 + (y - e)^2 \;=\; f \tag{7.2}$$

mit $d, e, f \in U$ und $f \neq 0$ beschreibbar. Auflösen von (7.1), o.E. nach y, und Einsetzen in (7.2) 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 (7.1) ist dann auch $y \in U(\sqrt{\delta})$.

(kk): Zwei Kreisgleichungen sind durch Subtraktion auf den Fall (gk) zurückführbar.

$\Leftarrow$: Es seien $j \in \{1, \ldots, n\}$ und $K_j := K(\sqrt{\delta_0}, \ldots, \sqrt{\delta_j})$. Mit $K_0 := K$ ist $\delta_j \in K_{j-1}$ und nach Satz 7.2 damit $\sqrt{\delta_j} \in \mathrm{kon}(K_{j-1})$ und dann auch

$$K_j = K_{j-1}(\sqrt{\delta_j}) \subset \mathrm{kon}(K_{j-1}).$$

Induktiv ergibt sich $K_n \subset \mathrm{kon}(K)$ und damit $x \in \mathrm{kon}(K)$. □

Satz 7.6 *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 seien $K_j := K(\sqrt{\delta_0}, \ldots, \sqrt{\delta_j})$ wie in Satz 7.5. Dann ist entweder $\sqrt{\delta_j} \in K_{j-1}$ und dann $K_j = K_{j-1}$ oder $\sqrt{\delta_j} \notin K_{j-1}$ und dann $\sqrt{\delta_j}$ als Wurzel von $X^2 - \delta_j \in K_{j-1}[X]$ algebraisch vom Grad 2 über K_{j-1} und damit $K_j = K_{j-1}(\sqrt{\delta_j})$ nach Satz 6.26 ein Unterkörper von $\mathbb{R}$ vom Grad 2 über K_{j-1}. Also ist $[K_j : K_{j-1}] \in \{1, 2\}$ und damit nach Satz 6.22

$$[K_n : K] \;=\; [K_n : K_{n-1}][K_{n-1} : K] \;=\; \ldots \;=\; \prod_{j=1}^{n} [K_j : K_{j-1}]$$

eine Zweierpotenz. Nach Satz 6.26 und Bemerkung 6.27, angewandt auf $E := K_n$, ist $\deg P_x = [K[x] : K]$ ein Teiler von $[K_n : K]$, also $\deg P_x = 2^m$ für ein $m \in \mathbb{N}_0$. □

Bemerkung 7.7 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]). Durch Anwendung auf $P = X^3 - a$ ergibt sich: Für $a \in \mathbb{N}$ ist entweder $\sqrt[3]{a} \notin \mathbb{Q}$ oder $\sqrt[3]{a} \in \mathbb{N}$.

2. Es seien K ein Körper und $P \in K[X]$ mit $\deg P \in \{2, 3\}$. Dann gilt ([Ü]): P ist reduzibel genau dann, wenn P eine Wurzel in K hat. Mit 1. ergibt sich (wieder [Ü]): Für $a \in \mathbb{N}$ ist entweder $\sqrt[3]{a} \in \mathbb{N}$ oder $\sqrt[3]{a}$ vom Grad 3 über $\mathbb{Q}$.

Bemerkung 7.8 (Unlösbarkeit des Delischen Problems)
Es ist $\sqrt[3]{2} \notin \mathrm{kon}(\mathbb{Q})$.

> Denn: Nach Bemerkung 7.7 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 $\sqrt[3]{2} \notin \mathrm{kon}(\mathbb{Q})$ nach Satz 7.6.

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 7.2 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 7.9 (Winkeldreiteilung)
1. Es seien $\alpha \in \mathbb{R}$ und $K_\alpha := \mathbb{Q}(\cos\alpha)$. Dann ist $\cos(\alpha/3) \in \mathrm{kon}(K_\alpha)$ genau dann, wenn $P := X^3 - 3X - 2\cos\alpha \in K_\alpha[X]$ eine Wurzel in K_α hat.
2. $\alpha := \pi/3$ ist nicht dreiteilbar.

Beweis. 1. Wir zeigen die Äquivalenz für $x := 2\cos(\alpha/3)$. Wegen

$$\cos(3t) \quad = \quad 4\cos^3 t - 3\cos t \qquad (t \in \mathbb{R}) \tag{7.3}$$

gilt mit $t = \alpha/3$

$$0 \quad = \quad 8\cos^3(\alpha/3) - 6\cos(\alpha/3) - 2\cos(\alpha)$$

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

$$\begin{aligned} x \in \mathrm{kon}(K_\alpha) &\Leftrightarrow x \text{ vom Grad } < 3 \text{ über } K_\alpha \\ &\Leftrightarrow P \text{ reduzibel in } K_\alpha[X] \\ &\Leftrightarrow P \text{ hat eine Wurzel in } K_\alpha; \end{aligned}$$

dabei wurden im ersten Schritt Satz 7.6 sowie Bemerkung 7.4, im zweiten Schritt Satz 6.31, und im letzten Bemerkung 7.7 verwendet.

2. Es gilt $\cos(\alpha) = 1/2$ (folgt etwa aus (7.3)), 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 7.7.1 keine Wurzel in $\mathbb{Q} = K_\alpha$. Damit folgt die Behauptung aus 1. □

Nach Satz 7.6 ist jedes $x \in \mathrm{kon}(\mathbb{Q})$ insbesondere algebraisch über $\mathbb{Q}$, also $\mathrm{kon}(\mathbb{Q}) \subset \mathbb{A}$. Wir haben im letzten Abschnitt gesehen, dass $\mathbb{R} \setminus \mathbb{A}$ überabzählbar ist, haben allerdings bisher keine „konkrete“ Zahl als transzendent ausmachen können. Wir beweisen nun:

Satz 7.10 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 $p \in \mathbb{P}$, $p > 2$ 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 $c_{p-1} = (-1)^p \cdots (-m)^p = (-1)^m (m!)^p$ gilt (siehe Analysis, Potenzreihenentwicklung um 0)

$$f^{(k)}(0) = k! c_k = \begin{cases} 0, & \text{falls } k < p-1 \\ (p-1)!(-1)^m (m!)^p, & \text{falls } k = p-1 \\ \in (p!)\mathbb{Z}, & \text{falls } k \geq p \end{cases} .$$

Mit einer entsprechenden Überlegung (Potenzreihenentwicklung um j) ergibt sich

$$f^{(k)}(j) \in (p!)\mathbb{Z} \qquad (k \in \mathbb{N}_0,\, j = 1, \ldots, m).$$

Für

$$F := \sum_{k=0}^{mp+p-1} f^{(k)} : \mathbb{R} \to \mathbb{R}$$

gilt (Teleskopsumme und $f^{(mp+p)} \equiv 0$)

$$\Big(\mathrm{e}^{-x} F(x)\Big)' = \mathrm{e}^{-x}\Big(F'(x) - F(x)\Big) = -\mathrm{e}^{-x} f(x) \qquad (x \in \mathbb{R}),$$

also für $j = 1, \ldots, m$

$$-\int_0^j \mathrm{e}^{-x} f(x)\,dx = \mathrm{e}^{-x} F(x)\Big|_0^j = \mathrm{e}^{-j} F(j) - F(0).$$

Mit $a_0, \ldots, a_m \in \mathbb{Z}$ folgt

$$\begin{aligned} D &:= -\sum_{j=1}^m \Big(a_j \mathrm{e}^j \int_0^j \mathrm{e}^{-x} f(x)\,dx\Big) = \sum_{j=1}^m a_j F(j) - F(0) \underbrace{\sum_{j=1}^m a_j \mathrm{e}^j}_{=-a_0} \\ &= \sum_{j=1}^m a_j \underbrace{F(j)}_{\in (p!)\mathbb{Z}} + a_0 \underbrace{\big(F(0) - f^{(p-1)}(0)\big)}_{\in (p!)\mathbb{Z}} + a_0 f^{(p-1)}(0) \\ &\equiv a_0 f^{(p-1)}(0) = (p-1)!\, a_0 (-1)^m (m!)^p =: b \mod p. \end{aligned}$$

Da P_e (und damit auch P) irreduzibel über $\mathbb{Q}$ ist, gilt $a_0 = P(0) \neq 0$. Für $p > \max\big(m, |a_0|\big)$ ist p kein Teiler von b (sonst müsste p nach Satz 2.6.1 einen der Faktoren teilen, was nicht der Fall ist). Also ist $D \neq 0$ und mit $D \in ((p-1)!)\mathbb{Z}$ damit

$$|D| \geq (p-1)! \,.$$

Andererseits gilt (mit $|f(x)| \leq m^{mp+p-1}$ für $0 \leq x \leq m$)

$$\begin{aligned} |D| &\leq \sum_{j=1}^m \Big(|a_j| \mathrm{e}^j \int_0^j \mathrm{e}^{-x} |f(x)|\,dx\Big) \leq m^{mp+p-1} \sum_{j=1}^m |a_j| \mathrm{e}^j j \\ &\leq \Big(m^{m+1}\Big)^p \mathrm{e}^m \sum_{j=1}^m |a_j| < (p-1)! \end{aligned}$$

für p genügend groß. Widerspruch! □

Bemerkung 7.11 Mit ähnlichen Methoden wie im vorangegangenen Beweis (aber mit mehr Aufwand[21]) 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 7.2 auch $\pi = \sqrt{\pi}^2 \in \mathrm{kon}(\mathbb{Q})$, und damit wäre π nach Satz 7.6 algebraisch über $\mathbb{Q}$.

[21] Einen Beweis findet man etwa in Müller, T., *Irrationalitätsbeweise*, Heldermann Verlag (2014)

8 Isomorphiesatz für Ringe und Quotientenkörper

Wir arbeiten nun die Rolle der Ideale in der Ringtheorie etwas genauer heraus.

Satz 8.1 *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

$$U - U = \sum_{x\in M} (R-R)x = U$$

und

$$RU \subset \sum_{x\in M} (RR)x = U,$$

also ist U ein Ideal. Weiter ist $y = \sum\limits_{x\in M} \delta_{xy}x \in U$ 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 8.2 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 8.1 genau die Ideale der Form $Rx(= xR)$

Beispiel 8.3 Es sei $R = \mathbb{Z}$. Für $x, y \in \mathbb{Z}$ ist $\langle\langle x\rangle\rangle = x\mathbb{Z}$ und

$$\langle\langle\{x, y\}\rangle\rangle \quad = \quad x\mathbb{Z} + y\mathbb{Z} = \mathrm{ggT}(x, y)\mathbb{Z}$$

nach Satz 8.1 und Satz 2.4, also auch $\langle\langle\{x, y\}\rangle\rangle$ ein Hauptideal.

Bemerkung 8.4 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/Definition 4.16 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

$$(x + I) \cdot (y + I) \quad := \quad (xy) + I \qquad (x, y \in R) \tag{8.1}$$

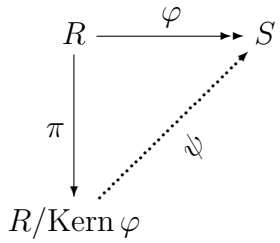
eine Verknüpfung $\cdot$ auf R/I wohldefiniert.

Denn: 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 rechnet man leicht nach, dass $\cdot$ assoziativ sowie distributiv über $+$ mit Einselement $1_R + I$ ist. Also sind R/I ein Ring und π_I ein Ringmorphismus. Analog zum Gruppenfall sind damit und nach Bemerkung 6.6 die Ideale genau die Kerne von Ringmorphismen. Als Standardbeispiel dient wieder $R = \mathbb{Z}$, $I = m\mathbb{Z}$. Hier ist $\mathbb{Z}_m = \mathbb{Z}/(m\mathbb{Z})$; vgl. Beispiel 4.17.1.



Bemerkung 8.5 Sind R, S Ringe, so gilt der Isomorphiesatz der Gruppentheorie (Satz 4.18) 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 R eine ,,Kopie" von $\mathbb{Z}_q$ für ein geeignetes $q \in \mathbb{N}_0$ enthält. Dazu setzen wir $\mathbb{Z}1_R := \{m1_R : m \in \mathbb{Z}\}$ und

$$q := q(R) \;:=\; \begin{cases} 0 & \text{falls } n1_R \neq 0_R \text{ für } n \in \mathbb{N}, \\ \min\{n \in \mathbb{N} : n1_R = 0_R\} & \text{sonst.} \end{cases}$$

Man nennt q die **Charakteristik** von R.

Satz 8.6 *Ist R ein Ring mit Charakteristik q, so gilt:*

1. *$\mathbb{Z}1_R$ ist Unterring von R und isomorph zu $(\mathbb{Z}_q, +, \cdot)$.*
2. *$\mathbb{Z}1_R$ ist genau dann nullteilerfrei, wenn $q \in \mathbb{P} \cup \{0, 1\}$.*
3. *Ist R ein Körper, so ist $q \in \mathbb{P} \cup \{0\}$.*

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 $\varphi(\mathbb{Z}) = \mathbb{Z}1_R$ nach Bemerkung 6.6 ein Unterring von R, und mit dem Isomorphisatz aus Bemerkung 8.5 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 $2 \le q \notin \mathbb{P}$ ist $\mathbb{Z}_q$ nicht nullteilerfrei nach Bemerkung 3.8 und für $q \in \mathbb{P}$ ist $\mathbb{Z}_q$ sogar ein Körper nach Satz 3.7. Schließlich sind $\mathbb{Z}_0 \simeq \mathbb{Z}$ und $\mathbb{Z}_1 = \{[0]_1\}$ nullteilerfrei.

3. Körper sind nullteilerfreie Ringe mit $0 \neq 1$. Also folgt 3. aus 2. □

Jeder Körper mit Charakteristik $q \neq 0$ enthält nach Satz 8.6 eine Kopie des Körpers $\mathbb{Z}_q$. Wir zeigen nun, dass jeder Körper der Charakteristik Null eine Kopie des Körpers $\mathbb{Q}$ enthält. Zunächst beweisen wir, dass jeder Integritätsring durch "Quotientenbildung", analog zur Konstruktion von $\mathbb{Q}$ aus $\mathbb{Z}$, in einen Körper eingebettet werden kann.

Bemerkung 8.7 (Quotientenkörper) Es sei R ein Integritätsring. Dann wird auf $M := R \times (R \setminus \{0\})$ durch

$$(a,b) \sim (a',b') \quad :\Leftrightarrow \quad ab' = a'b$$

für $(a,b),(a',b') \in M$ eine Äquivalenzrelation $\sim$ definiert.

> Denn: 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 mit der Kommutativität
>
> $$b'b''a \;=\; b''b'a \;=\; b''a'b \;=\; a''b'b \;=\; b'a''b\,,$$
>
> und daraus mit der Kürzungsregel aus Bemerkung 1.15 schon $b''a = a''b$, also $(a,b) \sim (a'',b'')$. Damit ist $\sim$ auch transitiv.

Durch einfaches aber insgesamt nicht ganz kurzes Nachrechnen überzeugt man sich, dass auf $Q := M/_\sim$ mit der Notation

$$\widetilde{\frac{a}{b}} \;:=\; [(a,b)]_\sim \quad ((a,b) \in M)$$

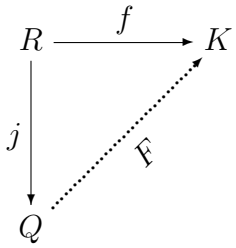
für die zugehörigen Äquivalenzklassen durch

$$\widetilde{\frac{a}{b}} + \widetilde{\frac{c}{d}} \;:=\; \widetilde{\frac{ad+cb}{bd}} \quad \text{und} \quad \widetilde{\frac{a}{b}} \cdot \widetilde{\frac{c}{d}} \;:=\; \widetilde{\frac{ac}{bd}} \quad \text{für} \quad \widetilde{\frac{a}{b}}, \widetilde{\frac{c}{d}} \in Q$$

zwei Verknüpfungen $+$ und $\cdot$ wohldefiniert sind, mit denen $(Q,+,\cdot)$ ein Körper ist. Dabei sind $0_Q = \widetilde{\frac{0}{1}}$ und $1_Q = \widetilde{\frac{1}{1}}$; zu $\widetilde{\frac{a}{b}} \neq 0_Q$ multiplikativ invers ist $\widetilde{\frac{b}{a}}$. Außerdem ist $j : R \to Q$ mit

$$j(a) := \widetilde{\frac{a}{1}} \qquad (a \in R) \tag{8.2}$$

eine Ringeinbettung. Wir nennen $Q = (Q, +, \cdot)$ den **Quotientenkörper** von R und schreiben $\mathrm{Quot}(R) := Q$.



Bemerkung und Definition 8.8 1. Es seien R und $j : R \to Q := \mathrm{Quot}(R)$ wie in Bemerkung 8.7. Ist K ein weiterer Körper und $f : R \to K$ eine Ringeinbettung, so gibt es genau einen Ringmorphismus $F : Q \to K$ mit $F \circ j = f$. Dabei ist F ebenfalls eine Einbettung, und es gilt

$$F\left(\frac{a}{b}\right) = \frac{f(a)}{f(b)} \qquad (a \in R,\, b \in R \setminus \{0\}),$$

also ist $F(Q)$ ein zu Q isomorpher Unterkörper von K. Die Abbildung F heißt die **kanonische Fortsetzung** von f.

Denn: Ist $F : Q \to K$ ein Ringmorphismus mit $F \circ j = f$, so ist F nach Bemerkung 6.7 eine Einbettung mit

$$F\left(\frac{a}{b}\right) = F\left(\frac{a}{1} \Big/ \frac{b}{1}\right) = \frac{F\left(\frac{a}{1}\right)}{F\left(\frac{b}{1}\right)} = \frac{F(j(a))}{F(j(b))} = \frac{f(a)}{f(b)}$$

für $a, b \in R$, $b \neq 0$. Umgekehrt rechnet man nach, dass durch $F\left(\frac{a}{b}\right) := \frac{f(a)}{f(b)}$ für $\frac{a}{b} \in Q$ ein Ringmorphismus von Q nach K mit $F \circ j = f$ wohldefiniert wird (wichtig: $f(b) \neq 0$ für $b \neq 0$).

2. Startet man mit einem Körper K und ist R ein Unterring von K, so ist $f : R \to K$ mit $f(a) := a$ für $a \in R$ eine Ringeinbettung. Ist F die kanonische Fortsetzung von f, so gilt in diesem Fall

$$F\left(\frac{a}{b}\right) = \frac{a}{b} \qquad (a \in R,\, b \in R \setminus \{0\}).$$

Insbesondere ist $F(\mathrm{Quot}(R)) = \{a/b : a, b \in R, b \neq 0\}$ ein Unterkörper von K.

Beispiel 8.9 Ist K ein Körper, so ist $K[X]$ ein Integritätsring und

$$\mathrm{Quot}(K[X]) = \left\{ \frac{P}{Q} : P, Q \in K[X],\, Q \neq 0 \right\}$$

der Quotientenkörper von $K[X]$. 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 6.25 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.

Definition 8.10 Es sei K ein Körper. Dann heißt, unter Verwendung der Notation aus Definition 6.3,

$$P(K) \ := \bigcap_{U \subset K \text{ Unterkörper}} U \ = \ \langle \{1_K\} \rangle_{\text{Körper}}$$

Primkörper von K. Damit ist $P(K)$ offenbar der kleinste Unterkörper von K.

Bemerkung 8.11 Ist K ein Körper, so ist

$$P(K) \ = \ \langle \{1_K\} \rangle_{\text{Körper}} \ \supset \ \{a/b : a, b \in \mathbb{Z}1_K,\ b \neq 0\} = \mathrm{Quot}(\mathbb{Z}1_K)$$

und $\mathrm{Quot}(\mathbb{Z}1_K)$ nach Bemerkung 8.8.2 (mit $R = \mathbb{Z}1_K$) ein Unterkörper von K. Also ist

$$P(K) = \mathrm{Quot}(\mathbb{Z}1_K).$$

Speziell für $K = \mathbb{Q}$ gilt $P(\mathbb{Q}) = \mathrm{Quot}(\mathbb{Z}) = \mathbb{Q}$.

Satz 8.12 *Es sei K ein Körper mit Charakteristik q. Dann gilt*

$$P(K) \ \simeq \ \begin{cases} \mathbb{Z}_q & \textit{falls } q \in \mathbb{P}, \\ \mathbb{Q} & \textit{falls } q = 0. \end{cases}$$

Beweis. Im Fall $q \in \mathbb{P}$ ist $\mathbb{Z}_q$ ein Körper. Also ist $\mathbb{Z}1_K$ nach Satz 8.6 ein zu $\mathbb{Z}_q$ isomorpher Körper sowie $\mathbb{Z}1_K = \mathrm{Quot}(\mathbb{Z}1_K) = P(K)$ nach Bemerkung 8.11. Im Fall $q = 0$ ist $\mathbb{Z}1_K \simeq \mathbb{Z}$ und $f : \mathbb{Z} \to K$ mit $f(m) := m1_K$ eine Ringeinbettung. Für die kanonische Fortsetzung $F : \mathbb{Q} = \mathrm{Quot}(\mathbb{Z}) \to K$ gilt dann

$$F\left(\frac{m}{n}\right) = \frac{m1_K}{n1_K} \quad (m, n \in \mathbb{Z}, n \neq 0).$$

Nach Bemerkung 8.11 ist $F(\mathbb{Q}) = \mathrm{Quot}(\mathbb{Z}1_K) = P(K)$, also $P(K)$ isomorph zu $\mathbb{Q}$ nach Bemerkung/Definition 8.8. □

Satz 8.13 *Es sei K ein endlicher Körper. Dann hat K eine Charakteristik $q \in \mathbb{P}$ und mit $d := [K : P(K)]$ gilt $\#K = q^d$.*

Beweis. Nach Satz 8.12 ist $P(K) \simeq \mathbb{Z}_q$ für ein $q \in \mathbb{P}$ und damit $\#P(K) = \#\mathbb{Z}_q = q$. Aus $d < \infty$ folgt, dass K isomorph zu $(P(K))^d$ ist (Lineare Algebra), also insbesondere $\#K = q^d$. □

Index