Jürgen Müller

Geometrie, elementare Zahlentheorie und Algebra

Skriptum zur Vorlesung
Wintersemester 2023/2024 [1]

Universität Trier
Fachbereich IV
Mathematik/Analysis

[1] In Teilen basierend auf dem Skript der entsprechenden Vorlesung von Professor Dr. Lutz Mattner aus dem Wintersemester 2014/15

Contents

1 Der Ring der ganzen Zahlen

Den Umgang mit Zahlen lernt man in einem sehr frühen Stadium des Lebens, meist ohne sich die Frage zu stellen, was eigentlich Zahlen sind. Je mehr man darüber nachdenkt, um so schwieriger scheint eine Antwort. Die Mathematik, die sich Zahlen zum Werkzeug macht, ist pragmatisch. In ihr definiert man Zahlen oder besser Zahlensysteme als Mengen von Objekten, die untereinander in gewisser, uns plausibel und sinnvoll erscheinender Weise in Beziehung stehen. Wir gehen zunächst kurz auf diesen – axiomatischen – Zugang zu den natürlichen und ganzen Zahlen ein.

Bemerkung und 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 $\cdot, \circ, *, \times, +, \ldots$ für f und schreibt xfy statt $f(x, y)$ für $x, y \in M$,[2] 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 auf M (die wir ohne Einschränkung mit $\cdot$ bezeichnen) 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. Bei assoziativen Verknüpfungen lässt man die Klammern meist weg, setzt also zum Beispiel $xyz := (xy)z = x(yz)$. Das **Pluszeichen** $+$ wird üblicherweise nur für kommutative Verknüpfungen benutzt.

3. Ein $e \in M$ heißt **linksneutral** (bezüglich $\cdot$) falls $ex \;=\; x$ für $x \in M$ gilt, **rechtsneutral** falls $xe = x$ für $x \in M$ gilt, und **neutral** falls beides gilt. Ist e linksneutral und e' rechtsneutral für die Verknüpfung $\cdot$ auf M, so ist

$$e = ee' = e'.$$

Insbesondere sind (im Falle der Existenz) neutrale Elemente eindeutig.

Bemerkung 1.2 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 $1 \notin \nu(\mathbb{N})$.[3]

[2] man spricht dann von Infix-Schreibweise

[3] $\nu(n)$ nennt man auch Nachfolger von n.

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

Damit definiert man die arabischen Ziffern durch $2 := \nu(1)$, $3 := \nu(2)$, $4 := \nu(3)$, $5 := \nu(4)$, $6 := \nu(5)$, $7 := \nu(6)$, $8 := \nu(7)$ und $9 := \nu(8)$.

Mit viel Aufwand kann man 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[4] $<$ auf $\mathbb{N}$ definiert durch $m < n$ genau dann, wenn $n = m + k$ für ein $k \in \mathbb{N}$. Weiter kann man zeigen: Auf $\mathbb{N}$ existiert genau eine assoziative und kommutative Verknüpfung $\cdot$ so, dass $n \cdot 1 = n$ ist und dass $m(n + 1) = mn + m$ für $n, m \in \mathbb{N}$ gilt. Insbesondere ist 1 neutrales Element bezüglich $\cdot$ und Minimum von $\mathbb{N}$.

Aus dem Prinzip der vollständigen Induktion folgt die wichtige **Wohlordnungseigenschaft** von $\mathbb{N}$:[5]

Satz 1.3 (Wohlordnung von $\mathbb{N}$)
Jede nichtleere Menge $M \subset \mathbb{N}$ hat ein Minimum.

Beweis. Es genügt zu zeigen: Für alle $n \in \mathbb{N}$ gilt: Ist $M \subset \mathbb{N}$ so, dass $M \cap \{1, \ldots, n\} \neq \varnothing$, so hat M ein Minimum.

Induktionsanfang $n = 1$: Ist $M \subset \mathbb{N}$ mit $M \cap \{1\} \neq \varnothing$, so ist $1 \in M$ Minimum von M.

Induktionsschritt $n \to n + 1$: Es sei $M \subset \mathbb{N}$ mit $M \cap \{1, \ldots, n + 1\} \neq \varnothing$. Existiert kein $m \in M$ mit $m < n + 1$, so ist $n + 1$ Minimum von M. Existiert andererseits ein $m \in M$ mit $m < n+1$, so ist $m \leq n$. Also ist $M \cap \{1, \ldots, n\} \neq \varnothing$ und damit hat M nach Induktionsannahme ein Minimum. □

Definition 1.4 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 $(M, \cdot, e)$. Halbgruppen bzw. eine Monoide M mit kommutativer Verknüpfung $\cdot$ heißt **kommutativ** oder auch **abelsch**.

[4] Für die Definition einer Ordnungsrelation und den Begriff eines Minimums bzw. Maximums siehe etwa https://www.math.uni-trier.de/~mueller/EinfMathe/Einf_Mathe_GW_WS2020-21.pdf, Definitionen 3.1 und 3.2.

[5] Man kann zeigen, dass die Wohlordnungseigenschaft sogar äquivalent zum Prinzip der vollständigen Induktion ist.

Beispiel 1.5 $(\mathbb{N}, \cdot, 1)$ ist ein abelsches Monoid und $(\mathbb{N}, +)$ eine abelsche Halbgruppe. 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**

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

Außerdem gilt die **Division mit Rest**: Sind $p \in \mathbb{N}_0$, $q \in \mathbb{N}$, so existiert ein Paar $(m, r) \in \mathbb{N}_0^2$ mit $r < q$ und

$$p = mq + r.$$

Denn: Die Menge $M := \{k \in \mathbb{N}_0 : kq \leq p\}$ ist wegen $kq \geq k$ endlich. Setzt man $m := \max M$, so ist $kq \leq p < kq + q$ und damit existiert ein $r \in \mathbb{N}_0$ mit $r < q$ und $p = kq + r$.

Bemerkung 1.6 Definition 1.7 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 beides gilt; entsprechend heißt x dann **(links-, rechts-)invertierbar**. Wir setzen

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

Stets ist $e \in M^*$. Ist jedes $x \in M$ invertierbar, d. h. $M = M^*$, so heißt M **Gruppe**.

Bemerkung 1.8 Es sei $(M, \cdot, e)$ ein Monoid.

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

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

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 $\left(x^{-1}\right)^{-1} = x$ und

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

da $x^{-1}x = xx^{-1} = e$ und $xyy^{-1}x^{-1} = xx^{-1} = e$ sowie $y^{-1}x^{-1}xy = y^{-1}y = e$.

Also 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 1.9 Es sei $X \neq \varnothing$ ein Menge. Dann ist [6] $\mathrm{Abb}(X)$ mit der Komposition $\circ$ von Funktionen als Verknüpfung ein Monoid mit mit neutralem Element id_X. Hier ist

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

und 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 1.10 Es sei R eine Menge und es seien $+$ und $\cdot$ Verknüpfungen auf R mit:

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

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

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

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

Dann 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 $(R, +, \cdot)$. Schließlich verwendet in allgemeinen Ringen Punkt-vor-Strich-Schreibweisen, also zum Beispiel $x + yz := x + (yz)$.

Bemerkung 1.11 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.[7] 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 Monotoniegesetze verträglich ist, d.h. ist $x < y$, so gilt

$$x + z < y + z$$

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

[7] Genaueres etwa unter https://www.math.uni-trier.de/~mueller/EinfMathe/Einf_Mathe_GW_WS2020-21.pdf, Anhang A.

für alle z und

$$xz < yz \quad \text{falls } z > 0.$$

Kommutative Ringe mit einer Ordnung, die diese Eigenschaften besitzt, nennt man auch geordnete Ringe. Aus der Wohlordnung von $\mathbb{N}$ folgt, 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.

Bemerkung 1.12 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 $(x - y)z = xz - yz$.

Wir greifen auf die üblichen Summen-, Produkt- und Potenzschreibweisen in allgemeinen Monoiden und Ringen zurück.[8] Gelegentlich erweist es sich als praktisch, Summen und Produkte in verallgemeinerter Form zu nutzen:

Ist $(M, \cdot, e)$ ein kommutatives Monoid und ist $J \neq \varnothing$ eine Menge, so setzen wir für $A \subset M$

$$A^{(J)} := \{x = (x_j)_{j \in J} \in A^J : J_x := \{j \in J : x_j \neq e\} \text{ endlich}\}.$$

Ist $(x_j)_{j \in J} \in A^{(J)}$, so schreiben wir

$$\prod_{j \in J} x_j := \prod_{j \in J_x} x_j.$$

Wichtig ist dabei, dass wegen der Kommutativität von $\cdot$ Produkte nicht von der Reihefolge der Faktoren abhängen. Im Falle des Additionszeichens als Verknüpfung wird natürlich $\prod$ durch $\sum$ ersetzt. Im Weiteren betrachten wir allgemeine Summen in $(\mathbb{N}, +, 0)$ und Produkte in $(\mathbb{N}, \cdot, 1)$.

Damit kann man die q-adische Entwicklung natürlicher Zahlen formalisieren:

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 $a = (a_j) = \big(a_j(n)\big) \in A^{(\mathbb{N}_0)}$ mit*

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

[8] Siehe etwa https://www.math.uni-trier.de/~mueller/EinfMathe/Einf_Mathe_GW_WS2020-21.pdf, Abschnitt 2

Beweis. 1. Wir zeigen die Existenz per Induktion nach n.
Für $n = 0$ ist $a_j(0) := 0$ 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

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

mit $1 \leq m < q$ und $0 \leq n' < q^k \leq n$. 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

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

2. Eindeutigkeit: Sind $a = (a_j), b = (b_j) \in A^{(\mathbb{N}_0)}$ mit $a \neq b$ und

$$m := \max\{j : a_j \neq b_j\},$$

wobei ohne Einschränkung $b_m > a_m$, so gilt ([Ü])

$$\sum_{j \in \mathbb{N}_0} b_j q^j - \sum_{j \in \mathbb{N}_0} a_j q^j = \sum_{j=0}^{m} (b_j - a_j) q^j \geq q^m - \sum_{j=0}^{m-1} a_j q^j > 0.$$

□

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

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

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 $xy \in R^*$).[9]

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

[9] Auch geordnete Ringe sind Integritätsbereiche.

2 Teiler und Primzahlen

Wir betrachten ein weiteres Beispiel einer Halbgruppe, die sich im Weiteren als recht praktisch erweist.

Bemerkung und Definition 2.1 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.

Ist R ein kommutativer Ring, so gelten weitere Rechenregeln für Minkowskisummen und Komplexprodukte in $\mathscr{P}(R)$. Zu beachten ist, dass das Komplexprodukt nicht distributiv über der Minkowskisumme ist. Allerdings gilt immerhin stets $(A + B)C \subset AC + BC$ und $a(B + C) = aB + aC$ für $A, B, C \subset R$ und $a \in R$.

Wir wollen die interessante Frage beantworten, wie $a\mathbb{Z} + b\mathbb{Z}$ dargestellt werden kann. Für $a \in \mathbb{Z}$ setzt man $|a| := \operatorname{sign}(a) \cdot a$, wobei

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

Satz 2.2 (**Division mit Rest**)
Es sei $(a, q) \in \mathbb{Z}^2$ mit $q \neq 0$. Dann existiert genau ein Paar $(m, r) \in \mathbb{Z}^2$ mit $a = mq + r$ und $0 \leq r < |q|$.

Beweis. Existenz: Wegen $q \neq 0$ ist $L := \mathbb{N}_0 \cap (a - \mathbb{Z}q) \neq \varnothing$. Ist $r := \min L$, so gilt $r < q$ wegen $y - |q| \in a - \mathbb{Z}q$ für $y \in a - \mathbb{Z}q$. Für m so, dass $a - mq = r$ ergibt sich die Behauptung.

Eindeutigkeit: Es seien $m, m' \in \mathbb{Z}$ und $0 \leq r, r' \leq |q| - 1$ so, dass $a = mq + r = m'q + r'$. Dann gilt $|r - r'| \leq |q| - 1$ und $r - r' = (m - m')q \in \mathbb{Z}q$. Hieraus folgt zunächst $m - m' = 0$ und dann auch $r - r' = 0$. □

Definition 2.3 Sind $a, q \in \mathbb{Z}$, so sagt man q **teilt** a, oder q ist ein **Teiler** von a, falls $a \in \mathbb{Z}q$, also $a = mq$ für ein $m \in \mathbb{Z}$ gilt. Man schreibt dann $q \mid a$ und andernfalls $q \nmid a$. Ist dabei $q \neq 0$, so ist m nach Satz 2.2 eindeutig bestimmt. Wir setzen dann $a/q := m$. Für $q \in \mathbb{Z}$ und $A \subset \mathbb{Z}$ schreiben wir zudem $q \mid A$ falls $q \mid a$ für jedes $a \in A$ gilt, wenn also $A \subset \mathbb{Z}q$ gilt.

Bemerkung 2.4 Es seien $a, b, c \in \mathbb{Z}$. Aus obiger Definition ergibt sich leicht ([Ü]):

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

Definition 2.5 Es seien $a, b \in \mathbb{Z}$ mit $a \neq 0$ oder $b \neq 0$. Dann heißt

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

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 2.6 (**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 $L := a\mathbb{Z} + b\mathbb{Z}$. Aus $d \mid a$ und $d \mid b$ folgt $d \mid L$ nach Bemerkung 2.4.3. und damit $L \subset d\mathbb{Z}$. Mit $q := \min(\mathbb{N} \cap L)$ ist weiter

$$q\mathbb{Z} \subset (a\mathbb{Z} + b\mathbb{Z})\mathbb{Z} \subset (a\mathbb{Z})\mathbb{Z} + (b\mathbb{Z})\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} = L.$$

Also reicht es, $d = q$ zu zeigen. Wegen $q \in L \subset d\mathbb{Z}$ folgt $d \mid q$ und damit ist jedenfalls $d \leq q$.

Weiter sei $a = mq + r$ wie in Satz 2.2. Dann ist

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

und $0 \leq r < |q|$, also $r = 0$ nach Definition von q. Damit ist q Teiler von a. Genauso gilt $q \mid b$. Also ist auch $q \leq \mathrm{ggT}(a, b) = d$. □

Bemerkung 2.7 Ein Verfahren zur Berechnung des $\mathrm{ggT}(a,b)$ ist der **Euklidische Algorithmus**[10]: Sind $a,b \in \mathbb{Z}\setminus\{0\}$, so wendet man sukzessive Division mit Rest an, startend mit $r_0 = b, r_1 = |a|$:

$$\begin{aligned}(b=)\ r_0 &= m_1 r_1 + r_2 \quad (= m_1|a| + r_2)\\ r_1 &= m_2 r_2 + r_3\\ &\ \ \vdots\end{aligned}$$

Da nach Satz 2.2 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 $r_{n-1} = m_n r_n$. 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

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

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

Andererseits sieht man durch Lesen des Gleichungssystems von oben nach unten und mit Satz 2.6

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

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

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

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

Nach Satz 2.6 ist damit $1029\cdot\mathbb{Z} + 1071\cdot\mathbb{Z} = 21\cdot\mathbb{Z}$.

Als weitere Folgerung aus Satz 2.6 erhalten wir

[10] 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 *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.

Satz 2.8 *Es seien $a, b, c \in \mathbb{Z}$ mit $\mathrm{ggT}(a, b) = 1$. Dann gilt:*

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

Beweis. Zunächst ist $1 \in a\mathbb{Z} + b\mathbb{Z}$ nach Satz 2.6 und damit auch

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

1. Es gelte $a \mid bc$. Mit $a \mid ac$ gilt dann $a \mid (ac)\mathbb{Z} + (bc)\mathbb{Z}$ nach Bemerkung 2.4.3 , also $a \mid c$ nach (2.1).
2. Es gelte $a \mid c$ und $b \mid c$, 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 nach Satz 2.6 auch $1 \in a\mathbb{Z} + c\mathbb{Z}$. Also folgt

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

Wieder nach Satz 2.6 sind a und bc teilerfremd. □

Bemerkung und Definition 2.9 Eine Zahl $p \in \mathbb{N} \setminus \{1\}$ heißt **Primzahl** falls sie nur die Teiler ± 1 und $\pm p$ hat. Wir setzen $\mathbb{P} := \{p : p \text{ Primzahl}\}$. Für jedes $n \in \mathbb{N} \setminus \{1\}$ ist

$$p := \min\{k > 1 : k \mid n\}$$

eine Primzahl, da p sonst einen Teiler a mit $1 < a < p$ hätte, der dann auch Teiler von n wäre im Widerspruch zur Minimalität von p. Insbesondere hat jedes $n > 1$ einen Primteiler. Wichtig ist zudem folgender Fakt: Für $p \in \mathbb{P}$ und $a, b \in \mathbb{Z}$ folgt aus $p \mid ab$ schon $p \mid a$ oder $p \mid b$.

> Denn: Gilt $p \mid ab$ und ist p kein Teiler von a, also $\mathrm{ggT}(a, p) = 1$ wegen p prim, so folgt $p \mid b$ nach Satz 2.8.1.

Allgemeiner ergibt sich daraus mittels Induktion über die Mächtigkeit von A: *Ist $A \subset \mathbb{Z}$ endlich und ist p prim, so folgt aus $p \mid \prod_{a \in A} a$ schon $p \mid a$ für ein $a \in A$.*

Satz 2.10 (Euklid) *Die Menge $\mathbb{P}$ ist unendlich.*

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 $q \mid n$, so folgt aus $q \mid \prod_{p\in\mathbb{P}} p$ auch $q \mid (n - \prod_{p\in\mathbb{P}} p = 1)$ nach Bemerkung 2.4.3. Widerspruch. □

Wir zeigen nun, dass jede natürliche Zahl $n \geq 2$ eine Primfaktorzerlegung hat und dass diese in geeigneter Weise eindeutig ist.[11]

Satz 2.11 (**Primfaktorzerlegung, Fundamentalsatz der Arithmetik**) *Für jedes $n \in \mathbb{N}$ existiert genau ein Tupel $(\alpha_p)_{p\in\mathbb{P}} = (\alpha_p(n))_{p\in\mathbb{P}} \in \mathbb{N}_0^{(\mathbb{P})}$* [12] *mit*

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

Beweis. 1. Existenz: Für $n = 1$ ist $\alpha_p(1) := 0$ $(p \in \mathbb{P})$ geeignet. Es sei also $n > 1$. Ist p_1 ein Primteiler von n, so 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 n_1 einen Primteiler p_2, also ist $n_1 = p_2 n_2$ 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 $n = \prod_{j=1}^{N} p_j$. Definiert man α_p als die Anzahl der $j \in \{1, \ldots, N\}$ mit $p_j = p$, so gilt damit

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

2. 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 $n = \prod_{p\in\mathbb{P}} p^{\nu_p} = \prod_{p\in\mathbb{P}} p^{\mu_p}$ und $\nu_q \neq \mu_q$ für ein $q \in \mathbb{P}$. Ohne Einschränkung sei $\nu_q > \mu_q$. Dann folgt aus $q \mid (n = \prod_{p\in\mathbb{P}} p^{\mu_p})$ mit Bemerkung und Definition 2.9 die Existenz eines $q' \in \mathbb{P}$ mit $\mu_{q'} > 0$ und $q \mid q'$. Da q' eine Primzahl ist, gilt schon $q = q'$. Durch Kürzen ergibt sich, dass n/q die Darstellungen

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

[11] Primzahlen können also gewissermaßen als Elementarbausteine der natürlichen Zahlen bezüglich der Multiplikation angesehen werden.

[12] Dabei ist $\mathbb{N}_0 = (\mathbb{N}_0, +, 0)$.

mit $\nu_q - 1 \neq \mu_q - 1$ hat. Dies widerspricht der Minimalität von n.

3. Für $n \in \mathbb{N}$ und $p \in \mathbb{P}$ ist $\alpha_p(n) > 0$ nach 2. genau dann, wenn p ein Teiler von n ist. Damit gilt auch $n = \prod_{p\in\mathbb{P},\, p|n} p^{\alpha_p(n)}$. □

Beispiel 2.12 Die Zahl $n = 2023$ hat die Primfaktorzerlegung $7 \cdot 17 \cdot 17$, also ist $\alpha_7(n) = 1$, $\alpha_{17}(n) = 2$ und $\alpha_p(n) = 0$ für alle anderen $p \in \mathbb{P}$.

Bemerkung 2.13 Wir schreiben $\mathbb{P} := \{p_j : j \in \mathbb{N}\}$, wobei $p_{j+1} > p_j$ für $j \in \mathbb{N}$. Dann heißt p_j die j-te Primzahl, etwa $p_1 = 2$, $p_2 = 3$, $p_3 = 5$. Nach dem Fundamentalsatz der Arithmetik ist damit die Abbildung $f : \mathbb{N}_0^{(\mathbb{N})} \to \mathbb{N}$ mit

$$f((\nu_j)_{j=1}^{\infty}) = \prod_{j\in\mathbb{N}} p_j^{\nu_j}$$

bijektiv mit $f^{-1}(n) = (\alpha_{p_j}(n))_{j=1}^{\infty}$.[13] Es gilt etwa

$$f((0,0,0,1,0,0,2,0,\ldots)) = 2023.$$

Wir stellen uns nun die Frage nach der relativen Häufigkeit der Primzahlen unter den natürliche Zahlen. Eine Aussage macht der berühmte Primzahlsatz, der 1896 gleichzeitig und unabhängig von de la Vallée-Poussin und Hadamard bewiesen wurde:[14]

Bezeichnet man mit $\pi(x)$ die Anzahl der Primzahlen $\leq x$, so gilt:[15]

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

Wir beweisen eine Vorstufe des Primzahlsatzes, die auf Tschebyscheff zurückgeht und mit elementaren Methoden auskommt. Ein wesentliches Hilfsmittel ist die folgende Formel: [16]

Satz 2.14 *(***Legendre***)* *Für $n \in \mathbb{N}$ und $p \in \mathbb{P}$ gilt*

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

[13] Theoretisch ist damit die Primfaktorzerlegung von n gegeben. Allerdings erweist es sich als extrem schwierig, die $\alpha_p(n)$ aus n zu berechnen. Dieser Umstand liegt verschiedenen Verschlüsselungsverfahren zugrunde, wie wir später noch sehen werden.

[14] siehe etwa https://de.wikipedia.org/wiki/Primzahlsatz

[15] $f(x) \sim g(x)$ bedeutet, dass $f(x)/g(x) \to 1$ gilt

[16] $\lfloor \cdot \rfloor$ bezeichnet die Gaußklammer

Beweis. Man beachte zunächst, dass $\alpha_p(n!) = \alpha_p(1) + \ldots + \alpha_p(k)$ gilt. Weiter ist

$$\left\lfloor \frac{n}{a} \right\rfloor = \#\{k \in \{1,\ldots,n\} : a \mid k\} = \#(a\mathbb{N} \cap \{1,\ldots,n\})$$

für $n, a \in \mathbb{N}$ ([Ü]). Wegen $\alpha_p(k) = \#\{\nu \in \mathbb{N} : p^\nu \mid k\}$ und $\lfloor n/p^\nu \rfloor = 0$ für $\nu > \ln n / \ln p$ ergibt sich

$$\sum_{k=1}^{n} \alpha_p(k) = \sum_{k=1}^{n} \sum_{\nu \geq 1,\, p^\nu \mid k} 1 = \sum_{\nu \geq 1} \sum_{k \leq n, p^\nu \mid k} 1 = \sum_{\nu=1}^{\lfloor \ln n / \ln p \rfloor} \left\lfloor \frac{n}{p^\nu} \right\rfloor .$$

□

Satz 2.15 (**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

$$\binom{2n}{n} \begin{cases} \leq \sum\limits_{k=0}^{2n} \binom{2n}{k} = (1+1)^{2n} = 2^{2n} \\ = (2n)!/(n!)^2 = (n+1)(n+2)\cdots(2n)/n! \geq 2^n \end{cases}$$

und für $s_n := \ln \binom{2n}{n}$ daher

$$n \ln 2 \leq s_n \leq 2n \ln 2. \tag{2.2}$$

Ist $k \in \mathbb{N}$ und ist p Teiler von $k!$, so ist $p \leq k$, da p einen der Faktoren teilt. Für $n \in \mathbb{N}$ ist unter Verwendung von Satz 2.14

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

Weiter gilt für $x \in \mathbb{R}$

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

Damit ergibt sich einerseits

$$s_n \leq \sum_{p \leq 2n} \ln p \sum_{\nu=1}^{\lfloor \ln(2n)/\ln p \rfloor} 1 = \sum_{p \leq 2n} \ln p \left\lfloor \frac{\ln 2n}{\ln p} \right\rfloor \leq \pi(2n) \ln(2n) \tag{2.3}$$

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

$$\sum_{n<p\le 2n} \ln p \le \sum_{p\le 2n} \ln p \cdot \left(\left\lfloor \frac{2n}{p} \right\rfloor - 2 \left\lfloor \frac{n}{p} \right\rfloor \right) \le s_n. \tag{2.4}$$

2. Beweis der linken Ungleichung: Für $n \in \mathbb{N}$ gilt mit (2.2) und (2.3) wegen $\ln 2 > 5/8$

$$\pi(2n) \ge \frac{n \ln 2}{\ln(2n)} \ge \frac{1}{4} \frac{2n}{\ln(2n)}.$$

Mit $\ln 2/(2 + 1/n) \ge 1/4$ für $n \ge 2$ ist für $n \ge 2$ auch

$$\pi(2n+1) \ge \pi(2n) \ge \frac{n \ln 2}{\ln(2n)} > \frac{n \ln 2}{2n+1} \frac{2n+1}{\ln(2n+1)} \ge \frac{1}{4} \frac{2n+1}{\ln(2n+1)}$$

und damit die Ungleichung außer für $n = 3$ bewiesen, dafür aber offenbar auch richtig.

3. Beweis der rechten Ungleichung: Wir setzen

$$\vartheta(x) \;:=\; \sum_{p\le x} \ln p \qquad (x \ge 0).$$

Für $n \in \mathbb{N}$ erhalten wir mit (2.4) und (2.2)

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

Damit folgt für $k \in \mathbb{N}_0$

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

also mit $0 = \vartheta(1) = \vartheta(2^0)$ und geometrischer Summenformel

$$\vartheta(2^{k+1}) \;=\; \sum_{j=0}^{k} \big(\vartheta(2^{j+1}) - \vartheta(2^j)\big) \;\le\; \sum_{j=0}^{k} 2^{j+1} \ln 2 \;=\; 2(2^{k+1}-1) \ln 2 \;\le\; 2^{k+2} \ln 2.$$

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

$$\begin{aligned} \big(\pi(n) - \pi(y)\big) \ln y \;&=\; \sum_{y<p\le n} \ln y \le \sum_{y<p\le n} \ln p \le \vartheta(n) \le \vartheta(2^{k+1}) \\ &\le\; 2^{k+2} \ln 2 \le 4n \ln 2, \end{aligned}$$

speziell für $y = n^{2/3}$ also

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

und wegen $\pi(n^{2/3}) \leq n^{2/3}$ 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,[17] folgt

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

□

Als Folgerung aus Satz 2.15 erhält man $p_n \leq 8n\ln(3n)$ ([Ü]). Da die Reihe $\sum_{n=1}^{\infty} 1/(n\ln(3n))$ etwa nach dem Integralkriterium[18] divergiert, folgt

Satz 2.16 (Euler)
Die Reihe über die Reziproken der Primzahlen divergiert, d. h.

$$\sum_{n\in\mathbb{N}} \frac{1}{p_n} = \infty.$$

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.

Bemerkung 2.17 Sind $a \in \mathbb{Z}$ und $m \in \mathbb{N}$, so gilt $a^m - 1 = (a-1)\sum_{j=0}^{m-1} a^j$ nach der geometrischen Summenformel, also

$$(a-1) \mid (a^m - 1) \tag{2.5}$$

und im Falle, dass m ungerade ist, wegen $a + 1 = -(-a-1)$ und $a^m + 1 = -((-a)^m - 1)$ auch

$$(a+1) \mid (a^m + 1) \tag{2.6}$$

Damit erhält man

1. Ist $2^k - 1 \in \mathbb{P}$, so ist $k \in \mathbb{P}$.

[17] 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 $x > \mathrm{e}^{1/\alpha}$. Also ist φ streng wachsend auf $(0, e^{1/\alpha}]$ und fallend auf $[e^{1/\alpha}, \infty)$.

[18] siehe https://www.math.uni-trier.de/~mueller/EinfMathe/Analysis_SoS2021.pdf

Denn: Es sei $k \in \mathbb{N} \setminus \mathbb{P}$. Ist $k = 1$, so ist $2^k - 1 = 1 \notin \mathbb{P}$. Ist $k > 1$, so ist $k = r \cdot m$ mit gewissen $r, m \in \mathbb{N} \setminus \{1\}$, also wegen (2.5)

$$(2^r - 1) \mid \big((2^r)^m - 1 = 2^k - 1\big),$$

wobei $1 < 2^r - 1 < 2^k - 1$, und damit $2^k - 1 \notin \mathbb{P}$.

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 $k = 2^s m$ für ein $s \in \mathbb{N}_0$ und ein $m \in \mathbb{N} \setminus \{1\}$ mit m ungerade. Mit (2.6) gilt

   $$(2^{2^s} + 1) \mid \big((2^{2^s})^m + 1 = 2^k + 1\big),$$

   wobei $1 < 2^{2^s} + 1 < 2^k + 1$. 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 10/2023) sind 51 Mersenne-Zahlen als prim erkannt, die größte davon (im Jahr 2018 identifiziert) ist

$$2^{82.589.933} - 1,$$

mit 24.862.048 Stellen im Dezimalsystem[19] Andererseits ist

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

Bis heute ist 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: Wir zeigen, dass $641 =: d$ die Zahl F_5 teilt.[20] Zunächst gilt

   $$(a + 1) \mid ((a + 1)(a - 1)(a^2 + 1) = a^4 - 1)$$

   für $a \in \mathbb{Z}$. Weiter ist $d = a + 1$ für $a := 5 \cdot 2^7$. Also gilt

   $$d \mid (a^4 - 1 = 5^4 2^{28} - 1).$$

   Andererseits ist auch $d = 5^4 + 2^4$ und damit

   $$d \mid (d \cdot 2^{28} = 5^4 2^{28} + 2^{32}).$$

   Also folgt $d \mid (2^{32} + 1 = F_5)$.

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

[19] siehe etwa https://de.wikipedia.org/wiki/Mersenne-Zahl

[20] Der (ziemlich geniale) Beweis geht auf Euler zurück

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

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

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 $m \mid (a' - a)$ und $m \mid (a'' - a')$ implizieren zusammen $m \mid (a'' - a' + a' - a = a'' - a)$.

Die Äquivalenzklasse $[a] := [a]_m := \{a' \in \mathbb{Z} : a \equiv_m a'\}$ ist gegeben durch

$$[a]_m = a + m\mathbb{Z}.$$

Speziell ist $a + 0\mathbb{Z} = \{a\}$. Mit Satz 2.2 sieht man, dass $[a]_m = [a']_m$ genau dann gilt, wenn a und a' bei Division mit Rest durch m den gleichen Rest $r \in \{0, \ldots, m-1\}$ haben. Daher nennt man $[a]_m$ **Restklasse modulo** m. Schreibt man

$$\mathbb{Z}_m := \mathbb{Z}/_{\equiv_m} = \{[a]_m : a \in \mathbb{Z}\}$$

für die Quotientenmenge, so gilt

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

mit $\#\mathbb{Z}_m = m$ für $m > 0$. 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 $[1]_m$ (wobei $[0]_1 = [1]_1$) 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 2.4.3 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 $\mathbb{Z}_4 = \{[0]_4, [1]_4, [2]_4, [3]_4\}$ 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 $[2]_4 \cdot [x]_4 = [1]_4$ bzw. 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

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

Für $m \in \{3, 9\}$ ist $[10]_m = [1]_m$ und zudem ist $[10]_{11} = [-1]_{11}$. Damit gilt

$$[n]_m = \begin{cases} \sum_{j=0}^{r} [a_j]_m \;=\; \Big[\sum_{j=0}^{r} a_j\Big]_m & \text{für } m = 3, 9 \\ \sum_{j=0}^{r} [a_j]\,[(-1)^j]_m \;=\; \Big[\sum_{j=0}^{r} a_j (-1)^j\Big] & \text{für } m = 11 \end{cases}$$

□

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 2.6 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

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

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

> Denn: Nach Bemerkung 1.8.2 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 und Definition 3.1 mittels Satz 3.4.

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

Satz 3.7 *Es sei $p \in \mathbb{P}$. Dann ist*

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

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 $a \in \{1,\dots,p-1\}$ und damit $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{[0]_p\}$ nach Bemerkung und 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 $r, s \in \{2,\dots,m-1\}$ mit $m = rs$ und damit $[0]_m = [r]_m[s]_m$ sowie $[r]_m,\ [s]_m \neq 0$.

Bemerkung und Definition 3.9 Es seien $(M, \cdot, e)$ ein Monoid und $U \subset M$. Dann heißt U ein **Untermonoid**, falls $e \in U$ gilt und $(U, \cdot_U, e)$ mit $x \cdot_U y := xy$ für $x, y \in U$ ein Monoid ist. Dies ist genau dann der Fall, wenn $e \in U$ ist und mit $a, b \in U$ auch $ab \in U$ gilt. Sind dabei $(M, \cdot, e)$ und $(U, \cdot_U, e)$ Gruppen, so heißt U **Untergruppe** von M. Man schreibt jeweils wieder kurz $\cdot$ statt $\cdot_U$. Für eine Untergruppe U von M heißt

$$\mathrm{ord}\, U := \#U \in \mathbb{N} \cup \{\infty\}$$

die **Ordnung** von U.

Satz 3.10 *Es seien $(G,\cdot,e)$ eine Gruppe und $U \subset G$, $U \neq \varnothing$. Dann sind die folgenden Aussagen äquivalent:*

(i) *U ist Untergruppe von G.*

(ii) *$e \in U$ und aus $a,b \in U$ folgt $ab \in U$ sowie $a^{-1} \in U$.*

(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 $ab \in U$.*

Beweis. (i) $\Rightarrow$ (ii): Da U ein Untermonoid ist, gilt $e \in U$ und $ab \in U$ für $a,b \in U$. Außerdem ist $a^{-1} \in U$ aufgrund der Eindeutigkeit der Inversen in G.
(ii) $\Rightarrow$ (i) und (ii) $\Rightarrow$ (iii) sind 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. Sind $x, x' \in U$ und ist $ax = ax'$, so ist $x = a^{-1}ax = a^{-1}ax' = x'$. Also ist die Abbildung

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

injektiv und damit eine Bijektion. Nach Voraussetzung gilt $aU \subset U$, so dass wegen der Endlichkeit von U schon $aU = U$ gelten muss. Ist nun $b \in U$, so existiert ein $x \in U$ mit $b = ax$, 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. Es sei $m \in \mathbb{N}$. Ist $G = (\mathbb{C},+,0)$, so haben wir folgende Kette ineinandergeschachtelter Untergruppen:

$$\{0\} \subset m\mathbb{Z} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}.$$

Sind $G = (\mathbb{C}\setminus\{0\},\cdot,1)$ und $\mathbb{S}_m := \{z \in \mathbb{C} : z^m = 1\}$[21], so haben wir folgende Inklusionen von Untergruppen:

$$\{1\} \subset \left\{ \begin{array}{l} \{-1,1\} \subset \mathbb{Q}\setminus\{0\} \subset \mathbb{R}\setminus\{0\} \\ \mathbb{Q}_+ \subset \mathbb{R}_+ \subset \mathbb{R}\setminus\{0\} \\ \mathbb{S}_m \subset \mathbb{S} := \{z \in \mathbb{C} : |z| = 1\} \end{array} \right\} \subset \mathbb{C}\setminus\{0\}.$$

Bemerkung und Definition 3.12 Ist $(G,\cdot,e)$ eine Gruppe und ist $\mathscr{U}$ eine Menge von Untergruppen, so ist auch $\bigcap_{U\in\mathscr{U}} U$ eine Untergruppe[22], denn es gilt $e \in U$ für alle $U \in \mathscr{U}$ und für $a,b \in \bigcap_{U\subset\mathscr{U}} U$ auch $a^{-1}b \in U$ für alle $U \in \mathscr{U}$.

[21] die Menge der m-ten Einheitswurzeln
[22] Dies gilt auch im Fall von $\mathscr{U} = \varnothing$, in dem $\bigcap_{U\in\mathscr{U}} U := G$ gesetzt ist.

Ist nun M eine beliebige Teilmenge von G und ist $\mathscr{U}_M$ die Menge aller Untergruppen U von G mit $M \subset U$, so heißt

$$\langle M \rangle \;:=\; \bigcap_{U \in \mathscr{U}_M} U$$

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 $\langle \{a\} \rangle$. Man nennt dann a ein **erzeugendes Element** von $\langle a \rangle$ und

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

Ordnung von a. Schließlich heißt G **zyklisch**, falls $\langle a \rangle = G$ für ein $a \in G$ gilt.

Bemerkung 3.13 Es sei G eine Gruppe. Dann ist für $a \in G$ die von a erzeugte Untergruppe abelsch und gegeben durch

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

Denn: Wir setzen $V := \{a^k : k \in \mathbb{Z}\}$. Wegen $a^k a^j = a^{k+j} = a^j a^k$ für $j, k \in \mathbb{Z}$ ist V nach Kriterium 3.10 (ii) eine (abelsche) Untergruppe von G. Da $a \in V$ ist, gilt $V \supset \langle a \rangle$. Andererseits ist $\langle a \rangle$ eine Untergruppe von G, die a enthält. Nach Kriterium 3.10 (iii) ist damit auch $V \subset \langle a \rangle$.

Insbesondere sind zyklische Gruppen stets abelsch.

Beispiele 3.14 1. Es sei $G = (\mathbb{Z}, +, 0)$. Dann gilt $\langle a \rangle = \{ka : k \in \mathbb{Z}\} = \mathbb{Z}a$ 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.

3. Für $G = \mathbb{S} = \exp(i\mathbb{R})$[23] und $\zeta = e^{2\pi \mathrm{i}/m}$ gilt

$$\langle \zeta \rangle = \mathbb{S}_m = \{e^{2\pi i k/m} : k = 0, \ldots, m-1\},$$

wobei $e^{2\pi i k/m} \neq e^{2\pi i j/m}$ für $0 \leq j < k \leq m-1$. Damit ist auch $\mathbb{S}_m$ eine zyklische Gruppe der Ordnung m.

[23] Wir nutzen im Weiteren die komplexe Exponentialfunktion inklusive Eigenschaften; siehe etwa https://www.math.uni-trier.de/~mueller/EinfMathe/Einf_Mathe_GW_WS2020-21.pdf, Abschnitt 6

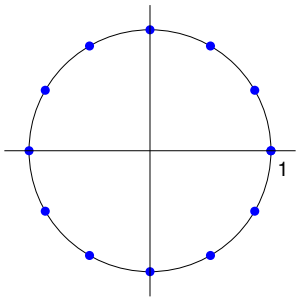


Figure 1: 12-te Einheitswurzeln

Satz 3.15 *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 $x^{k \operatorname{ord}(x)+j} = x^j$ für $k, j \in \mathbb{Z}$. Außerdem ist für $m \in \mathbb{Z}$ die Gleichung $x^m = e$ genau dann erfüllt, wenn $\operatorname{ord}(x) \mid m$ *gilt.*

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 Zusatzbehauptungen: Nach Voraussetzung existiert

$$n_x \quad := \quad \min\{n \in \mathbb{N} : x^n = e\}.$$

Für $k, j \in \mathbb{Z}$ gilt damit

$$x^{kn_x+j} \quad = \quad (x^{n_x})^k x^j \quad = \quad x^j.$$

Ist $m \in \mathbb{Z}$, so ist $m = kn_x + j$ mit $k \in \mathbb{Z}$ und $j \in \{0, \ldots, n_x - 1\}$ nach Satz 2.2 (Division mit Rest). Also ist

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

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

Bemerkung und Definition 3.16 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 schreiben wir

$$G/_U := \{aU : a \in G\}$$

für die Menge der Linksnebenklassen. Damit nennt man $\#(G/_U)$ **Index** von U (in G).[24]

Beispiel 3.17 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 m der Index von $m\mathbb{Z}$ in $\mathbb{Z}$.

Satz 3.18 (**Lagrange**).
Es seien G eine endliche Gruppe und U eine Untergruppe. Dann gilt

$$\operatorname{ord} G = \operatorname{ord} U \cdot \#(G/_U)$$

und insbesondere $\operatorname{ord} U \mid \operatorname{ord} G$.

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

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

□

[24] Man kann sich überlegen, dass der Index auch die Anzahl der Rechtsnebenklassen ist.

Bemerkung 3.19 Sind G eine endliche Gruppe und $x \in G$, so folgt aus dem Satz von Lagrange

$$(\operatorname{ord} x = \operatorname{ord}\langle x\rangle) \mid \operatorname{ord}(G)$$

und mit Satz 3.15 dann auch

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

Insbesondere ergibt sich, dass jede Gruppe G mit $\operatorname{ord}(G) \in \mathbb{P}$ zyklisch ist ([Ü]).

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

Definition 3.20 Die durch

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

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 3.21 (Satz von Euler und kleiner Satz von Fermat)
Ist $m \in \mathbb{N}$, so gilt

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

für alle $a \in \mathbb{Z}$ mit $\operatorname{ggT}(a, m) = 1$. Ist $p \in \mathbb{P}$, so gilt

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

für alle $a \in \mathbb{Z}$ mit $p \nmid a$.

Beweis. Bemerkung 3.19 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 $a^{\varphi(m)} \equiv 1 \mod m$. Ist $p \in \mathbb{P}$ kein Teiler von a, so ist $\operatorname{ggT}(a, p) = 1$, also dann $a^{p-1} = a^{\varphi(p)} \equiv 1 \mod p$. □

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

Satz 3.22 *Es seien $a, b \in \mathbb{Z}$, $m \in \mathbb{N}$ und $d := \operatorname{ggT}(a, m)$. Dann hat die Gleichung*

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

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

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

erfüllt ist. Zudem gilt: Ist $x \in \mathbb{Z}$ eine Lösung von (3.2), so ist

$$L_x := \{x + km/d : k = 0, \ldots, d-1\}$$

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. 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 2.6.

Ist nun d Teiler von b, so gilt für $x \in \mathbb{Z}$ die Äquivalenzkette

$$x \text{ löst (3.1)} \;\Leftrightarrow\; m \mid (ax - b) \;\Leftrightarrow\; \frac{m}{d} \mid \left(\frac{a}{d}\, x - \frac{b}{d}\right) \;\Leftrightarrow\; x \text{ löst (3.2)}.$$

Sind schließlich x Lösung von (3.2) und $y \in \mathbb{Z}$, so löst y die Gleichung (3.2) genau dann, wenn $[y]_{m/d} = [x]_{m/d}$ gilt, und dies ist nach Division mit Rest genau dann der Fall, wenn

$$y \in x + \frac{m}{d}\mathbb{Z} = x + m\mathbb{Z} + \frac{m}{d}\{0, \ldots, d-1\} = L_x + m\mathbb{Z}$$

gilt. 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 $\#L_x = d$. Die letzte Aussage ist dann geschenkt. □

Beispiele 3.23 Wir betrachten $m = 27$, $a = 6$, also $d = \mathrm{ggT}(6, 27) = 3$, und die Kongruenz

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

Für $b = 3$ ist nach Satz 3.22 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). Für $b = 2$ existiert nach Satz 3.22 wegen $(\mathrm{ggT}(6, 27) = 3) \nmid 2$ keine Lösung.

Von grundlegender Bedeutung ist das folgende Ergebnis über simultane Kongruenzen.

Satz 3.24 *Es seien $m_1, \ldots, m_N \in \mathbb{N}$ paarweise teilerfremd und $m := \prod_{j=1}^{N} m_j$. Dann gilt*

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 $f([x]_m) := ([x]_{m_1}, \ldots, [x]_{m_n})$ für $[x]_m \in \mathbb{Z}_m$ ist eine Bijektion von $\mathbb{Z}_m$ auf $\mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_N}$ definiert.*
3. (**Chinesischer Restsatz**)[25] *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 $x + m\mathbb{Z}$.

Beweis. 1. Aus $m \mid (x - x')$ folgt natürlich $m_j \mid (x - x')$ für $j = 1, \ldots, N$. Die umgekehrte Aussage ergibt sich unter Verwendung der paarweisen Teilerfremdheit der m_j induktiv mit Satz 2.8.2./3.

2. Nach 1. ist f wohldefiniert und injektiv. Wegen
$$\#(Z_{m_1} \times \ldots \times \mathbb{Z}_{m_N}) == \prod_{j=1}^{N} \#\mathbb{Z}_{m_j} = \prod_{j=1}^{N} m_j = m = \#\mathbb{Z}_m < \infty$$
ist f auch surjektiv.

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

Bemerkung 3.25 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:

Für $k \in \{1, \ldots, N\}$ sei mit der Notation und den Voraussetzungen von Satz 3.24
$$a_k := \frac{m}{m_k} = \prod_{j \neq k} m_j \,.$$

[25] 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 3.26.

Induktive Anwendung von Satz 2.8.3 ergibt $\mathrm{ggT}(a_k, m_k) = 1$, so dass nach Satz 3.22 (oder dem Lemma von Bézout) ein $x_k \in \mathbb{Z}$ existiert mit

$$a_k x_k \equiv b_k \mod m_k.$$

Wir setzen nun

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

Für $j \in \{1, \ldots, N\}$ und $k \neq j$ ist $a_k x_k \equiv 0 \mod m_j$ wegen $m_j \mid a_k$ und damit

$$x \equiv a_j x_j \equiv b_j \mod m_j,$$

d. h. x eine Lösung von (3.3).

Beispiel 3.26 Wir betrachten das System simultaner Kongruenzen

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

mit $m_1 = 3$, $m_2 = 5$, $m_3 = 7$ und $m = 105$. In der Notation von Bemerkung 3.25 ist hier $a_1 = 35$, $a_2 = 21$, $a_3 = 15$. Lösungen $x_1, x_2, x_3 \in \mathbb{Z}$ der 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 etwa $x_1 = 1$, $x_2 = 3$, $x_3 = 2$. 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 3.27 Nach dem kleinen Satz von Fermat (Satz 3.21) 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**. Falls also Carmichaelzahen existieren, kann man obigen Ansatz nicht ohne Weiteres nutzen, um von einer Zahl nachzuweisen, dass sie prim ist.[26]

Wir zeigen, dass Carmichaelzahlen existieren. Dazu beweisen wir zunächst folgendes hinreichende Kriterium,[27] wobei wir $E(n) := \{p \in \mathbb{P} : p \mid n\}$ setzen.

Satz 3.28 *Es sei* $1 < n \in \mathbb{N}$ *mit* $(p-1) \mid (n-1)$ *und* $\alpha_p(n) = 1$ *für alle* $p \in E(n)$.[28] *Dann ist* n *eine Carmichael-Zahl.*

Beweis. Es sei $a > 1$ mit $\mathrm{ggT}(a,n) = 1$. Ist $p \in E(n)$, so ist auch $\mathrm{ggT}(a,p) = 1$. Nach Voraussetzung existiert ein $k \in \mathbb{N}$ mit $n - 1 = k(p-1)$. Aus dem kleinen Satz von Fermat (Satz 3.21) folgt

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

Wegen $\alpha_p(n) = 1$ liefert Satz 3.24.1 nun $a^{n-1} \equiv 1 \mod n$. □

Beispiel 3.29 Für $3 \cdot 11 \cdot 17 = 561$ gilt $2 \mid 560, 10 \mid 560$ und $16 \mid 560$. Also ist 561 nach Satz 3.28 eine Carmichael-Zahl (und genauer die kleinste).[29]

Bemerkung 3.30 Wir betrachten wieder f aus Satz 3.24, jetzt im Zusammenhang mit primen Restklassen. Es gilt: Die Restriktion $f|_{\mathbb{Z}_m^*}$ ist eine Bijektion von $\mathbb{Z}_m^*$ auf $\mathbb{Z}_{m_1}^* \times \ldots \times \mathbb{Z}_{m_N}^*$.

> Denn: Für $x \in \mathbb{Z}$ gilt $[x]_m \in \mathbb{Z}_m^*$ genau dann, wenn $\mathrm{ggT}(m,x) = 1$ ist und $[x]_{m_j} \in \mathbb{Z}_{m_j}^*$ genau dann, wenn $\mathrm{ggT}(m_j,x) = 1$ ist (siehe Bemerkung und Definition 3.5). Mit Satz 2.8.3, induktiv angewandt, folgt, dass $\mathrm{ggT}(m,x) = 1$ genau dann gilt, wenn $\mathrm{ggT}(m_j,x) = 1$ für $j = 1, \ldots, N$ ist. Also ist $f([x]_m) \in \mathbb{Z}_{m_1}^* \times \ldots \times \mathbb{Z}_{m_N}^*$ genau dann, wenn $[x]_m \in \mathbb{Z}_m^*$ gilt. Da f injektiv ist, folgt die Behauptung.

[26] 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.

[27] Es gilt auch die Umkehrung; siehe etwa O. Forster, Algorithmische Zahlentheorie, Springer, Wiesbaden, 2015.

[28] n ist eine quadratfreie Zahl; siehe [Ü]

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

Definition 3.31 Eine Funktion $\varphi : \mathbb{N} \to \mathbb{N}$ heißt **(zahlentheoretisch) multiplikativ**, falls für jedes $N \in \mathbb{N}$ und paarweise teilerfremde $m_1, \ldots, m_N$

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

gilt.

Satz 3.32 *Die Eulersche φ-Funktion ist multiplikativ und für $n \in \mathbb{N}$ gilt*

$$\varphi(n) = n \cdot \prod_{p|n} \Big(1 - \frac{1}{p}\Big)$$

Beweis. 1. Wir schreiben wieder $m := \prod_{j=1}^{N} m_j$. Unter Benutzung von Bemerkung 3.30 für die zweite Gleichheit erhält man

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

2. Sind $k \in \mathbb{N}$ und $p \in \mathbb{P}$, so gilt $\varphi(p^k) = p^k - p^{k-1}$ wegen

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

Ist nun $n = \prod_{p|n} p^{\alpha_p(n)} \in \mathbb{N}$, so erhalten wir mit 1. wegen der Teilerfremdheit von p^j und q^k für unterschiedliche Primzahlen p, q und beliebige Exponenten j, k

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

□

Wir wenden zum Abschluss dieses Abschnitts einer Anwendung der vorhergehenden Theorie im Bereich der Kryptographie zu.[30] Diese basiert auf folgender Beobachtung

Bemerkung 3.33 Es seien $p, q \in \mathbb{P}$ mit $p \neq q$ und

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

[30] Tatsächlich brauchen wir im Grunde genommen nur den kleinen Sat von Fermat, so dass man diesen Teil auch schon dort behandeln könnte.

Dabei ist $m = \varphi(pq) = \varphi(n)$, was wir aber nicht verwenden. Ist $a \in \mathbb{N}$ teilerfremd zu m, so existiert nach Bemerkung und Definition 3.5 genau ein $b \in \{1, \ldots, m-1\}$ mit $[b]_m = ([a]_m)^{-1}$, also $ab \equiv 1 \mod m$.

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

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

Es sei nun $x \in \mathbb{Z}$ beliebig. Unter Verwendung des Satzes von Fermat (Satz 3.21) im ersten Fall des dritten Schrittes, ergibt sich

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

Analog erhalten wir $(x^a)^b \equiv x \mod q$. Wegen der Teilerfremdheit von p, q folgt mit Satz 3.24.1 schließlich

$$(x^a)^b \equiv x \mod n. \tag{3.4}$$

Bemerkung 3.34 (Prinzip der RSA-Kryptographie)

Das RSA-Verfahren[31], ein sogenanntes asymmetrisches Verschlüsselungsverfahren, beruht auf folgenden Grundgedanken

- Der Empfänger E wählt p, q, a, b wie im Bemerkung 3.33 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

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

- E berechnet daraus

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

  also x wegen (3.4)

Wesentlich dabei: Für große p, q ist m und damit auch b aus der Kenntnis von n und a mit derzeit bekannten Verfahren praktisch nicht berechenbar.[32] Bemerkenswert ist dabei, dass es auf der anderen Seite effiziente Algorithmen zur Primfaktorzerlegung für Quantencomputer bereits gibt.[33]

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

[32] Weitere Informationen und Beispiele findet man etwa unter https://de.wikipedia.org/wiki/RSA-Kryptosystem oder auch https://www.scai.fraunhofer.de/de/mediathek/material-fuer-mathematik-unterricht.html.

[33] siehe etwa https://de.wikipedia.org/wiki/Shor-Algorithmus

4 Ebene Geometrie

Wir wollen in diesem Abschnitt die Grundlagen der in der Schule betrachteten klassischen euklidschen Ebene in Ansätzen untersuchen. Wir starten mit einem axiomatischen Zugang zu ebenen Geometrien und werden sehen, dass das Parallelenaxiom eine wesentliche Rolle spielt. Ohne dieses Axiom gelangt man in natürlicher Weise zu nichteuklidschen Geometrien.

Definition 4.1 Es seien P ein nichtleere Menge und $\mathcal{G} \subset \mathscr{P}(P)$ nichtleer. Das Paar $(P, \mathcal{G})$ heißt **Inzidenzgeometrie**, falls gilt

(I1) Zu jedem Paar $(a, b) \in P \times P$ mit $a \neq b$ existiert genau ein $G \in \mathcal{G}$ mit $a \in G$ und $b \in G$. Man schreibt dann $G(a, b) := ab := G$.

(I2) Jedes $G \in \mathcal{G}$ ist mindestens zweielementig.

In dem Fall nennt man Elemente von P **Punkt**e. Elemente G von $\mathcal{G}$ nennt man **Gerade**n. Liegen mehrere Punkte auf einer Gerade, so nennt man sie **kollinear**. Drei Punkte a, b, c heißen **in allgemeiner Lange**, falls sie nicht kollinear sind. Gilt zusätzlich

(I3) Es existieren $a, b, c \in P$ in allgemeiner Lage,

so nennt man $(P, \mathcal{G})$ auch eine **Inzidenzebene**. Schießlich (und wichtig) heißen zwei Geraden G, H **parallel**, falls $G = H$ oder $G \cap H = \varnothing$ gilt. Man schreibt dann $G \parallel H$ und sagt auch, H sei eine **Parallele** zu G. Eine Inzidenzgeometrie heißt **affine Geometrie**, falls das **Parallelenaxiom**

(P) Zu jedem Paar $(p, G) \in P \times \mathcal{G}$ existiert *genau* eine Parallele H zu G mit $p \in H$

erfüllt ist.

Bevor wir zur euklidschen Ebene als Standardfall einer affinen Geometrie kommen, definieren wir noch kurz affine Räume.

Bemerkung und Definition 4.2 Es seien P eine nichtleere Menge und $V = V(+, \cdot)$ ein $\mathbb{R}$-Vektorraum $\neq \{0\}$. Weiter sei $\rightarrow\colon P \times P \to V$ eine Abbildung mit folgenden Eigenschaften, wobei wir $\overrightarrow{ab} := \rightarrow (a, b)$ für $a, b \in P$ schreiben:

(A1) (Dreiecksregel) Für beliebige $a, b, c \in P$ gilt $\overrightarrow{ab} + \overrightarrow{bc} = \overrightarrow{ac}$.

(A2) (Abtragbarkeitsregel) Zu jedem $(a, \mathbf{v}) \in P \times V$ existiert genau ein Punkt $b \in P$ mit $\mathbf{v} = \overrightarrow{ab}$.[34]

[34] Man nennt dann $\overrightarrow{ab}$ Verbindungsvektor von a nach b.

Dann heißt $(P, V, \to)$ ein **affiner Raum**. In einem affinen Raum ist durch

$$(a, \mathbf{v}) \mapsto b =: a + \mathbf{v},$$

wobei b wie in (A2) ist, eine Abbildung $+ : P \times V \to P$ [35] definiert mit

$$a + \overrightarrow{ab} = b.$$

Sind $a \in P$, $\mathbf{u} \in V \setminus \{0\}$ und ist $G \subset P$ von der Form

$$G = G_{\mathbf{u}}(a) := a + \mathbb{R}\mathbf{u} = \{a + \lambda\mathbf{u} : \lambda \in \mathbb{R}\},$$

so heißt G eine **affine Gerade** oder kurz **Gerade** in P durch a. Weiter nennt man $\mathbf{u}$ einen **Richtungsvektor** von G.

Ist speziell $P = V$, so wird $(V, V, \to)$ durch

$$\overrightarrow{ab} := b - a \qquad (a, b \in V)$$

zu einem affinen Raum. Sind $a' \in V$ und $\mathbf{u}' \in V \setminus \{0\}$, so ist $G_{\mathbf{u}'}(a') = G_{\mathbf{u}}(a)$ genau dann, wenn $a' \in G_u(a)$ gilt und $\mathbf{u}', \mathbf{u}$ linear abhängig sind. Insbesondere ist $\overrightarrow{ab}$ für alle $b \in G_{\mathbf{u}}(a) \setminus \{a\}$ ein Richtungsvektor von $G_{\mathbf{u}}(a)$. Für einen Punkt $p \in V$ gilt $p \notin G_{\mathbf{u}}(a)$ genau dann, wenn $\mathbf{u}$ und $\overrightarrow{pb}$ linear unabhängig sind für alle $b \in G_{\mathbf{u}}(a)$. Man sieht damit ([Ü]), dass $(V, \mathcal{G})$ mit $\mathcal{G} := \{G_{\mathbf{u}}(a) : a \in V, u \in V \setminus \{0\}\}$ eine Inzidenzgeometrie ist mit

$$G(a, b) = G_{\overrightarrow{ab}}(a).$$

Im Fall $\dim V \geq 2$ ist auch (I3) erfüllt. Außerdem gilt: Ist $G = G_{\mathbf{u}}(a)$ eine Gerade in V und ist $p \notin G$, so existiert kein Paar $(\lambda, \mu) \in \mathbb{R}^2$, das die Gleichung

$$p + \lambda\mathbf{u} = a + \mu\mathbf{u}$$

löst (sonst wäre $\overrightarrow{pa} = a - p = (\lambda - \mu)\mathbf{u}$). Damit sind G und $G_{\mathbf{u}}(p)$ disjunkt, also parallel.

Bemerkung und Definition 4.3 Ist $(V, +, \cdot) = (\mathbb{R}^n, +, \cdot)$ der n-dimensionale euklidsche Raum, so schreiben wir kurz $\mathbb{E}^n$ für $\mathbb{R}^n$ aufgefasst als affiner Raum $(\mathbb{R}^n, \mathbb{R}^n, \to)$. Nach Bemerkung und Definition 4.2 ist $(\mathbb{E}^n, \mathcal{G})$ mit $\mathcal{G}$ wie dort eine Inzidenzgeometrie und im Fall $n \geq 2$ ist auch (I3) erfüllt. Weiter nennt man für $a, b \in \mathbb{E}^n$

$$\overline{ab} := a + [0, 1]\overrightarrow{ab}$$

die **Strecke** zwischen a und b und

$$|\overline{ab}| := \|\overrightarrow{ab}\|_2,$$

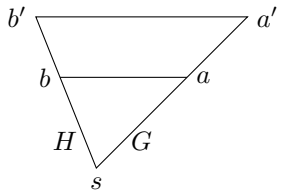
wobei $\|\cdot\|_2$ die euklidsche Norm bezeichnet, die **Länge** von $\overline{ab}$. Dabei ist $\overline{ab} = \overline{ba}$.

[35] Man beachte, dass $+$ keine innere Verknüpfung ist.

Bemerkung und Definition 4.4 (euklidsche Ebene) Wir betrachten den Fall $n = 2$ und schreiben kurz $\mathbb{E} := \mathbb{E}^2$. Man nennt $\mathbb{E}$ die **euklidsche Ebene**. Es sei $G = G_{\mathbf{u}}(p)$ eine Gerade in $\mathbb{E}$. Ist H eine zu $G_{\mathbf{u}}(p)$ verschiedene Gerade durch p, so ist $H = G_{\mathbf{v}}(p)$ für ein $\mathbf{v} \neq 0$ und $\mathbf{u}, \mathbf{v}$ sind linear unabhängig. Damit ist $(\mathbf{u}, \mathbf{v})$ eine Basis von $\mathbb{R}^2$. Sind $\lambda, \mu \in \mathbb{R}$ mit $a - p = \overrightarrow{pa} = \lambda\mathbf{v} - \mu\mathbf{u}$, so ist $p + \lambda\mathbf{v} = a + \mu\mathbf{u}$. Also ist $G \cap H \neq \varnothing$. Wegen $p \notin G$ sind G und H nicht parallel. Mit Bemerkung und Definition 4.2 gilt damit:

Zu jeder Geraden $G = G_{\mathbf{u}}(a)$ und jedem Punkt p gibt es *genau* eine zu G parallele Gerade durch p, nämlich $G_{\mathbf{u}}(p)$. Damit ist $\mathbb{E}$ eine affine Geometrie. [36]

Von grundlegender Bedeutung in der ebenen euklidschen Geometrie sind die Strahlensätze.



Satz 4.5 (erster und zweiter Strahlensatz)
Es seien $G, H \subset \mathbb{E}$ Geraden mit $G \cap H = \{s\}$. Weiter seien $a, a' \in G$, $b, b' \in H$ paarweise verschiedene Punkte $\neq s$. Sind die Geraden $G(a, b)$ und $G(a', b')$ parallel, so existiert ein $\sigma \in \mathbb{R}$ mit

$$\overrightarrow{sa'} = \sigma \cdot \overrightarrow{sa}, \quad \overrightarrow{sb'} = \sigma \cdot \overrightarrow{sb} \quad \textit{und} \quad \overrightarrow{a'b'} = \sigma \cdot \overrightarrow{ab}.$$

Insbesondere gilt

$$\frac{|\overline{sb'}|}{|\overline{sb}|} = \frac{|\overline{sa'}|}{|\overline{sa}|} = \frac{|\overline{a'b'}|}{|\overline{ab}|}.$$

Beweis. 1. Es seien $\lambda, \lambda' \in \mathbb{R} \setminus \{0\}$ so, dass $\overrightarrow{sa} = \lambda \cdot \overrightarrow{sa'}$ und $\overrightarrow{sb} = \lambda' \cdot \overrightarrow{sb'}$. Wegen $G(a, b) \parallel G(a', b')$ existiert ein $\mu \in \mathbb{R} \setminus \{0\}$ mit $\overrightarrow{ab} = \mu \cdot \overrightarrow{a'b'}$. Dann ist auch

$$\begin{aligned} \mu(b' - s) - \mu(a' - s) &= \mu(b' - a') = b - a = (b - s) - (a - s) \\ &= \lambda'(b' - s) - \lambda(a' - s). \end{aligned}$$

[36] Verzichtet man auf das Parallelenaxiom, so gelangt man zu nichteuklidschen Geometrien wie etwa der hyperbolischen Ebene, die ansonsten einem – durchaus beeindruckenden – Satz an weiteren Axiomen in Analogie zur euklidschen Ebene genügt. Näheres findet man etwa in den Lehrbüchern Agricola, I., Friedrich T., Elementargeometrie, 4., überarbeitete Auflage, Springer Spektrum, 2015, Kapitel 3. und Smoczyk, K., Geometrie für das Lehramt, BoD, 2019; siehe auch https://en.wikipedia.org/wiki/Poincare_disk_model.

Da $b' - s = \overrightarrow{sb'}$ und $a' - s = \overrightarrow{sa'}$ linear unabhängig sind, folgt $\mu = \lambda' = \lambda$ und damit auch $|\overline{sa'}|/|\overline{sa}| = 1/|\lambda| = 1/|\lambda'| = |\overline{sb'}|/|\overline{sb}|$.

2. Mit $\sigma := 1/\lambda = 1/\lambda'$ gilt simultan $\overrightarrow{sa'} = \sigma \cdot \overrightarrow{sa}$ und $\overrightarrow{sb'} = \sigma \cdot \overrightarrow{sb}$. Dann ist aber auch

$$\overrightarrow{a'b'} = \overrightarrow{sb'} - \overrightarrow{sa'} = \sigma(\overrightarrow{sb} - \overrightarrow{sa}) = \sigma \cdot \overrightarrow{ab}$$

und damit $|\overline{sa'}|/|\overline{sa}| = |\sigma| = |\overline{a'b'}|/|\overline{ab}|$. □

Bemerkung und Definition 4.6 Wir schreiben $\langle \cdot, \cdot \rangle$ für das kanonische Skalarprodukt in $\mathbb{R}^n$, also

$$\langle \mathbf{u}, \mathbf{v} \rangle := \mathbf{u}^T \mathbf{v} = \sum_{j=1}^{n} u_j v_j \quad (\mathbf{u} = (u_1, \ldots, u_n), \mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{R}^n).$$

Dann ist $\langle u, u \rangle = \|u\|_2^2$ und es gilt die Cauchy-Schwarzsche Ungleichung[37]

$$|\langle \mathbf{u}, \mathbf{v} \rangle| \leq \|\mathbf{u}\|_2 \cdot \|\mathbf{v}\|_2 \quad (\mathbf{u}, \mathbf{v} \in \mathbb{R}^n).$$

Dabei gilt Gleichheit genau dann, wenn $\mathbf{u}, \mathbf{v}$ linear abhängig sind. Die Vektoren $\mathbf{u}, \mathbf{v}$ heißen **senkrecht** zueinander, falls $\langle \mathbf{u}, \mathbf{v} \rangle = 0$ gilt. Man schreibt dann $\mathbf{u} \perp \mathbf{v}$. Außerden schreibt man $\mathbf{u} \perp M$ für eine Menge $M \subset \mathbb{R}^n$, falls $\mathbf{u} \perp \mathbf{v}$ für alle $\mathbf{v} \in M$ gilt.

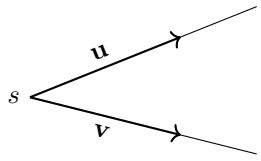


Figure 2: Winkel mit Scheitel s

Bemerkung und Definition 4.7 Es seien $p \in \mathbb{E}$ und $\mathbf{u} \in \mathbb{R}^2 \setminus \{0\}$. Die Menge $S_{\mathbf{u}}(p) := p + [0, \infty)\mathbf{u}$ wird **Strahl** mit Startpunkt p und Richtung $\mathbf{u}$ genannt. Sind $s \in \mathbb{E}$ und $\mathbf{u}, \mathbf{v} \in \mathbb{R}^2 \setminus \{0\}$, so nennt man

$$\angle_{\mathbf{u},\mathbf{v}}(s) := S_{\mathbf{u}}(s) \cup S_{\mathbf{v}}(s)$$

Winkel [38] mit **Scheitel** s und den **Schenkeln** $S_{\mathbf{u}}(s)$, $S_{\mathbf{v}}(s)$.

[37] siehe Lineare Algebra; vgl. https://de.wikipedia.org/wiki/Cauchy-Schwarzsche_Ungleichung

[38] Man beachte, dass ein Winkel eine Menge in $\mathbb{E}$ ist.

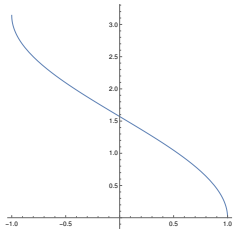


Figure 3: arccos

Nach der Cauchy-Schwarzschen Ungleichung ist $\langle \mathbf{u}, \mathbf{v} \rangle / (\|\mathbf{u}\|_2 \, \|\mathbf{v}\|_2) \in [-1, 1]$. Die Zahl

$$\measuredangle_{\mathbf{u},\mathbf{v}}(s) := \arccos\left(\frac{\langle \mathbf{u}, \mathbf{v} \rangle}{\|\mathbf{u}\|_2 \, \|\mathbf{v}\|_2}\right) \in [0, \pi]$$

heißt **Winkelweite** des Winkels. Insbesondere ist damit $\measuredangle_{\mathbf{u},\mathbf{v}}(s) = \pi/2$ genau dann, wenn $\mathbf{u} \perp \mathbf{v}$ gilt. Der Winkel heißt in diesem Fall ein **rechter Winkel**. Die Winkelweite ist genau dann 0, wenn $\mathbf{u} = \lambda \, \mathbf{v}$ mit $\lambda > 0$ ist, und genau dann π, wenn $\mathbf{u} = \lambda \, \mathbf{v}$ mit $\lambda < 0$ gilt. Wegen $\arccos(-t) = \pi - \arccos t$ gilt allgemein

$$\measuredangle_{-\mathbf{u},\mathbf{v}}(s) = \measuredangle_{\mathbf{u},-\mathbf{v}}(s) = \pi - \measuredangle_{\mathbf{u},\mathbf{v}}(s).$$

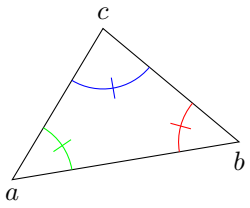


Figure 4: Dreieck $\Delta(a, b, c)$ mit Innenwinkeln α (grün), β (rot) und γ (blau)

Definition 4.8 Sind $a, b, c \in \mathbb{E}$ nicht kollinear, so heißt

$$\Delta(a, b, c) := \overline{ab} \cup \overline{bc} \cup \overline{ca}$$

ein **Dreieck**. Dabei nennt man a, b, c die **Ecken** und die Stecken $\overline{ab}, \overline{bc}, \overline{ca}$ die **Seiten** von $\Delta(a, b, c)$. Wir schreiben im Weiteren kurz $A := |\overline{bc}|$, $B := |\overline{ca}|$ sowie $C := |\overline{ab}|$. Außerdem schreiben wir α bzw. β bzw. γ für die Winkelweiten der Winkel $\measuredangle_{\overrightarrow{ac},\overrightarrow{ab}}(a)$ bzw. $\measuredangle_{\overrightarrow{ba},\overrightarrow{bc}}(b)$ bzw. $\measuredangle_{\overrightarrow{ca},\overrightarrow{cb}}(c)$. Diese Winkelweiten nennt man auch **Innenwinkelweiten** oder kurz **Innenwinkel** des Dreiecks. Die Winkelweiten $\pi - \alpha$, $\pi - \beta$ und $\pi - \gamma$ nennt man **Außenwinkelweiten**.

Satz 4.9 (Kosinussatz und Satz von Pythagoras)
Für jedes Dreieck $\Delta(a,b,c)$ gilt [39]

$$C^2 = A^2 + B^2 - 2AB \cdot \cos\gamma.$$

Insbesondere ist $\gamma = \pi/2$ genau dann, wenn

$$C^2 = A^2 + B^2.$$

Beweis. Sind $\mathbf{u}, \mathbf{v} \in \mathbb{R}^2$, so gilt

$$\|\mathbf{u} - \mathbf{v}\|_2^2 = \langle \mathbf{u} - \mathbf{v}, \mathbf{u} - \mathbf{v}\rangle = \|\mathbf{u}\|_2^2 - 2\langle \mathbf{u}, \mathbf{v}\rangle + \|\mathbf{v}\|_2^2.$$

Wegen $\overrightarrow{ab} = \overrightarrow{ac} + \overrightarrow{cb} = \overrightarrow{ac} - \overrightarrow{bc}$ ergibt sich mit $\mathbf{u} = \overrightarrow{ac}$ und $\mathbf{v} = \overrightarrow{bc}$

$$|\overline{ab}|^2 = |\overline{ac}|^2 + |\overline{bc}|^2 - 2\langle \overrightarrow{ac}, \overrightarrow{bc}\rangle = |\overline{ac}|^2 + |\overline{bc}|^2 - 2|\overline{ac}| \cdot |\overline{bc}| \cdot \cos\gamma.$$

Die zweite Aussage ergibt sich daraus, dass $\cos\gamma = 0$ für $\gamma \in [0,\pi]$ genau dann gilt, wenn $\gamma = \pi/2$ ist. □

Als wichtige Folgerung des Kosinussatzes ergibt sich

Satz 4.10 (Außenwinkelsatz)
Ist $\Delta(a,b,c)$ ein Dreieck, so gilt[40]

$$\alpha < \min\{\pi - \beta, \pi - \gamma\}.$$

Beweis. Nach dem Kosinussatz (angewandt mit α bzw. β statt γ) ist

$$2BC\cos\alpha = B^2 + C^2 - A^2 \quad \text{und} \quad 2AC\cos\beta = A^2 + C^2 - B^2,$$

also

$$2ABC(\cos\alpha + \cos\beta) = (A+B)(C^2 - (A-B)^2).$$

Da $\overrightarrow{ac}$, $\overrightarrow{cb}$ linear unabhängig sind, gilt nach der Cauchy-Schwarzschen Ungleichung $|\langle \overrightarrow{ac}, \overrightarrow{cb}\rangle| < AB$. Also folgt mit $\overrightarrow{ac} + \overrightarrow{cb} = \overrightarrow{ab}$

$$(A-B)^2 = A^2 + B^2 - 2AB < A^2 + B^2 + 2\langle \overrightarrow{ac}, \overrightarrow{cb}\rangle = \|\overrightarrow{ac} + \overrightarrow{cb}\|_2^2 = C^2$$

und damit $\cos\alpha + \cos\beta > 0$. Wegen $\cos(\pi - \beta) = -\cos\beta$ ist $\cos\alpha > \cos(\pi - \beta)$. Da cos in $[0,\pi]$ streng fallend ist, folgt $\alpha < \pi - \beta$. Entsprechend argumentiert man mit γ statt β. □

[39] entsprechende Aussagen gelten für die Winkel α und β.
[40] Entsprechende Aussagen gelten natürlich für β und γ.

Bemerkung und Definition 4.11 Ein Dreieck heißt **gleichschenklig**, falls *zwei* Seiten gleiche Länge haben.[41] Aus dem Kosinussatz ergibt sich, dass ein Dreieck genau dann gleichschenklig ist, wenn die den gleichlangen Seiten entsprechenden Winkel gleiche Weite haben.

Denn: Ist etwa $A = B$, so ist nach dem Kosinussatz

$$\cos\alpha = C/(2B) = C/(2A) = \cos\beta$$

und damit $\alpha = \beta$ wegen $\alpha, \beta \in [0, \pi]$. Ist umgekehrt etwa $\cos\alpha = \cos\beta$, so erhält man wie im Beweis zum Außenwinkelsatz mit Differenzbildung statt Addition

$$0 = 2ABC(\cos\alpha - \cos\beta) = (A - B)(C^2 - (A + B)^2).$$

Da nach der Dreiecksungleichung $C < A + B$ gilt, ist $A = B$.

Bemerkung 4.12 Aus dem Außenwinkelsatz erhält man den für die euklidsche Ebene charakteristischen **Winkelsummensatz**:[42] Ist $\Delta(a, b, c)$ ein Dreieck, so gilt

$$\alpha + \beta + \gamma = \pi.$$

Auf einen Beweis, der im Wesentlichen geometrischem Charakter hat, gehen wir in den Übungen ein.

Nach dem Winkelsummensatz hat ein Dreieck höchstens einen rechten Innenwinkel, d. h. einen Innenwinkel mit Wert $\pi/2$. Ein Dreieck heißt **rechtwinklig**, falls ein solcher Winkel existiert. Als Konsequenz des Satzes von Pythagoras leiten wir klassische Ergebnisse im Zusammenhang mit rechtwinkligen Dreiecken her. Vorbereitend führen wir weitere Begriffe der ebenen Geometrie ein.

Bemerkung und Definition 4.13 Es sei $G = G_{\mathbf{u}}(a)$ eine Gerade in $\mathbb{E}$. Ein Vektor $\mathbf{n} \neq 0$ heißt **Normalenvektor** von G, falls $\mathbf{n} \perp \mathbf{u}$ gilt. Damit ist

$$G_{\mathbf{u}}(a) = \{x \in \mathbb{E} : \langle \overrightarrow{ax}, \mathbf{n} \rangle = 0\}.$$

Normiert man $\mathbf{n}$ auf Länge 1, ersetzt man also $\mathbf{n}$ durch $\mathbf{n}/\|\mathbf{n}\|_2$, so spricht auch von der Hesseschen Normal(en)form der Gerade G. Der Vektor $\mathbf{n}$ ist dann bis auf Vorzeichen eindeutig festgelegt.

[41] Sind alle drei Seiten gleich lang, so nennt man das Dreieck gleichseitig.

[42] Bei hyperbolischen Dreiecken ist die Winkelsumme kleiner als π; siehe etwa https://en.wikipedia.org/wiki/Hyperbolic_triangle, bei sphärischen ist sie größer als π; siehe etwa https://en.wikipedia.org/wiki/Spherical_geometry.

Es sei nun $p \notin G$. Ist $\mathbf{v} = \overrightarrow{ap}$, so sind $\mathbf{u}, \mathbf{v}$ linear unabhängig. Dann ist

$$\mathbf{n} := \mathbf{v} - \|\mathbf{u}\|^{-2}\langle \mathbf{v}, \mathbf{u}\rangle \mathbf{u}$$

ein Normalenvektor von G. Man nennt damit die Gerade $G_{\mathbf{n}}(p)$ **senkrechtes Lot** auf G durch p. Der Schnittpunkt s von G und $G_{\mathbf{n}}(p)$ heißt **Lotfußpunkt** von p bzgl. G. Da $G \neq G_{\mathbf{n}}(p)$ ist, ist s eindeutig festgelegt. Außerdem ist $D := |\overline{sp}|$ nach dem Satz von Pythagoras der Abstand von p zur Gerade G, d. h. $D = \min\{|\overline{bp}| : b \in G\}$.

Ist $\Delta(a, b, c)$ ein Dreieck mit α, $\beta < \pi/2$, so liegt der Lotfußpunkt s von c bzgl. $G(a, b)$ in $\overline{ab} \setminus \{a, b\}$, denn sonst wäre die Winkelsumme eines der beiden Dreiecke $\Delta(a, s, c)$, $\Delta(b, s, c)$ größer als π. Man nennt $H := |\overline{sc}|$ die **Höhe** der Ecke c. Zudem setzen wir $P := |\overline{as}|$ und $Q := |\overline{sb}|$.

Satz 4.14 (Höhensatz und Kathetensatz von Euklid)
Es sei $\Delta(a, b, c)$ ein Dreieck mit α, $\beta < \pi/2$. Dann gilt

$$H^2 = PQ + AB\cos\gamma, \quad B^2 = PC + AB\cos\gamma \quad \textit{und} \quad A^2 = QC + AB\cos\gamma.$$

Insbesondere ist $\gamma = \pi/2$ genau dann, wenn

$$H^2 = PQ, \quad B^2 = PC \quad \textit{und} \quad A^2 = QC.$$

Beweis. Wir setzen zur Abkürzung $d := AB\cos\gamma$. Wegen $A^2 + B^2 = C^2 + 2d$ und $P + Q = C$ gilt

$$\begin{aligned}(A^2 - Q^2) + (B^2 - P^2) &= C^2 - P^2 - Q^2 + 2d \\ &= (P + Q)^2 - P^2 - Q^2 + 2d = 2PQ + 2d.\end{aligned}$$

Da $\Delta(a, s, c)$ und $\Delta(s, b, c)$ rechte Winkel an s haben, folgt aus dem Satz von Pythagoras $B^2 = H^2 + P^2$ und $A^2 = H^2 + Q^2$. Damit ist zunächst $2H^2 = 2PQ + 2d$, also $H^2 = PQ + d$, und dann auch $B^2 = PQ + P^2 + d = PC + d$ sowie $A^2 = PQ + Q^2 + d = QC + d$. □

Sind $m \in \mathbb{E}$ und $r > 0$, so schreiben wir

$$K_r(m) :== \{a \in \mathbb{E} : |\overline{am}| = r\} \subset \mathbb{E}$$

für den **Kreis** mit **Mittelpunkt** m und **Radius** r. Ein weiterer Klassiker der euklidschen Geometrie ist

Satz 4.15 (Thales)
Es seien $a, b \in \mathbb{E}$ verschieden, $m := (a + b)/2$ der Mittelpunkt der Stecke $\overline{ab}$ und $r := |\overline{ma}|$. Ist $c \notin G(a, b)$, so ist $c \in K_r(m)$ genau dann, wenn der Winkel γ des Dreiecks $\Delta(a, b, c)$ ein rechter ist.

Beweis. Wegen $\overrightarrow{mb} = -\overrightarrow{ma}$ gilt

$$AB\cos\gamma = \langle\overrightarrow{ca}, \overrightarrow{cb}\rangle = \langle\overrightarrow{cm} + \overrightarrow{ma}, \overrightarrow{cm} - \overrightarrow{ma}\rangle = |\overline{cm}|^2 - |\overline{ma}|^2 = |\overline{cm}|^2 - r^2.$$

Also ist $\cos\gamma = 0$ genau dann, wenn $|\overline{cm}| = r$ gilt. □

Wir betrachten nun Abbildungen, die Streckenlängen erhalten.

Bemerkung und Definition 4.16 Es sei $(V, \|\cdot\|))$ ein normierter Raum und $f : V \to$ eine Selbstabbildung[43] von V mit

$$\|f(\mathbf{u}) - f(\mathbf{v})\| = \|\mathbf{u} - \mathbf{v}\| \qquad (\mathbf{u}, \mathbf{v} \in V)$$

Dann heißt f **Isometrie** von V. Man sieht leicht:

1. Jede Isometrie von V ist injektiv.
2. Die Menge aller surjektiven Isometrien von X ist eine Untergruppe der symmetrischen Gruppe $S(V)$, genannt **Isometriegruppe** von V.

Im Falle der euklidschen Norm $\|\cdot\|_2$ auf $\mathbb{R}^n$ nennt man eine Isometrie eine **Bewegung** von $\mathbb{E}^n$. Eine Funktion $f : \mathbb{E}^n \to$ ist genau dann eine Bewegung, wenn

$$|\overline{f(a)f(b)}| = |\overline{ab}|$$

für alle $a, b \in \mathbb{E}^n$ gilt.

Bemerkung und Definition 4.17 Es sei $M_n(\mathbb{R})$ die Menge der $(n\times n)$-Matrizen mit reellen Einträgen. Sind $A \in M_n(\mathbb{R})$ und $c \in \mathbb{E}^n$ und ist $T = T_{A,c} : \mathbb{E}^n \to$ definiert durch

$$T(x) := c + Ax = c + A\,\overrightarrow{0x} \qquad (x \in \mathbb{E}^n), \tag{4.1}$$

so gilt

$$T(\overline{ab}) = \overline{TaTb} \qquad (a, b \in \mathbb{E}^n).$$

Eine Matrix $A \in M_n(\mathbb{R})$ heißt **orthogonal**, falls A invertierbar ist mit

$$A^{-1} = A^\top.$$

Die Menge aller orthogonalen $n\times n$-Matrizen mit reellen Einträgen $\mathrm{O}_n = \mathrm{O}_n(\mathbb{R})$ bildet mit der Matrixmultiplikation als Verknüpfung eine Gruppe ([Ü]), genannt **orthogonale Gruppe** des $\mathbb{R}^n$. Für $A \in \mathrm{O}_n$ und $c \in \mathbb{E}^n$ ist $T_{A,c}$ eine Bewegung von $\mathbb{E}^n$, denn für $a, b \in \mathbb{E}^n$ gilt mit $\mathbf{u} := \overrightarrow{ab} = b - a$

$$|\overline{T(a)T(b)}|^2 = \|A\mathbf{u}\|_2^2 = \big(A\mathbf{u}\big)^T A\mathbf{u} = \mathbf{u}^T A^T A\mathbf{u} = \mathbf{u}^\top\mathbf{u} = \|\mathbf{u}\|_2^2 = |\overline{ab}|^2.$$

[43] Die Schreibweise $f : V \to$ soll also für $f : V \to V$ stehen.

Wir zeigen, dass im Fall $n = 2$ jede Bewegung von der Form (4.1) ist.[44] Dabei nutzen wir wieder komplexe Arithmetik und die komplexe Exponentialfunktion. Für $p \in \mathbb{C} = \mathbb{E}$ und $r > 0$ gilt etwa

$$K_r(p) = \{p + re^{i\theta} : \theta \in \mathbb{R}\}.$$

Weiter beschreiben die Abbildung $\sigma : \mathbb{C} \to \mathbb{C}$ mit

$$\sigma(z) := \overline{z} \qquad (z \in \mathbb{C})$$

die Spiegelung von z an der reellen Achse[45] und die Abbildung $\tau_\theta : \mathbb{C} \to \mathbb{C}$ mit

$$\tau_\theta(z) := \mathrm{e}^{i\theta} z \qquad (z \in \mathbb{C},\, \theta \in \mathbb{R}),$$

für $\theta \in [0, \pi]$ eine Drehung von z um 0 mit Drehwinkel θ, d. h. $\measuredangle_{\mathrm{e}^{i\theta} z, z}(0) = \theta$ für $z \neq 0$. Der folgende Satz zeigt, dass jede Bewegung als Komposition einer Drehung und einer Verschiebung $w \mapsto c + w$ oder als Komposition von σ, einer Drehung und einer Verschiebung geschrieben werden kann.

Satz 4.18 *Eine Abbildung $T : \mathbb{C} \to \mathbb{C}$ ist genau dann eine Bewegung, wenn $\theta \in [0, 2\pi)$ und $c \in \mathbb{C}$ existieren mit*

$$T = c + \tau_\theta \tag{4.2}$$

oder

$$T = c + \tau_\theta \circ \sigma. \tag{4.3}$$

Beweis. Ist T von obiger Form, so ist T wegen[46]

$$|T(z) - T(w)| = |\mathrm{e}^{\mathrm{i}\theta}| \cdot |z - w| = |z - w|$$

für $z, w \in \mathbb{C}$ eine Isometrie.

Ist umgekehrt $T : \mathbb{C} \to \mathbb{C}$ eine Isometrie, so existiert wegen $|T(1) - T(0)| = 1$ ein $\theta \in [0, 2\pi)$ mit $T(1) - T(0) = \mathrm{e}^{\mathrm{i}\theta}$. Durch

$$S(z) := \mathrm{e}^{-\mathrm{i}\theta}(T(z) - T(0)) \qquad (z \in \mathbb{C})$$

ist wieder eine Isometrie von $\mathbb{C}$ definiert. Mit $c := T(0)$ ist außerdem

$$T(z) = c + \mathrm{e}^{\mathrm{i}\theta} S(z).$$

[44] Tatsächlich gilt eine entsprechende Aussage für beliebiges n; siehe etwa https://de.wikipedia.org/wiki/Bewegung_(Mathematik).

[45] Hier ist $\overline{z}$ die zu z konjugiert komplexe Zahl, also $\overline{z} = (x, -y) = x - \mathrm{i}y$ falls $z = (x, y)$.

[46] Dabei schreiben wir wie üblich $|z| = \|z\|_2 = \sqrt{x^2 + y^2}$ für $z = (x, y) \in \mathbb{C} = \mathbb{E}$. Man beachte, dass $|zz'| = |z| \cdot |z'|$ für $z, z' \in \mathbb{C}$ gilt.

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

$$x^2 + y^2 \quad = \quad |z - 0|^2 \quad = \quad \big|S(z) - S(0)\big|^2 \quad = \quad u^2 + v^2 \tag{4.4}$$

und damit

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

also $u = x$, und wiederum mit (4.4) dann $v = \pm y$, also $S(z) = z$ oder $S = \overline{z}$. Tatsächlich gilt $S = \mathrm{id}$ oder $S = \sigma$, denn sonst gäbe es $z = (x, y)$, $z' = (x', y') \in \mathbb{C} \setminus \mathbb{R}$ mit $S(z) = \overline{z}$ und $S(z') = z'$, was aber wegen

$$(x' - x)^2 + (y' - y)^2 = |z' - z|^2 = |z' - \overline{z}|^2 = (x' - x)^2 + (y' + y)^2$$

auf den Widerspruch $yy' = 0$ führen würde. □

Bemerkung 4.19 Zwei Mengen $F, F' \subset \mathbb{E}^n$ heißen **kongruent**, falls eine Bewegung T existiert mit $T(M) = M'$. Eine wesentliche Folgerung aus Satz 4.18 ist die Winkeltreue von Bewegungen T der Ebene $\mathbb{E}$ ([Ü]), d. h. für $\mathbf{u}, \mathbf{v} \in \mathbb{R}^2$ und $s \in \mathbb{E}$ gilt

$$\measuredangle_{\mathrm{e}^{\mathrm{i}\theta}\mathbf{u}, \mathrm{e}^{\mathrm{i}\theta}\mathbf{v}}(T(s)) = \measuredangle_{\mathbf{u},\mathbf{v}}(s).$$

Ist $\Delta := \Delta(a, b, c)$ ein Dreieck, so ist $T(\Delta) = \Delta(Ta, Tb, Tc)$, also insbesondere wieder ein Dreieck, und die Seitenlängen mit entsprechenden Innenwinkeln bleiben gleich.

Bemerkung und Definition 4.20 Ist $F \subset \mathbb{E}^n$, so heißt eine Bewegung T **Symmetrie** von F falls $T(F) = F$ gilt. Wir setzen

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

Aus Satz 4.18 folgt insbesondere, dass im Fall $n = 2$ jede Bewegung surjektiv ist.[47] Wie man leicht sieht ist daher $\mathrm{Sym}(F)$ eine Untergruppe der Isometriegruppe des $\mathbb{R}^2$, die sogenannte **Symmetriegruppe** von F.

Bemerkung und Definition 4.21 Wir betrachten den Fall $n = 2$ und die Gruppe $\mathbb{S}_m$ der m-ten Einheitswurzeln, also $\mathbb{S}_m := \langle\zeta\rangle = \{\zeta^0, \ldots, \zeta^{m-1}\}$, wobei $m \geq 2$ und $\zeta = \zeta_m := \mathrm{e}^{2\pi\mathrm{i}/m}$ (siehe Beispiel 3.14). Bezeichnet $\overline{\zeta^k\zeta^{k+1}}$ die Strecke zwischen ζ^k und ζ^{k+1}, so nennt nennt man

$$R_m := \bigcup_{k=0}^{m-1} \overline{\zeta^k\zeta^{k+1}}$$

[47] Tatsächlich gilt dies auch für beliebige n, was wir allerdings nicht beweisen.

reguläres m-Eck. Die Gruppe

$$\mathrm{D}_m \quad := \quad \mathrm{Sym}(R_m)$$

heißt m-te **Diedergruppe**.[48] Sind $\tau(z) := \tau_{2\pi/m}(z) = \zeta z$ die Drehung um 0 mit Drehwinkel $2\pi/m$ und σ die Spiegelung an $\mathbb{R}$, so sind $\sigma, \tau \in D_m$ nach Definition von R_m. Außerdem gilt $\mathrm{ord}(\sigma) = 2$, $\mathrm{ord}(\tau) = m$, $\tau^{-1} = \tau_{-2\pi/m}$ und wegen $\overline{\zeta} = \zeta^{-1}$

$$\tau \circ \sigma = \sigma \circ \tau^{-1}. \tag{4.5}$$

Bemerkung 4.22 Ist $T \in \mathrm{Sym}(F)$ und gilt $F \subset \{z : |z| \le r\}$ sowie $\pm a \in F$ für ein a mit $|a| = r$, so ist $c = 0$ in der Situation von Satz 4.18.

Denn: Nach Satz 4.18 ist T von der Form $T = c+\tau_\theta$ oder $T = c+\tau_\theta\circ\sigma$ mit $c \in \mathbb{C}$. Also ist

$$|T(\pm a)|^2 = |c \pm \mathrm{e}^{\mathrm{i}\theta} a|^2 = |c|^2 + r^2 \pm 2\,\mathrm{Re}(\mathrm{e}^{\mathrm{i}\theta} ac),$$

also $|T(a)|^2 \ge |c|^2+r^2$ oder $|T(-a)|^2 \ge |c|^2+r^2$. Wegen $T \in \mathrm{Sym}(F)$ ist $T(\pm a) \in F$ und damit $|T(\pm a)| \le r$. Also muss $c = 0$ sein.

Satz 4.23 *Mit $\langle\tau\rangle \circ \sigma = \{\tau^k \circ \sigma : k = 0, \dots, m-1\}$ gilt*

1. $\mathrm{D}_m = \langle\{\tau, \sigma\}\rangle = \langle\tau\rangle \cup \langle\tau\rangle \circ \sigma$ *und* $\mathrm{ord}(\mathrm{D}_m) = 2m$.
2. D_m *ist für $m \ge 3$ nicht abelsch*[49] *und für $m = 2$ abelsch, aber nicht zyklisch.*

Beweis.

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

Es sei $T \in \mathrm{D}_m$. Nach Satz 4.18 ist T von der Form $T = c + \tau_\theta$ oder $T = c + \tau_\theta \circ \sigma$ mit $c \in \mathbb{C}$. Ist m gerade, so gilt $\pm 1 \in R_m$ und damit $c = 0$ nach Bemerkung 4.22. Ist m ungerade, so ergibt sich ebenfalls $c = 0$ durch eine kleine Zusatzüberlegung; [Ü]. Aus $c = 0$ folgt $|T(z)| = |z|$ für alle z. Wegen $\mathbb{S}_m = R_m \cap \mathbb{S}$ gilt

$$T(\mathbb{S}_m) \quad = \quad \mathbb{S}_m, \tag{4.6}$$

also $\mathrm{e}^{\mathrm{i}\theta} = T(1) = \zeta^k$ für (genau) ein $k \in \{0, \dots, m-1\}$. Damit ist $T = \tau^k$ oder $T = \tau^k \circ \sigma$. Also gilt $\subset$ und damit auch $\mathrm{ord}(\mathrm{D}_m) \le 2m$. Wegen $\sigma \notin \langle\tau\rangle$ und $\mathrm{ord}(\tau) = m$ folgt $\mathrm{ord}(\mathrm{D}_m) = 2m$ aus dem Satz von Lagrange (Satz 3.18).

2. Es gilt $\tau^{-1} = \tau$ genau für $m = 2$. Nach (4.5) ist damit D_m genau dann abelsch, wenn $m = 2$ gilt. Schließlich rechnet man leicht nach, dass D_2 nicht zyklisch ist ([Ü]). □

[48] Mehr dazu etwa unter https://de.wikipedia.org/wiki/Diedergruppe.
[49] und damit auch nicht zyklisch

5 Morphismen und Gruppen kleiner Ordnung

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.[50]

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

1. Gilt

$$\varphi(ab) = \varphi(a) * \varphi(b) \qquad (a, b \in G), \tag{5.1}$$

so heißt φ **(Halbgruppen-)Morphismus** (von G nach H). Sind $(G, \cdot, e)$ und $(H, *, e_*)$ Monoide und erfüllt φ neben (5.1) auch

$$\varphi(e) = e_*,$$

so heißt φ **(Monoid-)Morphismus** (von G nach H). Ist $a \in G$ invertierbar, so ist $\varphi(a)$ invertierbar mit

$$\varphi(a^{-1}) = \varphi(a)^{-1}. \tag{5.2}$$

Denn: Es gilt $e_* = \varphi(e) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1})$ und entsprechend $e_* = \varphi(a^{-1})\varphi(a)$. Folglich ist $\varphi(a^{-1})$ invers zu $\varphi(a)$ in H.

Sind G und H Gruppen, so spricht man auch von einem **Gruppenmorphismus**. Um deutlich zu machen, dass φ ein Morphismus ist, schreibt man auch $\varphi : (G, \cdot) \to (H, *)$ beziehungsweise $\varphi : (G, \cdot, e) \to (H, *, e_*)$. Außerdem schreiben wir oft kurz $\cdot$ statt $*$ und dann auch wieder $uv := u * v$ sowie $e = e_*$, wenn sich der Bezug aus dem Zusammenhang ergibt.

2. 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**. 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 $G \simeq H$.

Beispiele 5.2 1. Es sei $m \in \mathbb{N}$. Dann ist durch

$$\varphi(a) \;:=\; [a]_m \qquad (a \in \mathbb{Z})$$

[50] Später betrachten wir analog zum Beispiel Ringmorphismen. Eine allgemeine Präzisierung und Untersuchung "strukturerhaltender Abbildungen algebraischer Strukturen" ist Gegenstand der Universellen Algebra; siehe etwa https://de.wikipedia.org/wiki/Universelle_Algebra. Eine noch allgemeinere Sichtweise wird in der Kategorientheorie eingenommen.

wegen $\varphi(0) = [0]_m$ und

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

für $a, b \in \mathbb{Z}$ ein Gruppenmorphismus φ von $(\mathbb{Z}, +, 0)$ nach $(\mathbb{Z}_m, +, [0])$ definiert. φ ist ein Epimorphismus, aber kein Monomorphismus, da etwa $\varphi(0) = [0] = \varphi(m)$ gilt

2. Wegen $e^{z+w} = e^z e^w$ für $z, w \in \mathbb{C}$, $e^0 = 1$ und $\exp(\mathbb{C}) = \mathbb{C} \setminus \{0\} = \mathbb{C}^*$ ist $\exp : (\mathbb{C}, +, 0) \to (\mathbb{C}^*, \cdot, 1)$ ein Epimorphismus. Auch exp ist kein Monomorphismus, da etwa $e^0 = 1 = e^{2\pi \mathrm{i}}$ gilt.

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

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

heißt hier **allgemeine lineare Gruppe**. Die Restriktion $\det = \det|_{\mathrm{GL}_n(K)}$ ist ein Epimorphismus.

Bemerkung 5.3 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.

Satz 5.4 *Es seien $(G, \cdot, e)$ eine Gruppe, $(H, *)$ eine Halbgruppe und $\varphi : G \to H$ ein Halbgruppenmorphismus. Dann ist $(\varphi(G), *, \varphi(e))$ eine Gruppe. Ist $(H, *, e_*)$ eine Gruppe, so ist $\varphi(e) = e_*$, 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 (5.1) ist dann $uv\,(= u * v) = \varphi(ab) \in \varphi(G)$. Da $*$ assoziativ ist, ist $(\varphi(G), *)$ eine Halbgruppe 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 $\varphi(G)$. Da (5.2) für alle $a \in G$ gilt, ist $(\varphi(G), *, \varphi(e))$ eine Gruppe. Ist $(H, *, e_*)$ eine Gruppe, so gilt $e_* = \varphi(e)(\varphi(e))^{-1} = \varphi(ee)(\varphi(e))^{-1} = \varphi(e)\varphi(e)(\varphi(e))^{-1} = \varphi(e)$. □

Bemerkung und Definition 5.5 Es seinen $(G, \cdot, e)$ und $(H, *, e_*)$ Gruppen und $\varphi : G \to H$ ein Morphismus.

1. Ist $V \subset H$ eine Untergruppe, so ist $\varphi^{-1}(V) \subset G$ eine Untergruppe.

   Denn: Es seien $a, b \in \varphi^{-1}(V)$. Dann gilt mit Satz 3.10 (iii) und (5.2)
   $$\varphi(a^{-1}b) = \varphi(a^{-1})\varphi(b) = \varphi(a)^{-1}\varphi(b) \in V,$$
   also $a^{-1}b \in \varphi^{-1}(V)$. Wieder mit Satz 3.10 (iii) ist $\varphi^{-1}(V) \subset G$ eine Untergruppe.

2. Die Menge
   $$\operatorname{Kern}\varphi \coloneqq \varphi^{-1}(\{e_*\})$$

heißt **Kern** von φ. Nach 1. ist $\operatorname{Kern}(\varphi)$ stets eine Untergruppe von G. Außerdem ist $e \in \operatorname{Kern}\varphi$ und zudem φ genau dann ein Monomorphismus, wenn $\operatorname{Kern}\varphi = \{e\}$ gilt.

Denn: Ist φ injektiv, so ist $\operatorname{Kern}\varphi$ einpunktig, also $\operatorname{Kern}\varphi = \{e\}$. Ist umgekehrt $\operatorname{Kern}\varphi = \{e\}$ und sind $a, b \in G$ mit $\varphi(a) = \varphi(b)$, so gilt $e_* = \varphi(a)^{-1}\varphi(b) = \varphi(a^{-1}b)$, also $a^{-1}b = e$ und damit $a = b$.

Beispiel 5.6 In Beispiel 5.2.1 ist $\operatorname{Kern}\varphi = \{a \in \mathbb{Z} : [a]_m = [0]_m\} = m\mathbb{Z}$, in 2. gilt $\operatorname{Kern}(\exp) = 2\pi\mathrm{i}\mathbb{Z}$ und in 3. ist

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

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

Bemerkung 5.7 Es seien G, H Gruppen und und $\varphi : G \to H$ ein Morphismus. Dann gilt

1. Ist $U \subset G$ eine Untergruppe, so ist $\varphi(U) \subset H$ eine Untergruppe. Ist U abelsch, so ist auch $\varphi(U)$ abelsch.
2. Ist $M \subset G$, so gilt $\varphi(\langle M \rangle) = \langle \varphi(M) \rangle$.
3. Ist G zyklisch bzw. abelsch, so ist auch $\varphi(G)$ zyklisch bzw. abelsch.

Die erste Aussage folgt aus Satz 5.4, zweite und dritte als [Ü].

Definition 5.8 Es seien G eine Gruppe und $U \subset G$ eine Untergruppe. Dann heißt U **Normalteiler** oder **normale** Untergruppe von G, in Zeichen

$$U \lhd G,$$

falls die Links- und die Rechtsnebenklassen gU und Ug für alle $g \in G$ übereinstimmen, also $gU = Ug$ für $g \in G$ gilt. In jeder Gruppe G sind G und $\{e\}$ sind Normalteiler von G. Ist G abelsch, so ist jede Untergruppe $U \subset G$ Normalteiler von G.

Beispiel 5.9 Wir betrachten die Diedergruppe

$$\mathrm{D}_3 = \{\mathrm{id}, \tau, \tau^2, \sigma, \tau \circ \sigma, \tau^2 \circ \sigma\}.$$

Für die Untergruppe $U = \langle \sigma \rangle$ gilt $\tau U \neq U\tau$ ([Ü]). Damit ist U kein Normalteiler von D_3. Andererseits ist $\langle \tau \rangle$ ein Normalteiler von D_3 (auch [Ü]).

Bemerkung und Definition 5.10 Es sei U eine Untergruppe von G. Dann ist für $g \in G$

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

nach Satz 3.10 (iii) eine Untergruppe von G, denn für $\alpha, \beta \in U^g$ und $a, b \in U$ mit $\alpha = gag^{-1}$, $\beta = gbg^{-1}$ gilt

$$\alpha^{-1}\beta = (gag^{-1})^{-1}gbg^{-1} = ga^{-1}g^{-1}gbg^{-1} = ga^{-1}bg^{-1} \in U^g.$$

U^g heißt die zu U durch g **konjugierte** Untergruppe. Für $g \in G$ gilt $gU = Ug$ genau dann, wenn $U^g = U$.

> Denn: Aus $gU = Ug$ folgt $U^g = gUg^{-1} = (Ug)g^{-1} = U$, 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 5.11 *Es sei $\varphi : G \to H$ ein Gruppenmorphismus. Ist $N \subset H$ ein Normalteiler von H, so ist $\varphi^{-1}(N)$ ein Normalteiler von G. Insbesondere ist* $\operatorname{Kern}\varphi$ *ein Normalteiler von G.*

Beweis. Wir setzen $U := \varphi^{-1}(N)$. Dann ist $\varphi(U) \subset N$. Für $g \in G$ gilt mit (5.1) und (5.2)

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

und damit $U^g \subset \varphi^{-1}(\varphi(U^g)) \subset \varphi^{-1}(N) = U$. Also gilt $U \lhd G$ nach Bemerkung und Definition 5.10. Die zweite Aussage folgt aus der ersten mit $N := \{e_*\}$. □

Wir wollen nun einen zentralen Satz der elementaren Gruppentheorie erarbeiten. Dazu gehen wir zunächst auf das wichtige Konzept von Faktorgruppen ein.

Bemerkung und Definition 5.12 Ist $(G, \cdot)$ eine Halbgruppe, so ist nach Beispiel 2.1 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

$$(aN)(bN) = a(Nb)N = a(bN)N = (ab)N \qquad (a, b \in G),$$

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

$$\pi_N(a) \quad := \quad aN \qquad (a \in G),$$

ein Halbgruppenmorphismus mit $\pi_N(e) = eN = N$ ist. Nach Satz 5.4 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**. Man kann sich leicht überlegen, dass $aN = N$ für $a \in G$ genau dann gilt, wenn $a \in N$ ist. Also ist

$$\mathrm{Kern}\, \pi_N = N.$$

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 (vgl. Satz 5.11).

Beispiel 5.13 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 3.17 und Beispiel 5.2.1.

Der folgende Satz ist von zentraler Bedeutung.

Satz 5.14 (Isomorphiesatz der Gruppentheorie) [51]

Es seien $\varphi : G \to H$ ein Gruppenmorphismus und $\pi := \pi_{\mathrm{Kern}\, \varphi}$. Dann existiert genau eine Funktion $\psi : G/_{\mathrm{Kern}\, \varphi} \to \varphi(G)$ mit $\psi \circ \pi = \varphi$, und diese ist ein Isomorphismus. Insbesondere sind $G/_{\mathrm{Kern}\, \varphi}$ und $\varphi(G)$ isomorph.

[51] Man findet die Aussage auch als Homomorphiesatz, was sich allerdings nur erklärt, wenn man statt von Morphismen etwas langatmig von Homomorphismen spricht.

Beweis. Nach Bemerkung 5.7.1 ist $\varphi(G)$ Untergruppe von H und nach Satz 5.11 $N := \operatorname{Kern}\varphi$ ein Normalteiler von G. Ist e_* das neutrale Element in H, so gilt für $a, b \in G$ die Äquivalenzkette

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

Wegen der Surjektivität von π ist damit durch

$$\psi(aN) = \psi(\pi(a)) := \varphi(a) \qquad (a \in G)$$

eine Funktion $\psi : G/_N \to \varphi(G)$ mit $\psi \circ \pi = \varphi$, $\psi(N) = e_*$ und $\psi(G) = \varphi(G)$ wohldefiniert. Die Eindeutigkeit von ψ ist klar und da φ und π Morphismen sind, gilt für $a, b \in G$

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

Also ist auch ψ ein (Gruppen-)Morphismus. Ist $a \in G$ mit $\psi(aN) = \varphi(a) = e_*$, so ist $a \in N$ und damit $aN = N$. Also ist $\operatorname{Kern}\psi = \{N\}$ und nach Bemerkung und Definition 5.5 folglich ψ injektiv. □

Beispiele 5.15 1. Es seien $G = (\mathbb{R}, +, 0)$ und $H = (\mathbb{C}^*, \cdot, 1)$. Dann ist durch

$$\varphi(t) := \exp(2\pi i t) \qquad (t \in \mathbb{R})$$

ein Morphismus definiert mit $\varphi(\mathbb{R}) = \mathbb{S}$ und $\operatorname{Kern}\varphi = \mathbb{Z}$. Nach dem Isomorphiesatz ist $\mathbb{R}/_{\mathbb{Z}}$ isomorph zu $\mathbb{S}$.

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^*.

Ein Anliegen in der Gruppentheorie ist es, möglichst viele Gruppen mittels Isomorphismen auf "bekannte" Gruppen zurückzuführen. Speziell für zyklische Gruppen leistet dies der folgende Satz.

Satz 5.16 *Es sei G eine Gruppe.*

1. *G ist genau dann zyklisch, wenn ein $m \in \mathbb{N}_0$ existiert mit $G \simeq (\mathbb{Z}_m, +, [0])$.*
2. *Es gilt $\operatorname{ord}(G) = p \in \mathbb{P}$ genau dann, wenn G isomorph zu $(\mathbb{Z}_p, +, [0])$ ist.*

Beweis. 1. $\Leftarrow$: Nach Beispiel 3.14 sind die Gruppen $\mathbb{Z}$ (und damit auch $\mathbb{Z}_0$) und $\mathbb{Z}_m$ zyklisch. Nach Bemerkung 5.7.3 ist damit auch G zyklisch.

$\Rightarrow$: Ist $x \in G$ ein erzeugendes Element, so ist $\varphi : \mathbb{Z} \to G$, definiert durch $\varphi(a) := x^a$, ein surjektiver Morphismus. Nach dem Isomorphiesatz ist G isomorph zu $\mathbb{Z}/_{\operatorname{Kern}\varphi}$. Nach Satz 3.15 ist $\operatorname{Kern}\varphi = \{0\}$ im Falle $\operatorname{ord}(G) = \infty$, also G isomorph zu $\mathbb{Z}_0 = \mathbb{Z}/_{\{0\}}$, und $\operatorname{Kern}\varphi = m\mathbb{Z}$ im Falle $m := \operatorname{ord}(G) < \infty$, also G dann isomorph zu $\mathbb{Z}_m = \mathbb{Z}/_{mZ}$

2. $\Rightarrow$: Nach Bemerkung 3.19 ist G zyklisch und nach 1. daher isomorph zu $\mathbb{Z}_p$. $\Leftarrow$ ist klar. □

Beispiel 5.17 Für $m \in \mathbb{N}$ hat nach Beispiel 3.14.3 die zyklische Gruppe $\mathbb{S}_m = \langle e^{2\pi i/m}\rangle$ die Ordnung m. Also ist $(\mathbb{S}_m, \cdot, 1)$ isomorph zu $(\mathbb{Z}_m, +, 0)$.

Wie in Satz 4.23 gesehen, wird die Diedergruppe D_m von der Drehung τ mit Drehwinkel $2\pi/m$ und der Spiegelung σ erzeugt. Dabei gilt $\operatorname{ord}(\tau) = m$, $\operatorname{ord}(\sigma) = 2$ und $\tau \circ \sigma = \sigma \circ \tau^{-1}$. Bis auf Isomorphie ist D_m die einzige Gruppe mit den entsprechenden Eigenschaften:

Satz 5.18 *Es seien $m \in \mathbb{N} \setminus \{1\}$ und G eine Gruppe der Ordnung $2m$, die von zwei Elementen a und b mit*

$$\operatorname{ord}(a) = 2, \quad \operatorname{ord}(b) = m \quad \textit{und} \quad ba = ab^{-1}$$

erzeugt wird. Dann ist G isomorph zur Diedergruppe D_m.

Beweis. Zunächst ergibt sich $ab^{-r} = b^r a$ für $r \in \mathbb{N}_0$ induktiv aus $ab^{-1} = ba$ und dann für negative r mit b^{-1} statt b. Damit erhält man für $j, k, n, p \in \mathbb{Z}$

$$(b^k a^j)^{-1} b^n a^p = a^{-j} b^{n-k} a^p = \begin{cases} b^{n-k} a^p & \text{falls } j \text{ gerade} \\ b^{k-n} a^{p+1} & \text{falls } j \text{ gerade} \end{cases}, \tag{5.3}$$

denn für gerade j ist $a^{-j} = e$, und für ungerade j ist $a^{-j} = a$ und daher $a^{-j} b^{n-k} = a b^{n-k} = b^{k-n} a$. Nach Satz 3.10 (iii) ist

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

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

$$\varphi(\tau^k \circ \sigma^j) \;:=\; b^k a^j \qquad \left(k \in \{0, \ldots, m-1\},\, j \in \{0, 1\}\right)$$

eine surjektive Abbildung $\varphi : D_m \to G$ (wohl-)definiert. Wegen

$$\#G = 2m = \#D_m$$

ist φ dann auch schon bijektiv. Aus $\operatorname{ord}(\tau) = m = \operatorname{ord}(b)$ und $\operatorname{ord}(\sigma) = 2 = \operatorname{ord}(a)$ folgt $\varphi(\tau^k \circ \sigma^j) = b^k a^j$ auch für beliebige $k, j \in \mathbb{Z}$. Sind $\alpha, \beta \in \mathrm{D_m}$ so existieren $j, k, n, p \in \mathbb{Z}$ mit $\alpha^{-1} = \tau^k \circ \sigma^j$ und $\beta = \tau^n \circ \sigma^p$. Mit (5.3) für D_m und für G ergibt sich für j gerade beziehungsweise ungerade

$$\varphi(\alpha \circ \beta) = \left\{ \begin{array}{ccc} \varphi(\tau^{n-k} \circ \sigma^p) & = & b^{n-k} a^p \\ \varphi(\tau^{k-n} \circ \sigma^{p+1}) & = & b^{k-n} a^{p+1} \end{array} \right\} = (b^k a^j)^{-1} b^n a^p = \varphi(\alpha)\varphi(\beta).$$

Damit ist φ ein Isomorphismus und folglich sind D_m und G isomorph. □

Satz 5.19 *Es seien G eine Gruppe und $M \subset G$, $M \neq \varnothing$. Dann gilt*

$$\langle M \rangle = \bigcup_{n \in \mathbb{N}} \left\{ \prod_{k=1}^{n} a_k^{\mu_k} : a_k \in M,\ \mu_k \in \{-1, 1\} \text{ für } k = 1, \ldots, n \right\} \tag{5.4}$$

und im Fall, dass $\langle M \rangle$ abelsch ist, auch

$$\langle M \rangle = \left\{ \prod_{a \in M} a^{j_a} : (j_a)_{a \in M} \in \mathbb{Z}^{(M)} \right\}. \tag{5.5}$$

Beweis. 1. Es sei V die rechte Seite in (5.4). Sind $a = a_1^{\mu_1} \cdots a_n^{\mu_n}$, $b = b_1^{\nu_1} \cdots b_m^{\nu_m} \in V$, wobei $a_k, b_k \in M$ und $\mu_k, \nu_k \in \{-1, 1\}$, so ist auch

$$a^{-1} b \;=\; a_n^{-\mu_n} \cdots a_1^{-\mu_1} \cdot b_1^{\nu_1} \cdots b_m^{\nu_m} \;\in\; V.$$

Nach Satz 3.10 (iii) ist V damit eine Untergruppe von G.

$\supset$: Ist U eine Untergruppe von G mit $M \subset U$, so gilt $V \subset U$ nach Satz 3.10 (ii). Da $\langle M \rangle$ eine solche Untergruppe ist, gilt $V \subset \langle M \rangle$.

$\subset$: Wegen $a_1 = a_1^1 \in V$ für $a_1 \in M$ ist $M \subset V$. Da V ein Untergruppe ist, ist nach Definition der erzeugten Untergruppe $\langle M \rangle \subset V$.

2. Nun sei $\langle M \rangle$ abelsch und W die rechte Seite in (5.5). Die Inklusion $W \subset \langle M \rangle$ ergibt sich wie in ersten Beweisteil. Mit 1. recht es also zu zeigen, dass $V \subset W$ gilt. Sind $a_1, \ldots a_n \in M$ sowie $\mu_1, \ldots, \mu_n \in \{-1, 1\}$ und setzt man $j_a := \sum_{k : a_k = a} \mu_k$ für $a \in M$, so gilt $a_1^{\mu_1} \cdots a_n^{\mu_n} = \prod_{a \in M} a^{j_a} \in V$. □

Satz 5.20 *Es sei G eine Gruppe mit* $\operatorname{ord}(x) = 2$ *für $x \in G \setminus \{e\}$. Dann ist G abelsch und* $\operatorname{ord} G \in \{2^n : n \in \mathbb{N}_0\} \cup \{\infty\}$.

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

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

Es sei nun G endlich. Dann existiert

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

Wir wählen $M \subset G$ mit $\#M = n$ und $\langle M\rangle = G$ (also ein minimales Erzeugendensystem von G). Mit Satz 5.19.2 und wegen $a^j \in \{e, a\}$ ist

$$G \;=\; \Big\{ \prod_{a\in M} a^{j_a} : (j_a) \in \mathbb{Z}^M \Big\} \;=\; \Big\{ \prod_{a\in F} a : F \subset M \Big\}, \tag{5.6}$$

Sind $F, F' \subset M$ mit $\prod\limits_{a\in F} a = \prod\limits_{b\in F'} b$, so ist schon $F = F'$, denn sonst wäre mit (ohne Einschränkung) einem $c \in F' \setminus F$ zunächst $F \cup (F' \setminus \{c\}) \subset M \setminus \{c\}$ und damit

$$c = \Big(\prod_{a\in F} a\Big)\Big(\prod_{b\in F', c\neq b} b\Big)^{-1} \in \langle F \cup (F' \setminus \{c\})\rangle \subset \langle M \setminus \{c\}\rangle,$$

also $G = \langle M\rangle = \langle M \setminus \{c\}\rangle$ im Widerspruch zur Minimalität von n. Mit (5.6) folgt $\#G = \#\{F : F \subset M\} = 2^n$. □

Basierend auf den vorhergehenden Ergebnissen können wir eine vollständige Charakterisierung der Gruppen von doppelter Primzahlordnung geben:

Satz 5.21 *Es sei G eine Gruppe der Ordnung $2p$ mit $p \in \mathbb{P}$. Dann ist entweder G zyklisch, also isomorph zu $(\mathbb{Z}_{2p}, +)$, oder isomorph zu D_p.*

Beweis. Der "entweder"-Teil der Behauptung ergibt sich aus der Azyklizität der Diedergruppen; siehe Satz 4.23.

Nach Bemerkung 3.19 gilt $\mathrm{ord}(x) \in \{2, p, 2p\}$ für $x \in G \setminus \{e\}$. Ist $\mathrm{ord}\ x = 2p$ für ein $x \in G$, so ist $G = \langle x\rangle$ und damit G zyklisch, also nach Satz 5.16 isomorph zu $(\mathbb{Z}_{2p}, +)$.

Es gelte nun also $\mathrm{ord}(x) \in \{2, p\}$ für $x \in G \setminus \{e\}$. Ist $p = 2$, so gilt $\mathrm{ord}(x) = 2$ für $x \in G \setminus \{e\}$, also ist G abelsch nach Satz 5.20. 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

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

Wegen $\mathrm{ord}(G) = 4$ ist also $G = \{e, a, b, ab\} = \langle\{a, b\}\rangle$, und folglich G isomorph zu D_2 nach Satz 5.18.

Es sei nun $p \geq 3$. Zunächst existiert wegen $\mathrm{ord}(G)$ gerade ein $a \in G$ mit $\mathrm{ord}(a) = 2$ ([Ü]). Außerdem ist $\mathrm{ord}(G) = 2p$ keine Zweierpotenz. Also existiert nach Satz 5.20 ein $b \in G$ mit $\mathrm{ord}(b) > 2$. Für $U := \langle b\rangle$ ist nach Bemerkung 3.19

$$\mathrm{ord}(U) = \mathrm{ord}(b) = p.$$

Da p ungerade ist, gilt $a^p = a \neq e$, also $a \notin U$ nach Bemerkung 3.19. Damit ist $U \cap Ua = \varnothing$ und $U \cap aU = \varnothing$, also wegen $\operatorname{ord}(U) = \#Ua = \#aU = p$ und $\operatorname{ord}(G) = 2p$

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

Insbesondere ist $G = \langle\{a, b\}\rangle$ und $aU = Ua$, d. h. $U \lhd G$ und folglich, unter Verwendung von $a^2 = e$ und Bemerkung 5.10

$$aUa = aUa^{-1} = U^a = U.$$

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 $(p = \operatorname{ord}(b)) \mid (k^2 - 1)$ nach Satz 3.15. Wegen p prim und $k^2 - 1 = (k+1)(k-1)$ folgt $p \mid (k+1)$ oder $p \mid (k-1)$, wegen $k \in \{0, \ldots, p-1\}$ also $k = p-1$ oder $k = 1$.

Im Fall $k = 1$ wäre $aba = b$, also $ab = ba^{-1} = ba$. Dann ist $(ab)^r = a^r b^r$ für $r \in \mathbb{N}$. Wegen $a^p = a$ und $b^p = 1$ ist daher

$$(ab)^2 = a^2 b^2 = b^2 \neq e \quad \text{und} \quad (ab)^p = a^p b^p = a \neq e,$$

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 5.18 folgt nun, dass G isomorph zu D_p ist. □

Satz 5.22 *Es gibt bis auf Isomorphie jeweils genau*

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

Insbesondere sind alle Gruppen der Ordnung ≤ 5 abelsch.

Beweis. Der erste Fall ist klar nach Satz 5.16, der zweite nach Satz 5.21 mit $p \in \{2, 3\}$. Der Zusatz gilt wegen der Kommutativität von D_2 (Satz 4.23). □

6 Polynomringe und Körpererweiterungen

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

Bemerkung und Definition 6.1 Es sei $R = (R, +, \cdot)$ ein Ring und es sei U eine Untergruppe von $(R, +, 0)$. Ist U ein Untermonoid von $(R, \cdot, 1)$, so heißt U **Unterring** von R. Ist R ein Körper und ist $U \setminus \{0\}$ eine Untergruppe von $(R^*, \cdot, 1)$, so heißt U **Unterkörper** (oder **Teilkörper**) von R.

Nach Satz 3.10 (iii) ist U eine Untergruppe von $(R, +, 0)$ genau dann, wenn $U - U \subset U$ gilt. Damit ist dies in allen obigen Fällen erfüllt. Nach Bemerkung und Definition 3.9 ist U ist zudem Untermonoid von $(R, \cdot, 1)$ genau dann wenn $U \cdot U \subset U$ und $1 \in U$ gilt.

Beispiel 6.2 $\mathbb{Q}$ und $\mathbb{R}$ sind Unterkörper von $(\mathbb{C}, +, \cdot)$ und $\mathbb{Z}$ ist ein Unterring von $(\mathbb{C}, +, \cdot)$.

Durch eine zu Bemerkung 3.12 analoge Argumentation erhält man mit Bemerkung und Definition 6.1 leicht: Beliebige Schnitte von Unterringen eines Rings sind Unterringe und beliebige Schnitte von Unterkörpern eines Körpers sind Unterkörper. Dies rechtfertigt die Namensgebungen in der folgenden

Definition 6.3 Es seien R ein Ring bzw. ein Körper und $M \subset R$. Ist $\mathscr{U}_M$ die Menge aller Unterringe bzw. aller Unterkörper von R mit $M \subset U$, so heißt

$$\langle M \rangle \;\coloneqq\; \langle M \rangle_{\text{Ring}} \;\coloneqq\; \bigcap_{U \in \mathscr{U}_M} U$$

von M **erzeugter Unterring** bzw.

$$\langle M \rangle \;\coloneqq\; \langle M \rangle_{\text{Körper}} \;\coloneqq\; \bigcap_{U \in \mathscr{U}_M} U$$

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 $\operatorname{Kern}(\varphi) \coloneqq \varphi^{-1}(\{0_S\})$ 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 und Definition 5.5 ist ein Morphismus φ genau dann ein Monomorphismus, wenn $\mathrm{Kern}(\varphi) = \{0\}$ gilt. Weiter sieht leicht: Kompositionen 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, so ist $\varphi^{-1}(V) \subset R$ ein Unterring.
- Ist $U \subset R$ ein Unterring, so ist $\varphi(U) \subset S$ ein Unterring.

Sind R ein *Körper* und $S \neq \{0_S\}$, so ist φ schon injektiv, also eine Einbettung.

> Denn: Ist $x \neq 0$, so gilt $1_S = \varphi(1_R) = \varphi(xx^{-1}) = \varphi(x)\varphi(x^{-1})$, also $\varphi(x) \neq 0_S$. Damit ist $\mathrm{Kern}(\varphi) = \{0_R\}$.

Nach Satz 5.4 ist $\varphi(R)$ ein Körper und mit (5.2) gilt für $x, y \in R$, $y \neq 0$

$$\varphi(x/y) = \varphi(x)/\varphi(y).$$

Bemerkung 6.7 Es seien R ein *kommutativer* Ring, $U \subset R$ ein Unterring und $x \in R$. Dann schreibt man

$$U[x] \coloneqq \langle U \cup \{x\} \rangle_{\mathrm{Ring}}$$

und spricht vom durch adjungieren von x zu U entstandenen Unterring. Es gilt

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

denn einerseits enthält jeder Unterring, der U und x enthält, auch notwendigerweise die rechte Seite und andererseits rechnet man nach, dass die rechte Seite ein Unterring ist, der U und x enthält. Für $\sum\limits_{k \in \mathbb{N}_0} a_k x^k$ und $\sum\limits_{\ell \in \mathbb{N}_0} b_\ell x^\ell$ gilt genauer

$$\Big(\sum_{k \in \mathbb{N}_0} a_k x^k \Big) \Big(\sum_{\ell \in \mathbb{N}_0} b_\ell x^\ell \Big) = \sum_{j \in \mathbb{N}_0} x^j \sum_{k+\ell=j} a_k b_\ell = \sum_{j \in \mathbb{N}_0} c_j x^j \tag{6.1}$$

mit $c_j = \sum\limits_{k=0}^{j} a_k b_{j-k}$.

Beispiel 6.8 Es sei $R := \mathbb{C}$. Für $a_0, \ldots, a_n \in \mathbb{C}$ ist

$$\sum_{j=0}^{n} a_j \mathrm{i}^j = \sum_{j \text{ gerade}} a_j (-1)^{j/2} + \mathrm{i} \sum_{j \text{ ungerade}} a_j (-1)^{(j-1)/2}$$

Damit ist

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

Entsprechend gilt wegen $(\sqrt{2})^j \in \mathbb{N} \cup \sqrt{2}\,\mathbb{N}$ für $j \in \mathbb{N}_0$

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

Bemerkung 6.9 Es sei R ein Ring. Ist $M \neq \varnothing$ eine beliebige Menge, so sind für $f, g \in R^M = \mathrm{Abb}(M, R)$ die Funktionen $f+g \in R^M$ und $f \cdot g \in R^M$ definiert durch

$$(f+g)(x) := f(x) + g(x), \quad (f \cdot g)(x) := f(x) \cdot g(x) \qquad (x \in M).$$

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. Schließlich setzen wir noch $(\lambda f)(x) := \lambda f(x)$ für $\lambda \in R$ und $f \in R^M$.

Bemerkung 6.10 Wir betrachten nun einen kommutativen Ring R und den Fall $M = \mathbb{N}_0$. Anders als in Bemerkung 6.9 definieren für $(a_j), (b_j) \in R^{\mathbb{N}_0}$ [52]

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

Dabei heißt (c_j) **Faltung** oder auch **Cauchy-Produkt**[53] von (a_j) und (b_j). Mit der Addition aus Definition 6.9 und obiger Multiplikation ist $(R^{\mathbb{N}_0}, +, \cdot)$ ein kommutativer Ring mit Einselement $(1, 0, \ldots) = \big(\delta_{j0}\big)_{j=0}^{\infty}$ ([Ü]). Setzt man

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

so gilt

$$X^k = \big(\delta_{jk}\big)_{j=0}^{\infty} \qquad (k \in \mathbb{N}_0).$$

[52] Wir schreiben hier wie bei abzählbaren Definitionsbereichen üblich Funktionen als Tupel
[53] In anderem Kontext oft als $(a_j) * (b_j)$ geschrieben.

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

$$(a_j) = (a_0, \ldots, a_n, 0, \ldots) \;=\; \sum_{j=0}^{n} a_j X^j = \sum_{j \in \mathbb{N}_0} a_j X^j.$$

Ist $(b_j) \in R^{(\mathbb{N}_0)}$ mit $b_j = 0$ für $j > m$, so gilt

$$\sum_{j=0}^{n} a_j X^j + \sum_{j=0}^{m} b_j X^j = \sum_{j=0}^{\max\{n,m\}} (a_j + b_j) X^j$$

und

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

Definition 6.11 In der Situation aus Bemerkung 6.10 ist $RX^0 = \{(a, 0, \ldots) : a \in R\}$ 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 a mit aX^0 für $a \in R$. Damit heißt

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

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

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

ein Polynom, so heißt die Funktion $\hat{P} : R \to R$, definiert durch

$$\hat{P}(x) \coloneqq \sum_{j=0}^{n} a_j x^j \qquad (x \in R)$$

die zugehörige **Polynomfunktion**. Ein $x \in R$ mit $\hat{P}(x) = 0$ heißt **Nullstelle** von $\hat{P}$ oder **Wurzel** des Polynoms P.

Bemerkung und Definition 6.12 Es sei R ein kommutativer Ring.

1. Für $x \in R$ und $P, Q \in R[X]$ gilt mit (6.1)

$$\widehat{(P+Q)}(x) = \hat{P}(x) + \hat{Q}(x) \quad \text{und} \quad \widehat{(PQ)}(x) = \hat{P}(x)\hat{Q}(x)\,.$$

Damit und wegen $\widehat{X^0}(x) = x^0 = 1_R$ ist die Funktion

$$R[X] \ni P \mapsto \hat{P}(x) \in R$$

ein Ringmorphismus, genannt **Auswertungsmorphismus** bezüglich x. Die Funktion

$$R[X] \ni P \mapsto \hat{P} \in R^R$$

ist ebenfalls ein Ringmorphismus. Wichtig ist dabei zu bemerken, dass es sich im Allgemeinen nicht um einen Monomorphismus handelt: Ist etwa $R = (\mathbb{Z}_2, +, \cdot)$ der Binärkörper, so sind $P_1 = X^2 + X$ und $Q = 0$ verschiedene Polynome über $\mathbb{Z}_2$. Die Polynomfunktionen $\hat{P}$ und $\hat{Q}$ sind jedoch gleich (der Nullfunktion).

2. Wie in der Algebra üblich, schreiben im Weiteren für $x \in R$ meist kurz $P(x)$ statt $\hat{P}(x)$. Ist $U \subset R$ ein Unterring, so ist $U[X] \subset R[X]$. Damit ist $\hat{P}(x)$ auch für $P \in U[X]$ definiert. Nach Bemerkung und Definition 6.7 gilt

$$U[x] = \big\{P(x) : P \in U[X]\big\}. \tag{6.2}$$

Bemerkung und Definition 6.13 Es seien R ein kommutativer Ring und $P = \sum\limits_{j\in\mathbb{N}_0} a_j X^j \in R[X]$. Dann heißt (mit $\max \varnothing := -\infty$)

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

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**. Ist auch $Q = \sum\limits_{j\in\mathbb{N}_0} b_j X^j \in R[X]$, so gilt[54]

$$\begin{aligned} \deg(P+Q) &\leq \max\{\deg P, \deg Q\}, \\ \deg(PQ) &\leq \deg P + \deg Q\,. \end{aligned}$$

Ist R ein Integritätsring, so gilt genauer die **Gradformel**

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

wegen $\sum\limits_{k=0}^{n+m} a_k b_{n+m-k} = a_n b_m \neq 0$ für $n := \deg P$, $m := \deg Q \in \mathbb{N}_0$.

Satz 6.14 (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: Wir zeigen per Induktion: Ist $n \in \mathbb{N}_0$ und sind $P, S \in K[X]$ mit $\deg P = n$, so existieren Q, R wie behauptet.

Ist $n = 0$ (oder $n = -\infty$), also $P = a_0 \in K$, so sind $R := P$, $Q := 0$ im Fall $\deg S > 0$ und $Q := a_0/b_0$, $R := 0$ im Fall $S = b_0 \neq 0$ geeignet.

[54] Man setzt natürlich $-\infty \leq a$ und $(-\infty) + a = a + (-\infty) := -\infty$ für $a \in [-\infty, \infty)$.

Es sei nun $n \in \mathbb{N}$ und die Behauptung gelte für jedes $k \in \{0, \ldots, n-1\}$. Weiter seien

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

mit $\deg P = n$ und ohne Einschränkung $\deg S =: m \leq n$ (sonst sind $Q = 0$ und $R = P$ geeignet). Für das Polynom

$$C := P - \frac{a_n}{b_m} X^{n-m} S \quad \in K[X]$$

gilt dann $\deg C < n$. Nach Induktionsvoraussetzung (angewandt mit Q statt P) existieren Polynome $Q', R \in K[X]$ mit $\deg R < \deg S$ und $C = Q'S + R$. Mit $Q := Q' + (a_n/b_m)X^{n-m}$ gilt dann

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

2. Eindeutigkeit: Sind $Q, Q', R, R' \in K[X]$ mit $P = QS + R = Q'S + R'$ und $\deg R, \deg R' < \deg S =: m$, so ist $(Q - Q')S = R' - R$ mit $\deg(R' - R) < m$. Wäre $Q \neq Q'$, also $\deg(Q - Q') \geq 0$, so wäre $\deg(R' - R) = \deg(Q - Q') + m \geq m$. Widerspruch. Also ist $Q = Q'$ und damit auch $R = R'$. □

Satz 6.15 *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*
$$P = Q(X - a)$$
und dabei gilt $\deg(Q) + 1 = \deg(P)$.

2. *Ist $P \neq 0$, so hat P höchstens* $\deg P$ *Wurzeln.*

Beweis. 1. Es sei $S := X - a$. Wegen $\deg S = 1$ existiert nach Satz 6.14 genau ein Paar (Q, R) in $K[X] \times K[X]$ mit $P = QS + R$ und $\deg R < 1$, also $R = r_0$ mit einem $r_0 \in K$. Mit Bemerkung 6.12 folgt

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

Damit ist $R = 0$. Mit der Gradformel gilt

$$\deg(P) = \deg(QS) = \deg(S) + \deg(Q) = 1 + \deg(Q).$$

2. Sind $a_1, \ldots, a_m$ paarweise verschiedene Wurzeln von P, so liefert 1. induktiv ein $Q \in K[X]$ mit $P = Q \prod_{j=1}^{m} (X - a_j)$ und $\deg(Q) + m = \deg(P)$. Wegen $P \neq 0$ und damit auch $Q \neq 0$ folgt $m \leq \deg(P)$. □

Sind K ein Körper, V ein K-Vektorraum, $M \subset V$ und $\mathscr{U}_M$ die Menge der linearen Unterraäume von V, die M enthalten, so schreiben wir

$$\operatorname{span}_K(M) := \bigcap_{U \in \mathscr{U}_M} U$$

für den von M erzeugten Unterraum von V. Dabei gilt

$$\operatorname{span}_K(M) = \Big\{ \sum_{x \in M} \lambda_x \, x : (\lambda_x) \in K^{(M)} \Big\}.$$

Man nennt M Erzeugendensystem von V, falls $\operatorname{span}(M) = V$ gilt, und Basis von V, falls M [55] zusätzlich K-linear unabhängig ist.

Definition 6.16 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.[56] Die Dimension des K-Vektorraums E heißt **Grad** von E über K, in Zeichen

$$[E : K] \coloneqq \dim_K(E).$$

Die Erweiterung heißt **endlich** falls $[E : K]$ endlich ist.

Beispiele 6.17 Es gilt $[\mathbb{C} : \mathbb{R}] = 2$, denn $\{1, \mathrm{i}\}$ ist eine zweielementige Basis des $\mathbb{R}$-Vektorraumes $\mathbb{C}$. Weiter ist $[\mathbb{R} : \mathbb{Q}] = \infty$, denn für jede endliche Menge $M \subset \mathbb{R}$ ist $\operatorname{span}_{\mathbb{Q}}(M) = \big\{ \sum_{x \in M} \lambda_x \, x : (\lambda_x) \in \mathbb{Q}^M \big\}$ abzählbar, also $\neq \mathbb{R}$.

Satz 6.18 *Es seien E eine endliche Erweiterung von K und F eine endliche Erweiterung von E. Ist B eine Basis von E als K-Vektorraum und ist C eine Basis von F als E-Vektorraum, so ist BC eine Basis von F als K-Vektorraum. Außerdem gilt*

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

Beweis. Es sei $y \in F$. Dann ist $y = \sum_{x \in C} \mu_x x$ mit Skalaren $\mu_x \in E$. Weiter existieren zu jeden $x \in C$ Skalare $\lambda_{\mu,x} \in K$ mit $\mu_x = \sum_{\mu \in B} \lambda_{\mu,x} \mu$. Also ist

$$y = \sum_{x \in C} \Big(\sum_{\mu \in B} \lambda_{\mu,x} \mu \Big) x \; = \sum_{x \in C} \sum_{\mu \in B} \lambda_{\mu,x} \mu x \, .$$

[55] also die Familie $(x)_{x \in M}$

[56] Die Abbildung $K \times E \ni (\lambda, x) \mapsto \lambda \cdot x \in E$ ist eine Skalarmultiplikation.

Damit ist BC ein Erzeugendensystem von F als K-Vektorraum. Ist $y = 0$, so folgt wegen der E-linearen Unabhängigkeit von C zunächst $\sum_{\mu \in B} \lambda_{\mu,x}\mu = 0$ für $x \in C$, und mit der K-linearen Unabhängigkeit von B dann $\lambda_{\mu,x} = 0$ für $\mu \in B$, $x \in C$. Damit ist BC eine Basis von F als K-Vektorraum.

Sind $(\mu, x), (\mu', x') \in B \times C$, so folgt aus $\mu x = \mu' x'$, also $\mu x - \mu' x' = 0$, wegen $\mu, \mu' \neq 0$ und der E-linearen Unabhängigkeit von C schon $x = x'$ und dann auch $\mu - \mu' = 0$. Also ist $\#(BC) = \#(B \times C) = \#B \cdot \#C$ und damit auch $[F : K] = [E : K][F : E]$. □

Definition 6.19 Es sei E eine Körpererweiterung von K. Dann heißt $x \in E$ **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 6.20

1. Sind K ein Körper und $a \in K$, so ist a Wurzel von $X - a \in K[X]$. Also ist K algebraisch über K.

2. Für $a \in \mathbb{Q}_+$ und $n \in \mathbb{N}$ ist $\sqrt[n]{a}$ algebraisch über $\mathbb{Q}$, da $P(\sqrt[n]{a}) = 0$ etwa für $P := X^n - a \in \mathbb{Q}[X]$.

3. $\mathbb{C}$ ist algebraisch über $\mathbb{R}$, denn für $x = (a, b) = a + \mathrm{i}b \in \mathbb{C}$ und

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

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

Bemerkung und Definition 6.21 Man schreibt

$$\mathbb{A} := \{x \in \mathbb{R} : x \text{ algberaisch über } \mathbb{Q}\}.$$

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 die Menge $\mathbb{R} \setminus \mathbb{A}$ der über $\mathbb{Q}$ transzendenten Zahlen überabzählbar. Insbesondere ist $\mathbb{R}$ nicht algebraisch über $\mathbb{Q}$.

Bemerkung 6.22 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. Ist $\varphi_x : K[X] \to E$ den Auswertungsmorphismus bezüglich x, so ist φ_x auch eine K-lineare Abbildung. Aus der Definition der Transzendenz ergibt sich unmittelbar, dass für $x \in E$ folgende Aussagen äquivalent sind:

(i) x ist transzendent über K.
(ii) $\left(x^j\right)_{j\in\mathbb{N}_0}$ ist linear unabhängig im K-Vektorraum E.
(iii) $\mathrm{Kern}(\varphi_x) = \{0\}$.

2. Ist E eine endliche Erweiterung von K, so ist $(x^j)_{j=0}^{[E:K]}$ für alle $x \in E$ linear abhängig im K-Vektorraum E, also x nach 1. algebraisch über K. Damit ist E algebraisch über K.

Satz 6.23 *Es seien E eine Körpererweiterung von K und $x \in E$ algebraisch über K. Dann gilt:*

1. *Es gibt genau ein normiertes Polynom $P_x \in K[X]$ minimalen Grades mit $P_x(x) = 0$ und jedes weitere Polynom $P \in K[X]$ mit Wurzel x ist ein Vielfaches von P_x, d. h. es existiert ein Polynom Q mit $P = QP_x$.*
2. *$\{x^j : j = 0, \ldots, \deg(P_x) - 1\}$ ist eine Basis des K-Vektorraumes $K[x]$.*

Beweis. 1. Wir setzen

$$n := \min\{\deg(P) : P \in K[X] \setminus \{0\},\, P(x) = 0\} \in \mathbb{N}.$$

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 $P \in K[X]$ beliebig, so existieren mit Polynomdivision (Satz 6.14) $Q, R \in K[X]$ mit $P = QP_x + R$ und $\deg R < \deg P_x$. Ist dabei $P(x) = 0$, so gilt $R(x) = P(x) - Q(x)P_x(x) = 0$ und mit der Minimalität von $\deg P_x$ folgt $\deg R = -\infty$, also $R = 0$ und damit $P = QP_x$. Ist dabei $\deg P = n$, so ist $\deg Q = 0$ nach der Dimensionsformel, also falls P ebenfalls normiert ist $Q = 1$ und damit $P = P_x$.

2. Es seien $\varphi_x : K[X] \to K[x]$ der Auswertungsmorphismus bzgl. x und n wie in 1. Wir setzen $U := \{S \in K[X] : \deg S < n\}$. Dann ist $B := \{X^0, \ldots, X^{n-1}\}$ eine Basis von U ([Ü]). Ist $y \in K[x]$, also $y = \varphi_x(P)$ für ein $P \in K[X]$ und sind R, Q wie im ersten Beweisteil, so ist $R \in U$ und

$$y = \varphi_x(P) = P(x) = Q(x)P_x(x) + R(x) = R(x) = \varphi_x(R).$$

Damit gilt schon $\varphi_x(U) = K[x]$. Außerdem folgt $\mathrm{Kern}(\varphi_x|_U) = \{0\}$ aus der Definition von n. Also ist $\varphi_x|_U$ ein K-Vektorraumisomorphismus und damit $\{x^0, \ldots, x^{n-1}\} = \varphi_x(B)$ eine Basis von $K[x]$. □

Bemerkung und Definition 6.24 Ist E eine Körpererweiterung von K und ist $x \in E$ algebraisch über K, so heißt das Polynom P_x aus Satz 6.23 das **Minimalpolynom** von x über K. Außerdem heißt

$$\deg(x) := \deg_K(x) := \deg P_x$$

dann **Grad** von x über K. Speziell ist x vom Grad 1 genau dann, wenn $x \in K$ gilt und dann $X - a \in K[X]$ das Minimalpolynom. Nach Satz 6.23 ist $\dim_K K[x] = \deg(x)$ sowie

$$K[x] = \operatorname{span}_K\{1, x, \ldots, x^{\deg(x)-1}\} = K + xK + \ldots + x^{\deg(x)-1}K.$$

Außerdem ist $K[x]$ nach Bemerkung 6.22.2. algebraisch über K.

Satz 6.25 *Ist E eine Körpererweiterung von K, so ist $x \in E$ genau dann algebraisch über K, wenn $K[x]$ ein Unterkörper von E ist.*

Beweis. $\Leftarrow$: Ist $x = 0$, so ist x algebraisch über K. Es sei also $x \neq 0$. Dann ist $1/x \in K[x]$. Nach Bemerkung 6.22.1 gibt es ein $P \in K[X]$ mit $1/x = P(x)$. Also ist x Wurzel von $Q := 1 - X \cdot P \in K[X] \setminus \{0\}$.

$\Rightarrow$: Da $K[x]$ ein Unterring von E ist, ist nur zu zeigen: Für $y \in K[x] \setminus \{0\}$ ist $1/y \in K[x]$. Es sei also $0 \neq y \in K[x]$. Nach Bemerkung 6.24 ist y algebraisch über K. Ist $P = a_r X^r - \sum_{j>r} a_j X^j \in K[X]$ mit $a_r \neq 0$ und $P_y(y) = 0$, so folgt

$$\frac{1}{y} = \sum_{j>r} \frac{a_j}{a_r} y^{j-r-1} \in \operatorname{span}\{y^k : k \in \mathbb{N}_0\} \subset K[x].$$

□

Beispiel 6.26 1. Wegen $\sqrt{2} \notin \mathbb{Q}$ ist $P_{\sqrt{2}} = X^2 - 2 \in \mathbb{Q}[X]$ das Minimalpolynom von $\sqrt{2}$. Also ist $\sqrt{2}$ vom Grad 2 über $\mathbb{Q}$. Nach Bemerkung und Definition 6.24 ist

$$\mathbb{Q}[\sqrt{2}] = \operatorname{span}_{\mathbb{Q}}\{1, \sqrt{2}\} = \mathbb{Q} + \sqrt{2}\,\mathbb{Q}.$$

und nach Satz 6.25 ist $Q[\sqrt{2}]$ ein Unterkörper von $\mathbb{R}$.

2. 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 $\mathbb{Q}$). Analog zu 1. ist $\mathbb{Q}[\mathrm{i}] = \mathbb{Q} + \mathrm{i}\,\mathbb{Q}$ und $\mathbb{Q}[\mathrm{i}]$ ein Unterkörper von $\mathbb{C}$.

Bemerkung und Definition 6.27 Es sei K ein Körper. Dann heißt ein nichtkonstantes Polynom $P \in K[X]$ **irreduzibel** (über K) wenn gilt: Ist $P = QS$ mit $Q, S \in K[X]$, so ist Q konstant oder S konstant.[57]

Ist $\deg P \geq 2$ und hat P eine Wurzel $a \in K$, so sieht man mit Polynomdivision, dass P reduzibel (d. h. nicht irreduzibel) ist. Ist $\deg P \in \{2, 3\}$ und ist P reduzibel, so hat P eine Wurzel $a \in K$ ([Ü]).

[57] Man beachte die Analogie zu Primzahlen.

Mithilfe des nächsten Resultats kann man manchmal entscheiden, ob ein gegebenes Polynom ein Minimalpolynom ist.

Satz 6.28 *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 und Definition 6.24 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.[58] Wir zeigen abschließend

Satz 6.29 *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 $x \in K[x]$ und da $K[x]$ nach Satz 6.25 ein Körper ist auch $1/x \in K[x]$, also $1/x \in A$ nach Bemerkung 6.24. Wir setzen $m := \deg(x) - 1$ und $n := \deg(y) - 1$. Sind $M, N \in \mathbb{N}_0$, so gilt $x^M \in K[x]$ und $y^N \in K[y]$. Nach Bemerkung 6.24 existieren $a_\mu, b_\nu \in K$ mit $x^M = \sum_{\mu=0}^{m} a_\mu x^\mu$, $y^N = \sum_{\nu=0}^{n} b_\nu y^\nu$ und daher $x^M y^N = \sum_{\mu=0}^{m} \sum_{\nu=0}^{n} a_\mu b_\nu x^\mu y^\nu$. 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 $\big((xy)^j\big)_{j \in \mathbb{N}_0}$ und $((x-y)^j)_{j \in \mathbb{N}_0}$ linear abhängig. Mit Bemerkung 6.22.1. folgt $x - y, xy \in A$. □

[58] Im klassischen Fall $K = \mathbb{Q}$ und $E = \mathbb{R}$ ist also $A_E(K) = \mathbb{A}$.

7 Konstruierbare Zahlen

Zu den klassischen Fragen der Mathematik gehört die nach der Konstruierbarkeit von Punkten in der Ebene $\mathbb{E}$, etwa im Falle eines Dreiecks $\Delta(a,b,c)$ des Lotfußpunkts von c bzgl. $G(a,b)$ aus den Daten a,b,c.

Dabei stellt sich zunächst die Frage, was man unter konstruktiv verstehen könnte. Wir betrachten Konstruktionen mit Zirkel[59] und Lineal.[60]

Bemerkung und Definition 7.1 Es seien $A \subset \mathbb{E}$ nicht einelementig und $p \in \mathbb{E}$. Dann heißt p **direkt konstruierbar** aus A falls es $a, a', b, b', c, c' \in A$ mit $a \neq b$ und $a' \neq b'$ gibt für die eine der folgenden drei Bedingungen erfüllt ist:

(GK) $p \in K_{|\overline{ab}|}(c) \cap G(a',b')$.

(2G) $G(a,b) \neq G(a',b')$ und $p \in G(a,b) \cap G(a',b')$.

(2K) $K_{|\overline{ab}|}(c) \neq K_{|\overline{a'b'}|}(c')$ und $p \in K_{|\overline{ab}|}(c) \cap K_{|\overline{a'b'}|}(c')$.

Ist $a \in A$, so folgt aus (GK), angewandt mit $a' = a$, $b' = b$ und $c = b$, dass a direkt konstruierbar aus A ist. Mit $A_0 := A$ setzen wir

$$A_n := \{p \in \mathbb{E} : p \text{ direkt konstruierbar aus } A_{n-1}\}$$

für $n \in \mathbb{N}$. Dann ist $A_{n-1} \subset A_n$ für $n \in \mathbb{N}$. Ein Punkt $p \in \mathbb{E}$ heißt **konstruierbar** aus A falls ein n existiert mit $p \in A_n$. Eine typische und wichtige Konstruktion mit Zirkel und Lineal ist die des Mittelpunkts $(a+b)/2$ einer Strecke $\overline{ab}$.[61]

Ist $M \subset \mathbb{R}$ mit $\{0,1\} \subset M$, so heißt eine Zahl $x \in \mathbb{R}$ **konstruierbar** aus M, falls der Punkt $(x,0) \in \mathbb{R}^2$ aus $A = M \times \{0\}$ im obigen Sinne konstruierbar ist.[62] Wir setzen

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

Damit ist $M \subset \mathrm{kon}(M) = \mathrm{kon}(\mathrm{kon}(M))$.

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* $\sqrt{x} \in \mathrm{kon}(M)$.

[59] genauer mit einem sog. nichtkollabierenden Zirkel

[60] Der Lotfußpunkt von c bzgl. $G(a,b)$ lässt sich übrigens alleine mit Zirkel konstruieren.

[61] Für eine Konstruktion siehe etwa https://www.geogebra.org/m/Cwdzez2Q, Konstruktion der Mittelsenkrechten, wobei unter unseren Spielregeln nur $r = |\overline{ab}|$ zulässig ist.

[62] Die aus heutiger Sicht nur noch schwer nachvollziehbare fundamentale Bedeutung lag darin, dass in der Antike im Grunde genommen nur Punkte der "Zahlengerade", die aus $\mathbb{Z}$ oder $\mathbb{Q}$ konstruierbar sind, als Zahlen angesehen wurden.

Beweis. Wir schreiben $K := \mathrm{kon}(M)$. Sind $x, y \in K$, so ist auch $(x+y)/2 \in K$; vgl. Bemerkung und Definition 7.1. Mit (GK) sieht man, dass zudem $-x, 2x \in K$ gilt und daher ist auch $x+y \in K$ (also ist K eine Untergruppe von $(\mathbb{R}, +, 0)$). Wieder mit Konstruktion der Mittelsenkrechten kann man weiterhin zeigen, das der Punkt $(0,1) \in \mathbb{E}$ aus $(0,0), (1,0)$ konstruiert werden kann. Mit dem Satz von Thales und dem Höhensatz von Euklid sieht man dann, dass mit $0 < x \in K$ auch $\sqrt{x} \in K$ liegt. Nach Satz 3.10(iii) bleibt noch zu zeigen: Ist $x \neq 0$, so ist $y/x \in K$. Dies ist im Wesentlichen eine Folgerung aus dem Stahlensatz.[63] □

Bemerkung 7.3 Jeder Unterkörper von $\mathbb{R}$ enthält schon $\mathbb{Q}$. Nach Satz 7.2 gilt für beliebige Mengen $M \subset \mathbb{Q}$ mit $\{0,1\} \subset M$ damit schon $\mathrm{kon}(M) \supset \mathbb{Q}$, wobei $\mathrm{kon}(M)$ eine echte Obermenge von $\mathbb{Q}$ ist, da etwa $\sqrt{2} \in \mathrm{kon}(M)$. Außerdem ist $\mathrm{kon}(M) = \mathrm{kon}(\mathbb{Q})$ wegen $\mathrm{kon}(M) = \mathrm{kon}(\mathrm{kon}(M)) \supset \mathrm{kon}(\mathbb{Q})$.

Bemerkung 7.4 Es sei K ein Körper mit $1 + 1 \neq 0$.

1. Ist E eine Körpererweiterung von K mit $[E : K] = 2$, so existiert ein $a \in E \setminus K$ mit $a^2 \in K$ und $E = K + Ka$.

   Denn: Es sei $x \in E \setminus K$. Wegen der linearen Unabhängigkeit von $(1, x)$ über K ist $\{1, x\}$ eine Basis des zwei-dimensionalen K-Vektorraumes E. Folglich existieren $p, q \in K$ mit $x^2 + px + q = 0$. Wegen $2 := 1 + 1 \neq 0$ gilt für $a := x + p/2$

   $$a^2 = \left(x + \frac{p}{2}\right)^2 = \frac{p^2}{2^2} - q \quad \in K.$$

   Dabei ist $a \in E \setminus K$, also ist $(1, a)$ linear unabhängig und damit $\{1, a\}$ eine Basis von E.

2. Sind $K \subset \mathbb{R}$ und $x \in \mathbb{R}$ vom Grad ≤ 2 über K, so ist $x \in \mathrm{kon}(K)$, denn im Fall $x \in K$ ist die Behauptung klar, und im Fall $\deg x = 2$ ist mit $E := K[x]$ und a wie in 1. sowie Satz 7.2

   $$x \in K[x] = K + Ka = K[\sqrt{a^2}] \subset \mathrm{kon}(K).$$

Satz 7.5 *Es seien K ein Unterkörper von $\mathbb{R}$ und $x \in \mathbb{R}$. Dann sind äquivalent:*

(i) $x \in \mathrm{kon}(K)$.

(ii) *Es existieren ein $n \in \mathbb{N}$ und $\delta_1, \ldots, \delta_n \geq 0$ so, dass $x \in K_n$, wobei $K_j = K_{j-1}[\sqrt{\delta_j}]$, $K_0 := K$ Körper mit $\delta_j \in K_{j-1}$ für $j = 1, \ldots, n$ sind.*

[63] siehe etwa https://de.wikipedia.org/wiki/Konstruierbare_Zahl

Beweis. (ii) ⇒ (i): Nach Bemerkung 7.4.2 mit $x := \sqrt{\delta_j}$ ist

$$\sqrt{\delta_j} \in \mathrm{kon}(K_{j-1})$$

und dann auch $K_j = K_{j-1}[\sqrt{\delta_j}] \subset \mathrm{kon}(K_{j-1})$, da $\mathrm{kon}(K_{j-1})$ nach Satz 7.2 ein Oberkörper von K_{j-1} ist. Induktiv ergibt sich $K_n \subset \mathrm{kon}(K)$ und damit $x \in \mathrm{kon}(K)$.

(i) ⇒ (ii): Es genügt, zu zeigen: Ist U ein Unterkörper von $\mathbb{R}$ und ist ein Punkt $(x_1, x_2) \in \mathbb{E}$ direkt konstruierbar aus $U \times U$, so existiert ein $0 \leq \delta \in U$ mit $x_1, x_2 \in U[\sqrt{\delta}]$. Mehrfache Anwendung, startend mit $U = K$, ergibt dann die Behauptung, wobei zu beachten ist, dass $\sqrt{\delta}$ von Grad ≤ 2 über U ist und damit nach Satz 6.25 auch $U[\sqrt{\delta}]$ ein Körper ist.

Wir beweisen die Aussage durch Fallunterscheidung nach den drei Konstruktionsarten (2G), (GK) und (2K):

(2G): Ist $G = G(a, b)$ eine Gerade mit $a, b \in U^2$ und $a \neq b$, so ist $\mathbf{n} = (u_1, u_2) = (a_2 - b_2, b_1 - a_1) = \mathrm{i}(b - a) \in U^2$ ein Normalenvektor von G und die Normalengleichung von der Form

$$u_1 x_1 + u_2 x_2 + v = \langle \overrightarrow{ax}, \mathbf{n} \rangle = 0 \tag{7.1}$$

mit $v \in U$. Ein Schnittpunkt $x = (x_1, x_2) \in \mathbb{R}^2$ zweier solcher Geraden ist Lösung eines linearen Gleichungssystems mit Koeffizientenmatrix in $M_2(U)$ und rechter Seite in U^2 und liegt daher in U^2.

(GK): Sind $a, b, c \in U^2$ und $a \neq b$, so gilt $x \in K_{|\overline{ab}|}(c)$ genau dann, wenn

$$(x_1 - c_1)^2 + (x_2 - c_2)^2 = (b_1 - a_1)^2 + (b_2 - a_2)^2. \tag{7.2}$$

Ist $x \in G(a', b')$ mit $a', b' \in U^2$, so liefert Auflösen von (7.1) (mit a', b' statt a, b) ohne Einschränkung nach x_2 und Einsetzen in (7.2) eine quadratische Gleichung für x_1 mit Koeffizienten in U. Auflösen dieser über $\mathbb{R}$, falls möglich, liefert $x_1 \in U[\sqrt{\delta}]$ für ein $\delta \in U$ mit $\delta \geq 0$ (genauer ist δ die Diskriminante der quadratischen Gleichung). Mit (7.1) ist dann auch $x_2 \in U[\sqrt{\delta}]$.

(2K): Zwei Kreisgleichungen ergeben nach Subtraktion eine lineare Gleichung. Damit kann man (2K) auf den Fall (GK) zurückführen ([Ü]). □

Bemerkung 7.6 Es sei E eine endliche Körpererweiterung von K. Nach Bemerkung 6.22.2 ist jedes $x \in E$ algebraisch über K und nach Bemerkung 6.24 und Satz 6.25 $K[x] \subset E$ eine Körpererweiterung von K vom Grad $[K[x] : K] = \deg x$. Dabei ist E auch eine Körpererweiterung von $K[x]$ und mit Satz 6.18

$$[E : K] = \big[E : K[x]\big] \cdot \deg x.$$

Satz 7.7 *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 $\delta_0, \ldots, \delta_n$ wie in Satz 7.5. Dann ist $\sqrt{\delta_j}$ vom Grad ≤ 2 über K_{j-1}, also $[K_j : K_{j-1}] \in \{1, 2\}$. Nach Satz 6.18 ist

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

und folglich $[K_n : K]$ eine Zweierpotenz. Nach Bemerkung 7.6, angewandt auf $E := K_n$, ist $\deg x$ ein Teiler von $[K_n : K]$, also $\deg x = 2^m$ für ein $m \in \mathbb{N}_0$. □

Insbesondere ist $\mathrm{kon}(\mathbb{Q}) \subset \mathbb{A}$ nach Satz 7.7. Im Jahr 1882 bewies Ferdinand von Lindemann, dass die Kreiszahl π transzendent ist, also $\pi \in \mathbb{R} \setminus \mathbb{A}$ gilt. Insbesondere ist also $\pi \notin \mathrm{kon}(\mathbb{Q})$. Dies impliziert dies die Nichtlösbarkeit des klassischen Problems der **Quadratur des Kreises**.[64]

Bemerkung 7.8 Man kann zeigen ([Ü]): Ist $P \in \mathbb{Z}[X]$ normiert und ist $x \in \mathbb{Q}$ eine Wurzel von P, so ist $x \in \mathbb{Z}$. Durch Anwendung auf $P = X^n - a$ ergibt sich für $a, n \in \mathbb{N}$: Ist $\sqrt[n]{a}$ keine natürliche Zahl, so ist $\sqrt[n]{a}$ irrational und damit $\deg \sqrt[n]{a} \in \{2, \ldots, n\}$. Im Fall $n = 3$ ergibt sich aus Bemerkung und Definition 6.27 sowie Satz 6.28, dass $\deg \sqrt[3]{a} = 3$ ist ([Ü]).

Satz 7.9 *Ist $a \in \mathbb{N}$ und $\sqrt[3]{a} \notin \mathbb{N}$, so ist $\sqrt[3]{a} \notin \mathrm{kon}(\mathbb{Q})$.*

Beweis. Nach Bemerkung 7.8 ist $\sqrt[3]{a}$ vom Grad 3 über $\mathbb{Q}$. Insbesondere ist damit $\deg \sqrt[3]{a} = 3$ keine Zweierpotenz, also $\sqrt[3]{a} \notin \mathrm{kon}(\mathbb{Q})$ nach Satz 7.7. □

Eine weitere klassische Frage ist die nach der **Würfelverdopplung**, auch **Delisches Problem** genannt, bei dem aus einem gegebenen Würfel ein Würfel des doppelten Volumens konstruiert werden soll.[65] Die Lösbarkeit ist gleichbedeutend mit der Konstruierbarkeit von $\sqrt[3]{2}$ aus $\mathbb{Q}$ (bzw. $\{0, 1\}$). Nach Satz 7.9 ist dies nicht der Fall.

Wir betrachten ein drittes klassisches Konstruktionsproblem, die **Winkeldreiteilung**: Mit $E_\alpha := \mathrm{kon}(\{0, 1, \cos(\alpha)\})$, wobei $\alpha \in \mathbb{R}$, heißt ein Winkel der Winkelweite α **dreiteilbar** (mit Zirkel und Lineal), falls

$$\cos(\alpha/3) \in E_\alpha$$

[64] siehe etwa https://de.wikipedia.org/wiki/Quadratur_des_Kreises

[65] 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.

gilt.[66] Weiter schreiben wir $K_\alpha := \langle\{0, 1, \cos\alpha\}\rangle_{\text{Körper}}$ für den von $0, 1, \cos\alpha$ erzeugten Unterkörper von $\mathbb{R}$. Nach Definition ist $E_\alpha \subset \text{kon}(K_\alpha)$. Da E_α nach Satz 7.2 ein Unterkörper von $\mathbb{R}$ ist, der $0, 1, \cos\alpha$ enthält, ist andererseits $K_\alpha \subset E_\alpha$ und damit auch $\text{kon}(K_\alpha) \subset \text{kon}(E_\alpha) = E_\alpha$, also

$$E_\alpha = \text{kon}(K_\alpha).$$

Satz 7.10 (Winkeldreiteilung)
Für $\alpha \in \mathbb{R}$ gilt $\cos(\alpha/3) \in E_\alpha$ genau dann, wenn $X^3 - 3X - 2\cos\alpha \in K_\alpha[X]$ eine Wurzel in K_α hat.

Beweis. Wir setzen $P := X^3 - 3X - 2\cos\alpha$. Für $t \in \mathbb{R}$ gilt mit binomscher Formel

$$\begin{aligned}\cos(3t) &= \text{Re}(e^{3it}) = \text{Re}((e^{it})^3) = \text{Re}((\cos t + \mathrm{i}\sin t)^3)\\ &= \cos^3 t - 3\cos t\sin^2 t = \cos^3 t - 3\cos t\,(1 - \cos^2 t)\\ &= 4\cos^3 t - 3\cos t,\end{aligned}$$

also mit $t = \alpha/3$

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

Folglich ist $x := 2\cos(\alpha/3)$ eine Wurzel von $P \in K_\alpha[X]$, also x vom Grad ≤ 3 über K_α. Wegen $\text{kon}(K_\alpha) = E_\alpha$ und mit Bemerkung 7.4 und Satz 7.7 ist $x \in E_\alpha$ (bzw. äquivalent $\cos(\alpha/3) \in E_\alpha$) genau dann, wenn x nicht vom Grad 3 über K_α ist. Nach Satz 6.28 ist dies genau dann der Fall, wenn P reduzibel über K_α ist und nach Bemerkung und Definition 6.27 ist dies wiederum genau dann der Fall, wenn P eine Wurzel in K_α hat. □

Beispiel 7.11 Es gilt $\cos(\pi/3) = 1/2$, also ist hier $K_\alpha = \mathbb{Q}$ und zudem

$$P = X^3 - 3X - 1 \in \mathbb{Z}[X] \subset \mathbb{R}[X].$$

Wegen

$$P(-2) = -3,\ P(-1) = 1,\ P(0) = -1,\ P(1) = -3,\ P(2) = 1$$

hat $\hat{P}$ nach dem Zwischenwertsatz drei Nullstellen in $\mathbb{R} \setminus \mathbb{Z}$, also hat P keine Wurzel in $\mathbb{Z}$ und folglich nach Bemerkung 7.8 keine Wurzel in $\mathbb{Q} = K_\alpha$. Satz 7.10 impliziert, dass der Winkel $\pi/3$ nicht dreiteilbar ist.[67]

[66] Mit Satz 7.2 ist dann auch $\sin(\alpha/3) \in \{\pm\sqrt{1 - \cos^2(\alpha/3)}\} \subset E_\alpha$.

[67] Im Jahre 1837 publizierte Pierre-Laurent Wantzel den ersten Beweis der Unmöglichkeit einer solchen Konstruktion und den ersten Beweis der Unmöglichkeit der Würfelbverdopplung.

Index