Jürgen Müller

Elementare Zahlentheorie und Algebra

Skriptum zur Vorlesung
Wintersemester 2011/2012

Universität Trier
Fachbereich IV
Mathematik/Analysis

Inhaltsverzeichnis

1 Teilbarkeit und Primzahlen

Wir starten mit einigen einfachen Resultaten zur Teilbarkeit ganzer Zahlen. Dazu gehen wir (noch einmal) kurz auf die Definition, d.h. das ,,Wesen" natürlicher bzw. ganzer Zahlen ein.
Die Menge $\mathbb{N}$ der natürlichen Zahlen kann axiomatisch beschrieben werden durch die Bedingungen (Peano-Axiome):

(N1) $\mathbb{N}$ enthält ein Element, genannt 1.

(N2) Es gibt eine injektive Abbildung $N : \mathbb{N} \to \mathbb{N}$ mit $1 \notin N(\mathbb{N})$ (N für ,,Nachfolger").

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

Damit kann man zeigen: Es existieren eindeutig bestimmte Abbildungen $+$ und $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ so, dass

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

und

$$\begin{aligned} m \cdot 1 &= m, \\ m \cdot N(n) &= mn + m. \end{aligned}$$

Außerdem sind damit die üblichen Relationen $<$ und $\leq$ gegeben durch

$$n < m :\Leftrightarrow \exists\, k \in \mathbb{N} : m = n + k$$

und

$$n \leq m :\Leftrightarrow n < m \text{ oder } n = m.$$

Schließlich gilt das Wohlordnungsprinzip: Jede Menge $\emptyset \neq A \subset \mathbb{N}$ hat ein Minimum.

Die Menge $\mathbb{Z}$ der ganzen Zahlen lässt sich durch Äquivalenzklassenbildung in $\mathbb{N} \times \mathbb{N}$ so erzeugen, dass die Rechenregeln $+$ und $\cdot$ und die Ordnungsrelation $<$ sich übertragen ($\to$ Einführung in die Mathematik). Jede nichtleere Menge $A \subset \mathbb{Z}$ hat ein Minimum, falls sie nach unten beschränkt ist und ein Maximum, falls sie nach oben beschränkt ist.

Definition 1.1 Es seien $a, b \in \mathbb{Z}$. Man sagt, a sei *Teiler von* b (bzw. a *teilt* b), falls ein $q \in \mathbb{Z}$ existiert mit $b = q \cdot a$. Man schreibt dann $a|b$. Anderenfalls schreiben wir $a \nmid b$
Ist $B \subset \mathbb{Z}$ eine Menge, so schreiben wir $a|B$, falls $a|b$ für jedes $b \in B$ gilt (d. h. falls $B \subset a\mathbb{Z}$).

Es gilt damit ([Ü]):

Satz 1.2 *1. Für alle $b \in \mathbb{Z}$ gilt $\pm 1|b$ und $\pm b|b$.*

2. Sind $a, b, c \in \mathbb{Z}$, so folgt aus $a|b$ und $b|c$ auch $a|c$.

3. Sind $a, b_j \in \mathbb{Z}$ für $j = 1, \ldots, n$ mit $a|b_j (j = 1, \ldots, n)$, so gilt

$$a \Big| \sum_{j=1}^{n} b_j x_j \qquad \text{für alle } x_1, \ldots, x_n \in \mathbb{Z}$$

oder, m.a.W., $a| \sum_{j=1}^{n} b_j \mathbb{Z}$.

4. Aus $a|b$ folgt $b = 0$ oder $|a| \leq |b|$.

Satz 1.3 *(Division mit Rest)*
Es sei $(a, b) \in \mathbb{Z}^2, a \neq 0$. Dann existiert (genau) ein Paar $(q, r) \in \mathbb{Z}^2$ mit $b = qa + r$ und $0 \leq r < |a|$.

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

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

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

Als Anwendung beweisen wir folgendes Ergebnis über die Darstellung natürlicher Zahlen:

Es sei $q \in \mathbb{N}, q \geq 2$. Dann existert für alle $n \in \mathbb{N}_0$ genau eine Folge $(a_j) = \big(a_j(n)\big)$ in $\{0, \ldots, q-1\}$ mit $a_j = 0$ bis auf endlich viele j und so, dass

$$n = \sum_{j=0}^{\infty} a_j(n) q^j.$$

(Denn: 1. Existenz.
$n = 0$: $a_j(0) = 0$ $(j \in \mathbb{N}_0)$ ist geeignet.
$n - 1 \to n$: Wir wählen $k \in \mathbb{N}_0$ so, dass $q^k \leq n < q^{k+1}$. Division mit Rest ergibt

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

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

$$n' = \sum_{j=0}^{\infty} a_j(n') q^j.$$

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

$$n = mq^k + n' = \sum_{j=0}^{\infty} a_j(n) q^j.$$

2. Eindeutigkeit: Es seien $(a_j), (\widetilde{a}_j)$ abbrechende Folgen in $\{0, \ldots, q-1\}$ mit $n = \sum\limits_{j=0}^{\infty} a_j q^j = \sum\limits_{j=0}^{\infty} \widetilde{a}_j q^j$. Angenommen, es existiert ein $j \in \mathbb{N}_0$ mit $a_j \neq \widetilde{a}_j$. Dann gilt für $m := \max\{j : a_j \neq \widetilde{a}_j\}$ (ohne Einschränkung $a_m > \widetilde{a}_m$)

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

Widerspruch.)

Mit obigen Bezeichnungen ist die Abbildung

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

bijektiv. (Für $M \subset \mathbb{Z}$ bezeichnet dabei $M^{[\mathbb{N}_0]}$ die Menge der abbrechenden Folgen in M, d. h. die Menge aller Folgen, für die nur endlich viele Folgeglieder $\neq 0$ sind.)
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 $q = 10$ (besser vielleicht: $q = \mathrm{X}$) spricht man auch von der Dezimal-, im Falle $q = 2$ von der Binär- und im Falle $q = 16$ von der Hexadezimaldarstellung. Schließlich schreibt man im Dezimalfall auch kurz $a_r \dots a_0$ statt $(a_r \dots a_0)_{10}$.

Definition 1.4 Es seien $a, b \in \mathbb{Z}, a \neq 0$ oder $b \neq 0$. Dann heißt

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

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

Satz 1.5 *Es seien $a, b \in \mathbb{Z}$ und es sei $d := ggT(a, b)$. Dann ist*

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

Insbesondere gilt $ggT(a, b) = 1$ genau dann, wenn $1 \in a\mathbb{Z} + b\mathbb{Z}$.

Beweis. Ist $ab = 0$, so ist die Behauptung trivial (nach Definition ist dann $d = 0$) .
Es seien also $a \neq 0$ und $b \neq 0$. Wir setzen

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

Dann gilt : $m\mathbb{Z} \subset L \subset d\mathbb{Z}$ und insbesondere $d|m$.
(Denn: Aus $d|a$ und $d|b$ folgt $d|(a\mathbb{Z} + b\mathbb{Z})$ nach S. 1.2.3. Also ist $L \subset d\mathbb{Z}$ und $d|m$. Außerdem gilt $m \cdot \mathbb{Z} \subset (a\mathbb{Z} + b\mathbb{Z})\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z} = L$.)
Weiter ist $m|a$.
(Denn: Ist $a = qm + r$ nach S. 1.3, so ist $r = a - mq \in a - m\mathbb{Z} \subset L - L = L$ und $0 \leq r < |m|$, also $r = 0$ nach Definition von m. Also ist m Teiler von a.)
Genauso ist $m|b$, also ist $m \leq \mathrm{ggT}(a, b) = d$. Mit $d|m$ folgt $d = m$ und damit auch $d\mathbb{Z} = m\mathbb{Z} \subset L$. □

Als Folgerung ergibt sich

Satz 1.6 *Es seien $a, b, c \in \mathbb{Z}$ mit $ggT(a, b) = 1$. Dann gilt:*

1. *Ist $a|bc$, so ist $a|c$.*
2. *Ist $a|c$ und $b|c$, so ist $ab|c$.*
3. *Ist $ggT(a, c) = 1$, so ist auch $ggT(a, bc) = 1$.*

Beweis.

1. Nach Satz 1.5 existieren $x, y \in \mathbb{Z}$ mit $ax + by = 1$, also $c = axc + byc$. Da $a|bc$ und $a|a$, gilt $a|c$ nach Satz 1.2.3.
2. Wie in 1. ist $c = axc + byc$. Da $c = ua = bv$ für gewisse $u, v \in \mathbb{Z}$ gilt, folgt
$$c = xabv + byua = ab(xv + yu).$$
3. Nach Voraussetzung ist $1 = ax + by = au + cv$ für gewisse $x, y, u, v \in \mathbb{Z}$. Also folgt
$$1 = (by + ax)(cv + au) = (bc)(yv) + a(xcv + uby + axu)$$
d.h. $1 \in bc\mathbb{Z} + a\mathbb{Z}$. Nach S. 1.5 sind a und bc teilerfremd.

□

Bemerkung 1.7 Ein Verfahren zur Berechnung des ggT(a, b) ist der Euklidsche Algorithmus.
Sind $a, b \in \mathbb{Z} \setminus \{0\}$, so wendet man sukzessive Division mit Rest an, startend mit $r_0 = b, r_1 = |a|$:

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

Da nach Satz 1.3 dabei $r_1 > r_2 > \cdots (\geq 0)$ gilt, bricht das Verfahren nach endlich vielen Schritten ab (d. h. $r_{n+1} = 0$ für ein $n \in \mathbb{N}$). Also ergibt sich als letzte Gleichung

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

Dabei gilt $r_n = \mathrm{ggT}(a, b)$.
(Denn: Einerseits sieht man durch Lesen des Gleichungssystems von unten nach oben: $r_n | r_{n-1}, \ldots, r_n | r_1, r_n | r_0$, also r_n Teiler von a und b.
Andererseits ist, wie man durch Lesen des Gleichungssystems von oben nach unten sieht, $r_2 \in a\mathbb{Z} + b\mathbb{Z}, \ldots, r_n \in a\mathbb{Z} + b\mathbb{Z}$. also $r_n \in \mathrm{ggT}(a, b)\mathbb{Z}$ nach Satz 1.5. Da r_n Teiler von a, b ist, ist $r_n = \mathrm{ggT}(a, b)$.)

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

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

Bemerkung und Definition 1.8 Eine Zahl $p \in \mathbb{N} \setminus \{1\}$ heißt *Primzahl*, falls p nur die Teiler ± 1 und $\pm p$ hat. Wir setzen

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

.
Es gilt dabei: Sind $b, c \in \mathbb{Z}$, so folgt aus $p|bc$ schon $p|b$ oder $p|c$.
(Denn: Ist p kein Teiler von b, so ist $\mathrm{ggT}(b, p) = 1$. Also gilt $p|c$ nach Satz 1.6.2.)
Allgemeiner ergibt sich daraus: Ist $B \subset \mathbb{Z}$ endlich, so folgt aus $p| \prod_{b \in B} b$ schon $p|b$ für ein $b \in B$.

Satz 1.9 *(Primfaktorzerlegung, Fundamentalsatz der Arithmetik)*
Für alle $n \in \mathbb{N} \setminus \{1\}$ existieren genau eine endliche Menge $E(n) \subset \mathbb{P}$ und ein Tupel $\big(\alpha_p(n)\big)_{p \in E(n)}$ natürlicher Zahlen mit

$$\boxed{n = \prod_{p \in E(n)} p^{\alpha_p(n)}.}$$

Setzt man noch $E(1) := \emptyset$ und $\alpha_p(n) := 0$ für $p \in \mathbb{P} \setminus E(n)$, so gilt damit für alle $n \in \mathbb{N}$

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

(man beachte: nur endlich viele Faktoren sind $\neq 1$ und $E(n) = \{p \in \mathbb{P} : p|n\}$). Außerdem gilt damit: Ist $\mathbb{N}_0^{[\mathbb{P}]}$ die Menge aller $\nu = (\nu_p)_{p\in\mathbb{P}}$ mit $\nu_p \in \mathbb{N}_0$ und $\nu_p = 0$ bis auf endliche viele p, so ist die Abbildung

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

bijektiv mit Umkerabbildung

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

Beweis. (zu S. 1.9) 1. Existenz:
Ist n Primzahl, so ist die Behauptung klar. Ist n keine Primzahl, so existiert ein Primteiler p von n.
(Denn: $p := \min\{k > 1 : k|n\}$ ist 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.)
Also ist $n = pn'$ für ein $n' \in \mathbb{N}$ mit $1 < n' < n$.
Mit der gleichen Arumentation gilt: $n' \in \mathbb{P}$ oder es existiert ein $p' \in \mathbb{P}$ mit $n' = p'n''$ und $1 < n'' < n'$. So fortfahrend erhält man eine Darstellung von n als Produkt von Primzahlen.

2. Eindeutigkeit:
Wir zeigen per Induktion nach $k \in \mathbb{N}$:
Ist $n = \prod_{p\in E} p^{\nu_p}$ mit $E \subset \mathbb{P}$ endlich, $\nu_p \in \mathbb{N}$ sowie $\sum_{p\in E} \nu_p = k$, und ist $n = \prod_{q\in F} q^{\mu_q}$ mit $F \subset \mathbb{P}$ endlich und $\mu_q \in \mathbb{N}$, so gilt $E = F$ und $\mu_p = \nu_p$ für $p \in E(= F)$.
$k = 1 : n = p$ ist Primzahl und damit nicht als Produkt mehrerer Primzahlen darstellbar.
$k \to k+1$: Es sei $n = \prod_{p\in E} p^{\nu_p} = \prod_{q\in F} q^{\mu_q}$ mit $\sum_{p\in E} \nu_p = k+1$. Ist $p_0 \in E$, so folgt aus $p_0 \Big| \prod_{q\in F} q^{\mu_q}$ mit B/D 1.8 schon $p_0|q_0$ für ein $q_0 \in F$. Damit ist $q_0 = p_0$ (da q_0 Primzahl).
Also gilt

$$\left(\prod_{p\in E\setminus\{p_0\}} p^{\nu_p}\right) p_0^{\nu_{p_0}-1} = \left(\prod_{q\in F\setminus\{q_0\}} q^{\mu_q}\right) q_0^{\mu_{q_0}-1}.$$

Aus $\left(\sum_{p\in E\setminus\{p_0\}} \alpha_p\right) + \alpha_{p_0} - 1 = k$ folgt nach Induktionsvoraussetzung $E = F$ und $\nu_p = \mu_p$ $(p \in E)$. □

Wir wollen uns etwas mit der Frage der ,,Häufigkeit" von Primzahlen in $\mathbb{N}$ beschäftigen. Zunächst gilt

Satz 1.10 *(Euklid)*

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

Beweis. Angenommen, $\mathbb{P}$ ist endlich. Für $N := 1 + \prod_{p\in\mathbb{P}} p$ gilt dann: p ist kein Teiler von N für alle $p \in \mathbb{P}$ (sonst wäre $p|(N - \prod_{p\in\mathbb{P}} p = 1)$). Also hat N keine Primteiler. Widerspruch zu Satz 1.9. □

Genauer als in Satz 1.10 gilt

Satz 1.11

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

Beweis. Für $E \subset \mathbb{P}$ endlich sei

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

Dann gilt $\bigcup_{E\subset\mathbb{P},|E|<\infty} M_E = \mathbb{N}$ nach S. 1.9. Hieraus folgt

$$\sup_{E\subset\mathbb{P},|E|<\infty} \sum_{n\in M_E} \frac{1}{n} = \infty\,.$$

(Denn: Ist $R > 0$, so existiert ein $F \subset \mathbb{N}$ endlich mit $\sum_{n\in F} 1/n \geq R$. Ist $E \subset \mathbb{P}$ endlich mit $F \subset M_E$, so folgt $\sum_{n\in M_E} 1/n \geq R$.)

Weiter gilt mit der Eindeutigkeitsaussage aus S. 1.9 und $\dfrac{1}{1-x} \leq e^{2x}$ für $0 \leq x \leq 1/2$

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

Damit ergibt sich $\sum_{n\in M_E} 1/n < \infty$ und

$$\infty = \sup_{E\subset\mathbb{P},|E|<\infty} \frac{1}{2} \log \left(\sum_{n\in M_E} \frac{1}{n} \right) \leq \sum_{p\in\mathbb{P}} \frac{1}{p}.$$

□

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

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

(wobei $f(x) \sim g(x)$ bedeutet, dass $\dfrac{f(x)}{g(x)} \to 1\,(x \to \infty)$ gilt.)

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

Satz 1.12 *Für alle $n \in \mathbb{N}$ und $p \in \mathbb{P}$ gilt*

$$\alpha_p(n!) = \sum_{\nu=1}^{\infty} \left[\frac{n}{p^\nu}\right] \quad \left(= \sum_{\nu=1}^{\left[\frac{\log n}{\log p}\right]} \left[\frac{n}{p^\nu}\right] \right).$$

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

$$\left[\frac{n}{a}\right] = \Big|\{k \in \{1, \ldots, n\} : a|k\}\Big|.$$

Damit erhält man

$$\alpha_p(n!) = \sum_{k=1}^{n} \alpha_p(k) = \sum_{k=1}^{n} \sum_{\nu : p^\nu | k} 1 = \sum_{\nu=1}^{\left[\frac{\log n}{\log p}\right]} \sum_{\substack{k=1 \\ p^\nu | k}}^{n} 1 = \sum_{\nu=1}^{\left[\frac{\log n}{\log p}\right]} \left[\frac{n}{p^\nu}\right].$$

□

Wir zeigen damit

Satz 1.13 *(Tschebyscheff)*
Für $n \in \mathbb{N}, n \geq 2$ gilt

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

Beweis. 1. Zunächst gilt für $x \geq 0$

$$[2x] - 2[x] = \begin{cases} 0, & \text{falls } x - [x] < 1/2 \\ 1, & \text{falls } x - [x] \geq 1/2 \end{cases}$$

und damit nach S. 1.12

$$\begin{aligned} s_n &:= \log\big((2n)!\big) - 2\log(n!) = \sum_{\substack{p\in\mathbb{P}\\(p\leq 2n)}} \alpha_p\big((2n)!\big)\,\log p - 2\sum_{\substack{p\in\mathbb{P}\\(p\leq n)}} \alpha_p(n!)\log p \\ &= \sum_{\mathbb{P}\ni p\leq 2n} \sum_{\nu=1}^{\left[\frac{\log 2n}{\log p}\right]} \underbrace{\left(\left[\frac{2n}{p^\nu}\right] - 2\left[\frac{n}{p^\nu}\right]\right)}_{\in\{0,1\}} \log p\,. \end{aligned}$$

Aus

$$2^n \leq \frac{n+1}{1}\cdots\frac{2n-1}{n-1}\cdot\frac{2n}{n} = \binom{2n}{n} \leq \sum_{k=0}^{2n}\binom{2n}{k} = (1+1)^{2n} = 2^{2n}$$

folgt

$$n\log 2 \leq \log\binom{2n}{n} = s_n \leq 2n\log 2$$

2. Mit 1. erhält man

$$n\log 2 \leq \sum_{\mathbb{P}\ni p\leq 2n} \underbrace{\left[\frac{\log 2n}{\log p}\right]\log p}_{\leq \log(2n)} \leq \pi(2n)\log(2n)$$

Aus $\log 2 > 1/2$ ergibt sich

$$\pi(2n) > \frac{n\log 2}{\log(2n)} > \frac{1}{4}\,\frac{2n}{\log(2n)}$$

und weiter

$$\pi(2n+1) > \pi(2n) > \frac{n\log 2}{\log(2n)} > \underbrace{\frac{n\log 2}{2n+1}}_{\geq 1/4 (n\geq 2)}\,\frac{2n+1}{\log(2n+1)} \geq \frac{1}{4}\,\frac{2n+1}{\log(2n+1)}.$$

Dies ist die linke Ungleichung.

3. Wir setzen

$$\vartheta(x) := \sum_{\substack{p\in\mathbb{P}\\p\leq x}} \log p \qquad (x \geq 0).$$

Sind $n \in \mathbb{N}$ und $p \in \mathbb{P}$ mit $n < p \leq 2n$, so ist $1/2 \leq n/p < 1$, also

$$\left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right] = 1$$

und damit nach 1.

$$\vartheta(2n) - \vartheta(n) = \sum_{p\in\mathbb{P},\, n<p\leq 2n} \log p \leq \sum_{p\in\mathbb{P}, p\leq 2n} \left(\left[\frac{2n}{p}\right] - 2\left[\frac{n}{p}\right]\right) \log p \leq s_n \leq 2n \log 2\,.$$

Insbesondere ist für beliebiges $k \in \mathbb{N}_0$

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

also

$$\vartheta(2^{k+1}) \underset{\vartheta(1)=0}{=} \sum_{\ell=0}^{k} \big(\vartheta(2^{\ell+1}) - \vartheta(2^\ell)\big) \leq \sum_{\ell=0}^{k} 2^{\ell+1} \log 2 = 2\log 2(2^{k+1} - 1) \leq 2^{k+2} \log 2.$$

Es sei nun wieder $n \in \mathbb{N}$ gegeben. Ist k so, dass $2^k \leq n < 2^{k+1}$ und $0 < y < n$, so ergibt sich

$$\big(\pi(n) - \pi(y)\big) \log y \leq \sum_{p\in\mathbb{P}, y<p\leq n} \log p \leq \vartheta(n) \leq \vartheta(2^{k+1}) \leq 2^{k+2} \log 2 \leq 4n \log 2.$$

Wählt man etwa $y = n^{2/3}$, so erhält man

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

also

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

Da $x \mapsto \dfrac{\log x}{x^{1/3}}$ bei $x = e^3$ maximal wird ([Ü]), folgt

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

□

Bemerkung 1.14 Ein äußerst schwieriges Problem ist die konkrete Bestimmung großer Primzahlen. Ein möglicher Ansatz liegt darin, Primzahlen der Form

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

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

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

(Denn:
1. Ist $k \notin \mathbb{P}, k \neq 1$, so ist $k = r \cdot s$ mit gewissen $r, s \in \mathbb{N} \setminus \{1\}$. Also folgt

$$2^k - 1 = (2^r)^s - 1 = \underbrace{(2^r - 1)}_{>1} \underbrace{\sum_{j=0}^{s-1} 2^{j \cdot r}}_{>1} \notin \mathbb{P}.$$

2. Zunächst gilt: Ist $s > 1$ ungerade und $a \in \mathbb{N} \setminus \{1\}$, so ist

$$a^s + 1 = -(-a^s - 1) = -((-a)^s - 1) = (a+1) \underbrace{\sum_{j=0}^{s-1} (-a)^j}_{>1} \notin \mathbb{P}.$$

Also: Ist $k \neq 2^n$ für alle $n \in \mathbb{N}_0$, so ist $k = 2^m s$ für ein $m \in \mathbb{N}_0$ und ein $s > 1$, s ungerade. Damit ist $2^k + 1 = (2^{2^m})^s + 1 \notin \mathbb{P}$.)
Die Zahl $M_p := 2^p - 1$ mit $p \in \mathbb{P}$ heißt p-te Mersenne-Zahl, $F_n := 2^{2^n} + 1$ heißt n-te Fermat-Zahl. Man kann zeigen:

1. Es gilt $M_p \in \mathbb{P}$ unter anderem für $p \in \{2, 3, 5, 7, 13, 17, 19, 31\}$. Insgesamt sind heute (Stand 11.11) 47 Mersenne-Primzahlen bekannt. Die größte davon ist $2^{43112609} - 1$ mit 12978189 Stellen im Dezimalsystem!

   Andererseits ist $2^{11} - 1 = 2047 = 23 \cdot 89$, also $M_{11} \notin \mathbb{P}$.

   Bis heute ist unbekannt, ob es unendlich viele der M_p prim sind und auch ob unendlich viele nicht prim sind.

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

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

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

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

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

2 Algebraische Strukturen und Modulorechnung

Um die weitere Vorlesung auf ein gemeinsames Fundament zu stellen, wiederholen wir die Definitionen zentraler algebraischer Strukturen, die (zum Teil) aus den Grundvorlesungen bekannt sind.

Definition 2.1 Es seien $G \neq \emptyset$ eine Menge und $* : G \times G \to G$ eine Abbildung. Dann heißt $(G, *)$ *Gruppe*, falls gilt:

(G.1) (Assoziativgesetz) Für alle $x, y, z \in G$ ist

$$(x * y) * z = x * (y * z).$$

(G.2) Es existiert ein $e \in G$ mit

(G.2.1) $x * e = x$ für alle $x \in G$ (ein solches e heißt *rechtsneutral*).

(G.2.2) Für alle $x \in G$ existiert ein $y \in G$ mit $x * y = e$ (ein solches y heißt *rechtsinvers* zu x (bzgl. e)).

Gilt zudem

(G.3) (Kommutativgesetz) Für alle $x, y \in G$ ist

$$x * y = y * x,$$

so heißt $(G, *)$ *abelsch* (oder *kommutativ*).
Wir schreiben auch kurz G statt $(G, *)$ und xy statt $x * y$.

Bemerkung 2.2 1. Man kann zeigen, dass nur ein e wie in (G.2) existiert und dass dieses e auch linksneutral ist, d. h. $e * x = x$ für alle $x \in G$. Genauso existiert zu jedem $x \in G$ nur ein Rechtsinverses (genannt x^{-1}), und dieses ist auch linksinvers, d. h. $x^{-1} * x = e$.
2. Für alle $a, b \in G$ sind die Gleichungen $a * x = b$ und $y * a = b$ eindeutig lösbar mit den Lösungen

$$x = a^{-1} * b \qquad \text{und} \qquad y = b * a^{-1}.$$

3. Für alle $a, b \in G$ ist $(a^{-1})^{-1} = a$ und $(a * b)^{-1} = b^{-1} * a^{-1}$.

Beispiele 2.3 1. $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),(\mathbb{C},+)$ sind abelsche Gruppen.
2. $(\mathbb{Q}\setminus\{0\},\cdot),(\mathbb{R}\setminus\{0\},\cdot),(\mathbb{C}\setminus\{0\},\cdot)$ sind abelsche Gruppen.
3. Ist $M\neq\emptyset$ ein Menge, so setzen wir

$$S(M):=\{f:M\to M, f \text{ bijektiv}\}\ .$$

Dann ist $(S(M),\circ)$, wobei $\circ$ die Hintereinanderausführung bezeichnet, eine Gruppe. Ist $n\in\mathbb{N}$, so schreiben wir $S_n:=S(\{1,\ldots,n\})$. Für $n\geq 3$ ist S_n nicht abelsch. Die Gruppe $(S_n,\cdot)$ heißt symmetrische Gruppe, jedes $\sigma\in S_n$ heißt eine Permutation von $\{1,\ldots,n\}$.

Definition 2.4 Es sei $R\neq\emptyset$ eine Menge und es seien $+:R\times R\to R$ und $\cdot:R\times R\to R$ Abbildungen. Dann heißt $R=(R,+,\cdot)$ *Ring*, falls gilt:

(R.1) $(R,+)$ ist eine abelsche Gruppe (Schreibweise: $0=0_R$ für neutrales Element; $-x$ für Inverses von x).

(R.2) (Assoziativgesetz für $\cdot$) Für alle $x,y,z\in R$ ist $x\cdot(y\cdot z)=(x\cdot y)\cdot z$.

(R.3) (Distributivgesetze) Für alle $x,y,z\in R$ ist

$$(x+y)\cdot z=(x\cdot z)+(y\cdot z)$$
$$x\cdot(y+z)=(x\cdot y)+(x\cdot z)$$

Gilt zudem

(R.4) (Kommutativgesetz für $\cdot$) Für alle $x,y\in R$ ist

$$x\cdot y=y\cdot x,$$

so heißt $(R,+,\cdot)$ *kommutativ*.
Man schreibt kurz: xy statt $x\cdot y$, $x-y$ statt $x+(-y)$ und $x+yz$ statt $x+(y\cdot z)$.

Bemerkung 2.5 In Ringen R gilt für $x,y,z\in R$:

1. $0\cdot x=x\cdot 0=0$.
2. $(-x)y=x(-y)=-(xy)$ $(=:-xy)$.
3. $(-x)(-y)=xy$.

4. $x(y-z) = xy - xz$ und $(x-y)z = xz - yz$.

Definition 2.6 Es sei $(R, +, \cdot)$ ein Ring. Dann heißt

1. $(R, +, \cdot)$ *nullteilerfrei*, falls aus $xy = 0$ schon $x = 0$ oder $y = 0$ folgt.
2. $1 = 1_R \in R$ *Einselement*, falls $1 \cdot x = x \cdot 1 = x$ $(x \in R)$.
3. $(R, +, \cdot)$ ein *Integritätsring* (oder *Integritätsbereich*), falls $(R, +, \cdot)$ nullteilerfreier, kommutativer Ring mit Einselement $1 \neq 0$ ist.
4. $(R, +, \cdot)$ ein *Körper*, falls $(R, +, \cdot)$ kommutativer Ring mit Einselement $(\neq 0)$ und $(R \setminus \{0\}, \cdot)$ eine (dann auch abelsche) Gruppe ist (m. a. W. zu jedem $x \in R \setminus \{0\}$ existiert x^{-1}).

Beispiele 2.7 1. $(\mathbb{Z}, +, \cdot)$ ist ein Integritätsbereich, aber kein Körper.
2. $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ sind Körper.
3. Es seien R ein Ring und M eine nichtleere Menge. Wir definieren

$$R^M := \{f : M \to R\}$$

und für $f, g \in R^M$ die Funktionen $f + g \in R^M$ und $f \cdot g \in R^M$ (wie üblich) durch $(f+g)(x) := f(x) + g(x)$ und $(f \cdot g)(x) := f(x) \cdot g(x)$ für $x \in M$.
Damit ist $R^M = (R^M, +, \cdot)$ ein Ring mit Nullelement 0_{R^M}, definiert durch $0_{R^M}(x) = 0_R$ für $x \in M$. Ist R kommutativ, so ist auch R^M kommutativ. Hat R ein Einslement 1_R, so ist durch $1_{R^M}(x) := 1_R$ für $x \in M$ ein Einselement in R^M gegeben. Ist $|R| \geq 2$ und $|M| \geq 2$, so ist R^M nicht nullteilerfrei.

Bemerkung 2.8 1. Jeder Körper ist Integritätsbereich (d. h. nullteilerfrei).
2. Ein Ring ist genau dann nullteilerfrei, wenn folgende Kürzungsregel gilt: Aus $xy = xz$ folgt $x = 0$ oder $y = z$ und aus $xz = yz$ folgt $z = 0$ oder $x = y$.

Definition 2.9 Es seien $K = (K, +, \cdot) = (K, +_K, \cdot_K)$ ein Körper und $V \neq \emptyset$ eine Menge. Ferner seien zwei Abbildungen $+(= +_V) : V \times V \to V$ und $\cdot(= \cdot_V) : K \times V \to V$ gegeben. Dann heißt $V = (V, +, \cdot)$ ein *K-Vektorraum* (oder *K-linearer Raum*), falls gilt

(V1) $(V, +)$ ist eine abelsche Gruppe.

(V2) Für alle $\lambda, \mu \in K, x \in V$ ist

$$\lambda \cdot (\mu \cdot x) = (\lambda \cdot_K \mu) \cdot x.$$

(V3) Für alle $x \in V$ ist $1_K \cdot x = x$.

(V4) (Distributivgesetz) Für alle $\lambda, \mu \in K, x, y \in V$ ist

$$\lambda \cdot (x + y) = \lambda \cdot x + \lambda \cdot y,$$
$$(\lambda +_K \mu) \cdot x = \lambda \cdot x + \mu \cdot x.$$

Die Elemente von V heißen dabei *Vektoren* und die Elemente aus K *Skalare*.
Für Rechenregeln (analog zu B. 2.5) verweisen wir auf die lineare Algebra. Insbesondere gilt: Aus $\lambda \cdot x = 0$ folgt $\lambda = 0$ oder $x = 0$.

Beispiel 2.10 Ist K ein Körper, so ist für alle $n \in \mathbb{N}$

$$K^n := \{x = (x_1, \ldots, x_n) : x_j \in K \, (j = 1, \ldots, n)\}$$

mit

$$K^n \times K^n \ni (x, y) \mapsto x + y := (x_1 +_K y_1, \ldots, x_n +_K y_n) \in K^n$$
$$K \times K^n \ni (\lambda, x) \mapsto \lambda \cdot x := (\lambda \cdot_K x_1, \ldots, \lambda \cdot_K x_n) \in K^n$$

ein K-Vektorraum.
Allgemeiner ist für $M \neq \emptyset$ auch $(K^M, +, \cdot)$, wobei $+$ wie in B. 2.7.3 und $\cdot : K \times K^M \to K^M$, definiert ist durch

$$(\lambda \cdot f)(x) := \lambda \cdot f(x) \qquad (x \in M),$$

ein K-Vektorraum.

Definition 2.11 Ist A ein K-Vektorraum und ist $\bullet : A \times A \to A$, so heißt $A = (A, +, \cdot, \bullet)$ eine *K-Algebra*, falls gilt:

(A1) $(A, +, \bullet)$ ist ein Ring mit Einselement.

(A2) Für alle $\lambda \in K, x, y \in A$ ist

$$\lambda \cdot (x \bullet y) = (\lambda \cdot x) \bullet y = x \bullet (\lambda \cdot y).$$

Beispiel 2.12 Es sei K ein Körper. Wir setzen für $n \in \mathbb{N}$

$$K^{n\times n} := M_n(K) := \big\{(a_{jk})_{j,k=1,\dots,n} : a_{jk} \in K, j,k = 1,\dots,n\big\}.$$

Dann ist $(K^{n\times n}, +, \cdot, \bullet)$ mit der üblichen Matrizenaddition $+$, Skalarmultiplikation $\cdot$ und Matrizenmultiplikation $\bullet$ eine K-Algebra.
Ist $M \neq \emptyset$ eine Menge und $(K^M, +, \cdot)$ wie in B. 2.10, so ist $(K^M, +, \cdot, \bullet)$, wobei

$$(f \bullet g)(x) := f(x) \cdot g(x) \qquad (x \in M),$$

(also punktweise Multiplkation) eine K-Algebra.

Wir wollen nun weitere, für die Zahlentheorie wichtige Gruppen bzw. Ringe einführen.

Bemerkung und Definition 2.13 Es seien $a, a' \in \mathbb{Z}, m \in \mathbb{N}_0$. Dann heißt a *kongruent* a' *modulo* m, falls

$$m|(a - a')$$

d. h. falls $a' \in a + m\mathbb{Z}$. Wir schreiben dann

$$a \equiv a' \mod m.$$

Man sieht leicht, dass durch

$$a \sim a' :\Leftrightarrow a \equiv a' \mod m$$

eine Äquivalenzrelation auf $\mathbb{Z}$ gegeben ist. Die entsprechenden Äquivalenzklassen (also $a + m\mathbb{Z}$) werden *Restklassen* (modulo m) genannt. Wir schreiben für die Restklasse $a + m\mathbb{Z}$ mit Repräsentant $a \in \mathbb{Z}$ auch

$$[a] := [a]_m := a \mod m$$

und außerdem setzen wir

$$\mathbb{Z}_m := \{[a]_m : a \in \mathbb{Z}\}.$$

Es gilt dabei

$$\mathbb{Z}_m = \big\{[0]_m, [1]_m, \dots, [m-1]_m\big\} \qquad (m \neq 0)$$

und $\mathbb{Z}_0 = \mathbb{Z}$. Für $m = 4$ ist etwa

$$\mathbb{Z}_4 = \big\{[0]_4, [1]_4, [2]_4, [3]_4\big\}\ .$$

Bemerkung und Definition 2.14 In $\mathbb{Z}_m$ sind repräsentantenweise eine Addition und eine Multiplikation (wohl-)definiert: Man setzt für $a, b \in \mathbb{Z}$

$$[a]_m + [b]_m := [a+b]_m$$
$$[a]_m \cdot [b]_m := [ab]_m \ .$$

Wichtig: Die Definition ist unabhängig vom Repräsentanten!.
(Denn: Ist etwa $[a] = [a']$, $[b] = [b']$, so ist $m|(a-a')$ und $m|(b-b')$, also nach S. 1.2.3 auch

$$m|\big((a-a')b + a'(b-b') = ab - a'b'\big).$$

Damit ist $[ab] = [a'b']$. Die Behauptung für $+$ ergibt sich aus $m|(a-a'+b-b')$.)

Satz 2.15 *Für alle $m \in \mathbb{N}$ ist $(\mathbb{Z}_m, +, \cdot)$ ein kommutativer Ring mit Einselement $[1]$ (und Nullelement $[0]$).*

Beweis. Ergibt sich unmittelbar aus der repräsentantenweisen Definition und den entsprechenden Eigenschaften in $(\mathbb{Z}, +, \cdot)$. □

Beispiel 2.16 Für $m = 4$ gilt etwa

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

oder anders ausgedrückt

$$(2 \mod 4) + (3 \mod 4) = 5 \mod 4 = 1 \mod 4.$$

Entsprechend ist

$$[2]_4[2]_4 = [4]_4 = [0]_4 \quad \text{bzw.} \quad (2 \mod 4) \cdot (2 \mod 4) = 4 \mod 4 = 0 \mod 4.$$

Dieses Beispiel zeigt insbesondere, dass $(\mathbb{Z}_4, +, \cdot)$ nicht nullteilerfrei, also kein Integritätsring ist (und damit auch kein Körper). Man sieht sofort, dass $[2]_4$ kein inverses Element (Bzgl. $[1]$) besitzt (d.h. die Gleichung $[2]_4 \cdot [x]_4 = [1]_4$, m.a.W. die Gleichung $2x \equiv 1 \mod 4$, hat keine Lösung).

Die Existenz inverser Elemente klärt

Satz 2.17 *Es sei $m \in \mathbb{N}$. Dann gilt: Zu $a \in \mathbb{Z}$ existiert genau dann ein $x \in \mathbb{Z}$ mit $ax \equiv 1 \mod m$ (d. h. $[a]_m \cdot [x]_m = [1]_m$), wenn $ggT(a, m) = 1$ ist.*

Beweis. $ax \equiv 1 \mod m$ für ein $x \in \mathbb{Z}$ gilt genau dann, wenn $1 \in ax + m\mathbb{Z}$ für ein $x \in \mathbb{Z}$. Nach S. 1.5 gilt dies genau dann, wenn $\mathrm{ggT}(a, m) = 1$ ist. □

Eine nette Anwendung von Kongruenzen sind bekannte Teilbarkeitskriterien.

Satz 2.18 *Es sei $n \in \mathbb{N}$ mit Dezimaldarstellung*

$$n = (a_r a_{r-1} \dots a_0)_{10}.$$

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. Es gilt für $m \in \mathbb{N}$

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

Für $m \in \{3, 9\}$ ist $[10]_m = [1]_m$, also

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

Aus $[10]_{11} = [-1]_{11}$ ergibt sich 3. in analoger Weise. □

Zurück zur allgemeinen Theorie: Wir haben in B. 2.16 gesehen, dass $(\mathbb{Z}_m \setminus \{0\}, \cdot)$ im Allgemeinen keine Gruppe ist. Betrachtet man geeignete Teilmengen von $\mathbb{Z}_m \setminus \{0\}$, so sieht die Sache besser aus:

Bemerkung und Definition 2.19 Sind $a, a' \in \mathbb{Z}$ und ist $m \in \mathbb{N}$, so folgt aus

$$a \equiv a' \mod m$$

und $\mathrm{ggT}(a, m) = 1$ auch $\mathrm{ggT}(a', m) = 1$.
(Denn: Nach S. 1.5 existieren $x, y \in \mathbb{Z}$ mit $1 = ax+my$. Ist weiter k so, dass $a = a'+km$, so gilt damit

$$1 = a'x + m(y + kx),$$

d. h. $1 \in a'\mathbb{Z} + m\mathbb{Z}$ und damit wieder nach S. 1.5 $\mathrm{ggT}(a', m) = 1$.)
Im Falle $\mathrm{ggT}(a, m) = 1$ heißt die Restklasse $[a]_m$ *prime Restklasse (modulo m)* (man beachte wieder: die Definition ist repräsenantenunabhängig). Weiter setzen wir

$$\mathbb{Z}_m^* := \{[a]_m : [a]_m \text{ prime Restklasse}\}.$$

Ist etwa $m = 4$, so ist $\mathbb{Z}_4^* = \{[1]_4, [3]_4\}$.

Es gilt damit

Satz 2.20 *Für alle $m \in \mathbb{N}$ ist $(\mathbb{Z}_m^*, \cdot)$ eine (abelsche) Gruppe.*

Beweis. Zunächst gilt für $[a]_m, [b]_m \in \mathbb{Z}_m^*$ auch $[a]_m[b]_m = [ab]_m \in \mathbb{Z}_m^*$, denn nach S. 1.6.3 ist $\mathrm{ggT}(ab, m) = 1$. Damit ist $\cdot : \mathbb{Z}_m^* \times \mathbb{Z}_m^* \to \mathbb{Z}_m^*$.
(G.1), (G.3) sind erfüllt, da $(\mathbb{Z}_m, +, \cdot)$ ein kommutativer Ring ist. Außerdem ist $[1]_m \in \mathbb{Z}_m^*$ und als Einselement in $(\mathbb{Z}_m, +, \cdot)$ auch neutrales Element in $(\mathbb{Z}_m^*, \cdot)$. Ist schließlich $[a]_m \in \mathbb{Z}_m^*$, so hat die Gleichung $[a]_m[x]_m = [1]_m$ nach S. 2.17 eine Lösung $[x]_m \in \mathbb{Z}_m$. Wieder nach S. 2.17 ist $[x]_m$ eine prime Restklasse, d. h. $[x]_m \in \mathbb{Z}_m^*$. Also ist $[x]_m$ (rechts-)invers zu $[a]_m$. Damit ist auch (G.2) erfüllt. □

Beispiele 2.21 1. $(\mathbb{Z}_4^*, \cdot) = (\{[1]_4, [3]_4\}, \cdot)$ ist eine (abelsche) Gruppe.
2. Es sei $p \in \mathbb{P}$. Dann ist $\mathrm{ggT}(a, p) = 1$ für alle $a \in \{1, \ldots, p-1\}$. Also ist

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

und damit $(\mathbb{Z}_p \setminus \{[0]\}, \cdot)$ nach S. 2.20 eine (abelsche) Gruppe. Folglich ist in diesem Fall nach S. 2.15 und D. 2.6

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

(mit p Elementen).

3 Die Sätze von Lagrange, Euler und Fermat (klein)

Definition 3.1 Es sei $(G, *)$ eine Gruppe. Ist $\emptyset \neq U \subset G$, so heißt U bzw. $(U, *)$ *Untergruppe* von G, falls $(U, *_{|U\times U})$ eine Gruppe ist.

Bemerkung 3.2 Es sei $(G, *)$ eine Gruppe.
1. Ist U eine Untergruppe, so ist $e \in U$ (denn mit $a \in U$ ist auch $e = a * a^{-1} \in U$).
2. Für $\emptyset \neq U \subset G$ sind äquivalent:

a) U ist eine Untergruppe

b) $e \in U$ und mit $a, b \in U$ sind auch $a * b$ und $a^{-1} \in U$.

c) Mit $a, b \in U$ ist auch $a * b^{-1} \in U$.

(Denn: $a) \Leftrightarrow b)$ und $a) \Rightarrow c)$ sind klar nach Definition.
$c) \Rightarrow b)$: Ist $a \in U$, so ist $e = a * a^{-1} \in U$. Also ist auch $a^{-1} = e * a^{-1} \in U$. Sind $a, b \in U$, so gilt damit auch $a * b = a * (b^{-1})^{-1} \in U$.)

Ist U **endlich**, so ist U schon dann Untergruppe, wenn mit $a, b \in U$ auch $a * b \in U$ gilt.
(Denn: Zunächst gilt: Ist $b \in U$ fest und ist $f_b : U \to U * b := \{x * b : x \in U\}$ definiert durch $f_b(x) := x * b$ $(x \in U)$, so ist f_b injektiv (man beachte: aus $x * b = y * b$ folgt $x = x * b * b^{-1} = y * b * b^{-1} = y$). Nach Definition ist f_b auch surjektiv und damit ist $|U| = |U * b|$.
Ist nun $b \in U$, so ist nach Voraussetzung $U * b \subset U$. Da U endlich ist, ist $U * b = U$. Also existiert für alle $a \in U$ ein $x \in U$ mit $x * b = a$, d. h. $a * b^{-1} = x \in U$.)

Beispiele 3.3 1. Ist $(G, *)$ eine beliebige Gruppe, so sind $U = G$ und $U = \{e\}$ stets Untergruppen (sogenannte triviale Untergruppen).
2. Ist $(G, *) = (\mathbb{C}, +)$, so haben wir folgende Kette ineinandergeschachtelter Untergruppen $(m \in \mathbb{N})$:

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

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

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

Bemerkung und Definition 3.4 Ist $(G,*)$ eine Gruppe und ist $(U_\alpha)_{\alpha\in I}$ eine Familie von Untergruppen, so ist auch $\bigcap\limits_{\alpha\in I} U_\alpha$ eine Untergruppe.
(Denn mit $a,b\in\bigcap\limits_{\alpha\in I} U_\alpha$ ist auch $a*b^{-1}\in\bigcap\limits_{\alpha\in I} U_\alpha$.)
Ist $M\subset G$ beliebig, so heißt

$$<M>:=\bigcap_{U\supset M \text{ Untergruppe}} U$$

die *von M erzeugte Untergruppe*. M heißt dann auch ein *Erzeugendensystem* von $<M>$. Ist speziell $M=\{a\}$, so schreiben wir kurz $<a>$ statt $<\{a\}>$.

Wir definieren $a^k\in G$ für $a\in G$ und $k\in\mathbb{Z}$ wie üblich durch $a^0:=e$,

$$a^k:=a*a^{k-1},\quad a^{-k}:=(a^{-1})^k(=(a^k)^{-1})\qquad(k\in\mathbb{N})\ .$$

(Im Falle einer additiven Gruppe $(G,+)$ schreiben wir meist kx statt x^k.)

Satz 3.5 *Es seien $(G,*)$ eine Gruppe und $M\subset G$. Dann gilt*

1. $<M>=\left\{a_1^{\varepsilon_1}*\cdots*a_n^{\varepsilon_n}:n\in\mathbb{N},a_j\in M,\varepsilon_j=\pm1,j=1,\dots,n\right\}$.
2. *Ist G abelsch, so ist auch*

$$<M>=\left\{\prod_{a\in F}a^{k_a}:F\subset M\ \textit{endlich},k_a\in\mathbb{Z}\right\}\ .$$

Beweis. E seien U_1 bzw. U_2 die rechte Seite in 1. bzw. 2.
$\supset$ in 1. und 2.: Ist U eine Untergruppe mit $U\supset M$, so ist auch $U\supset U_j$ für $j=1,2$ nach B. 3.2.2.
$\subset$ in 1.: Sind $a=a_1^{\varepsilon_1}*\cdots*a_n^{\varepsilon_n}$ und $b=b_1^{\delta_1}*\cdots*b_m^{\delta_m}$ aus U_1, so ist auch

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

Nach B. 3.2.2 ist U_1 eine Untergruppe. Aus $M\subset U_1$ folgt $<M>\subset U_1$ nach Definition von $<M>$.
$\subset$ in 2.: Sind $a_1,\dots,a_n\in M$ und $\varepsilon_1,\dots,\varepsilon_n\in\{\pm1\}$, so gilt

$$a_1^{\varepsilon_1}*\cdots*a_n^{\varepsilon_n}=\prod_{a\in\{a_1,\dots,a_n\}}a^{k_a}$$

mit $k_a:=\sum\limits_{j:a_j=a}\varepsilon_j$. Also ist $U_1\subset U_2$ und folglich auch $<M>=U_1\subset U_2$. □

Bemerkung und Definition 3.6 1. Es sei $(G, *)$ eine Gruppe. Dann ist für $a \in G$ nach S. 3.5

$$<a> = \{a^k : k \in \mathbb{Z}\}$$

die von a erzeugte Untergruppe.
$(G, *)$ heißt *zyklisch*, falls $G = <a>$ für ein $a \in G$ gilt. In diesem Fall nennt man a ein *erzeugendes Element* von G.
2. Für eine Untergruppe U von G heißt

$$\text{ord } (U) := |U| \ \big(\in \mathbb{N} \cup \{\infty\}\big)$$

die *Ordnung* von U und

$$\text{ord } a := \text{ord } <a>$$

die *Ordnung* von a.

Beispiele 3.7 1. Es sei $(G, *) = (\mathbb{Z}, +)$. Dann gilt $<a> = a\mathbb{Z}$ und insbesondere

$$\mathbb{Z} = <1> = <-1> \ .$$

Also ist $\mathbb{Z}$ zyklisch und ± 1 sind erzeugende Elemente (und zwar die einzigen).
2. Ist $(G, *) = (\mathbb{Z}_m, +)$, so gilt $<[a]> = \{[ka] : k \in \mathbb{Z}\}$ und insbesondere

$$\mathbb{Z}_m = <[1]> \ .$$

Also ist auch $\mathbb{Z}_m$ zyklisch. Allgemeiner ist hier auch $\mathbb{Z}_m = <[a]>$ für jede prime Restklasse $[a]$ nach S. 2.17.

Bemerkung und Definition 3.8 Es sei $(G, *)$ eine Gruppe. Ist $H \subset G$ eine Untergruppe, so definieren wir für $a, a' \in G$

$$a \sim a' :\Leftrightarrow a' * a^{-1} \in H \quad (\Leftrightarrow a' \in H * a := \{x * a : x \in H\}).$$

Man sieht leicht, dass $\sim$ eine Äquivalenzrelation auf G ist. Die Äquivalenzklassen sind die Teilmengen $H * a$ $(a \in G)$, die hier *Rechtsrestklassen* genannt werden.
Durch Betrachtung von $a^{-1} * a'$ anstelle von $a' * a^{-1}$ erhält man entsprechend die *Linksrestklassen* $a * H$; für abelsche Gruppen gilt natürlich $a * H = H * a$. Stets (also auch im nichtabelschen Fall) ist für alle $a \in G$

$$|H * a| = |H| = |a * H|$$

(vgl. B. 3.2.2).
Weiter setzen wir

$$ {}_H\backslash G := \{H * a : a \in G\}, \qquad G/_H := \{a * H : a \in G\} . $$

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

$$ G : H := \left|G/_H\right| \left(\in \mathbb{N} \cup \{\infty\}\right) $$

heißt *Index* von H (in G).

Beispiel 3.9 Es seien $(G, *) = (\mathbb{Z}, +)$ und $H = m\mathbb{Z}$ für $m \in \mathbb{N}$. Dann gilt

$$ H * a = a * H = a + m\mathbb{Z} = [a]_m \qquad (a \in G). $$

Hier ist $G : H = \mathbb{Z} : m\mathbb{Z} = |\mathbb{Z}_m| = m$.

Satz 3.10 *(Lagrange)*
Ist $(G, *)$ eine endliche Gruppe und ist H eine Untergruppe, so ist

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

Beweis. Ergibt sich unmittelbar daraus, dass die Äquivalenzklassen $H * a$ eine Zerlegung von G in $G : H$ Teilmengen induzieren und dass $|H * a| = \operatorname{ord} H$ für alle $a \in G$ gilt. □

Als Anwendung ergibt sich

Satz 3.11 *Es sei $(G, *)$ eine Gruppe und es sei $x \in G$. Dann gilt*

1. *Es ist $\operatorname{ord} x < \infty$ genau dann, wenn ein $n \in \mathbb{N}$ existiert mit $x^n = e$. In diesem Fall ist*

   $$ x^{k\operatorname{ord}(x)+j} = x^j $$

   für $k \in \mathbb{Z}$ und $j = 0, \ldots, \operatorname{ord}(x) - 1$. Insbesondere ist $x^{\operatorname{ord}(x)} = e$.

2. *Ist $\operatorname{ord}(G) < \infty$, so ist $x^{\operatorname{ord} G} = e$.*

Beweis. 1. Wir zeigen $\Leftarrow$ und die Zusatzbehauptung: Es existiere also ein $n \in \mathbb{N}$ mit

$$x^n = e.$$

Ist

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

so folgt aus $x^m = e$ auch

$$x^{km+j} = (x^m)^k * x^j = x^j$$

für alle $k \in \mathbb{Z}, j = 0, \ldots, m-1$. Folglich ist $<x> = \{x^0, x^1, \ldots, x^{m-1}\}$ und damit ord $x \leq m$ (und insbesondere ord $x < \infty$).
Weiter sind $e = x^0, x, \ldots, x^{m-1}$ paarweise verschieden, da ansonsten $0 \leq j < k \leq m-1$ existieren würden mit $x^j = x^k$ und damit $x^{k-j} = e$, im Widerspruch zur Minimalität von m. Also ist auch $m \leq$ ord x.
Wir zeigen $\Rightarrow$: Angenommen, es existiert kein $n \in \mathbb{N}$ mit $x^n = e$. Dann ist $x^{k-j} \neq e$ für alle $j < k$ und damit $x^j \neq x^k$ für alle $j < k$. Also sind alle x^k paarweise verschieden. damit ist aber ord $x = \infty$.
2. Nach S. 3.10 gilt mit $H = <x>$

$$\text{ord } G = \big(G : <x>\big) \text{ ord } x,$$

also ord $x \,|\, $ ord G. Mit 1. folgt $x^{\text{ord }(G)} = (x^{\text{ord } x})^{G:<x>} = e$. □

Durch Anwendung auf die primen Restklassengruppen $\mathbb{Z}_m^*$ ergeben sich wichtige zahlentheoretische Konsequenzen.

Definition 3.12 Für $m \in \mathbb{N}$ sei

$$\varphi(m) := |\mathbb{Z}_m^*|,$$

also $\varphi(m)$ die Anzahl der $a \in \mathbb{N}$ mit $a \leq m$ und ggT$(a, m) = 1$. Die Funktion $\varphi : \mathbb{N} \to \mathbb{N}$ heißt *Eulersche Phi-Funktion*. Dabei gilt $\varphi(1) = 1$ und $\varphi(p) = p - 1$ für $p \in \mathbb{P}$ nach B. 2.21.

Satz 3.13
1. (Euler) Ist $m \in \mathbb{N}$, so gilt für alle $a \in \mathbb{Z}$ mit ggT$(a, m) = 1$

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

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

(i) Ist p kein Teiler von a, so ist $a^{p-1} \equiv 1 \mod p$.

(ii) $a^p \equiv a \mod p$.

Beweis. 1. Ergibt sich aus S. 3.11.2 angewandt auf $(G, *) = (\mathbb{Z}_m^*, \cdot)$ und der Definition von φ.
2. Ist p kein Teiler von a, so ist $\mathrm{ggT}(a, p) = 1$, da $p \in \mathbb{P}$. Nach 1. ist

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

Dann gilt auch

$$[a^p]_p = [a^{p-1}]_p [a]_p = [a]_p.$$

Ist $p|a$, so gilt auch $p|a^p$, also $a^p \equiv 0 \equiv a \mod p$. □

Bemerkung und Definition 3.14 Der erste Teil des Fermatschen Satzes liefert eine notwendige Bedingung dafür, dass $n \in \mathbb{N}$ eine Primzahl ist. Ist nämlich $n \in \mathbb{N}$ beliebig und so, dass

$$a^{n-1} \not\equiv 1 \mod n$$

für ein a mit $n \nmid a$ (also etwa für ein $a \in \{1, \ldots, n-1\}$), so ist n keine Primzahl.
Man könnte auf den Gedanken kommen, dass umgekehrt aus

$$a^{n-1} \equiv 1 \mod n \tag{3.1}$$

für alle a mit $\mathrm{ggT}(a, n) = 1$ schon folgt, dass $n \in \mathbb{P}$ ist. Dies ist jedoch i.A. falsch!
Man nennt eine Zahl $n \in \mathbb{N} \setminus \mathbb{P}$ *pseudoprim* zur Basis a, falls (3.1) gilt. Ist n pseudoprim zur Basis a für alle a mit $\mathrm{ggT}(a, n) = 1$, so heißt n *Carmichaelzahl*. Man kann zeigen, dass unendlich viele Carmichaelzahlen existieren. Wir werden später nachrechnen, dass

$$n = 561 = 3 \cdot 11 \cdot 17$$

eine solche ist (genauer: die kleinste). Dies wurde 1912 von Carmichael erkannt.

4 Lineare Kongruenzen und Anwendungen

Wir betrachten lineare Gleichungen oder Gleichungssysteme in $\mathbb{Z}_m$, also sogenannte lineare Kongruenzen. Zunächst befassen wir uns mit einer Gleichung. Es seien $a, b \in \mathbb{Z}, m \in \mathbb{N}$. Wir suchen Lösungen $x \in \mathbb{Z}$ von

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

also der Gleichung

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

in $\mathbb{Z}_m$.
Es gilt (wobei zu beachten ist, dass $d|c$ für $c, d \in \mathbb{Z}$ mit $d \neq 0$ genau dann gilt, wenn die (scheinbar) rationale Zahl c/d ganz ist)

Satz 4.1 *Die Gleichung (4.1) ist genau dann lösbar, wenn $d := ggT(a, m)|b$. In diesem Fall gilt: x löst (4.1) genau dann, wenn x die Gleichung*

$$\frac{a}{d}x \equiv \frac{b}{d} \mod \frac{m}{d}$$

löst, und dann sind die mod m *unterschiedlichen Lösungen von (4.1) gegeben durch $x_k = x + \frac{m}{d}k\,(k = 0, \ldots, d-1)$.*

Beweis. 1. (4.1) ist genau dann lösbar, wenn $x, y \in \mathbb{Z}$ existieren mit

$$ax + my = b,$$

d. h. $b \in a\mathbb{Z} + m\mathbb{Z}$. Nach S. 1.5 ist dies genau dann der Fall, wenn $d|b$.
2. Da d Teiler von a, b, m ist, gilt

$$ax \equiv b \mod m, \text{ d. h. } m|(ax - b)$$

genau dann, wenn

$$\frac{m}{d}\Big|\Big(\frac{a}{d}x - \frac{b}{d}\Big), \text{ d. h. } \Big[\frac{a}{d}x\Big]_{\frac{m}{d}} = \Big[\frac{b}{d}\Big]_{\frac{m}{d}}.$$

Da $\mathrm{ggT}\big(\frac{a}{d}, \frac{m}{d}\big) = 1$ gilt, existiert nach S. 2.20 das Inverse $[c]_{m/d}$ von $[a/d]_{m/d}$ in $\mathbb{Z}^*_{m/d}$. Damit löst $[c]_{m/d}[b/d]_{m/d}$ die letzte Gleichung und dies ist auch die einzige Lösung in $\mathbb{Z}_{m/d}$. Ist $x \in [c]_{m/d}$ so hat man also genau die Lösungen $x_k = x + k \cdot \frac{m}{d}$ $(k \in \mathbb{Z})$ von (4.1), wobei $x = x_0, \ldots, x_{d-1}$ mod m paarweise verschieden sind. □

Beispiele 4.2 1. Wir betrachten die Gleichung

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

Es gilt $\mathrm{ggT}(6, 27) = 3$ und $3|b = 3$. Also ist die Gleichung lösbar. Um die Gleichung zu lösen, betrachtet man

$$2x = \frac{6}{3}\, x \equiv \frac{3}{3} = 1 \mod \frac{27}{3} = 9.$$

Die (mod 9 eindeutige) Lösung ist gegeben durch $x = 5$. Damit sind die Lösungen der Ausgangsgleichung gegeben durch $5, 14, 23 \mod 27$.
2. Die Gleichung

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

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

Von grundlegender Bedeutung ist das folgende Ergebnis über simultane Kongruenzen.

Satz 4.3 *Es seien $m_1, \ldots, m_n \in \mathbb{N}$ paarweise teilerfremd, d. h. $ggT(m_j, m_k) = 1$ für $j \neq k$. Dann gilt mit $m := \prod_{j=1}^{n} m_j$*

1. *Für $x, \tilde{x} \in \mathbb{Z}$ ist*

$$x \equiv \tilde{x} \mod m \text{ genau dann, wenn } x \equiv \tilde{x} \mod m_j \ (j = 1, \ldots, n) .$$

2. *Die Abbildung $f : \mathbb{Z}_m \to \prod_{j=1}^{n} \mathbb{Z}_{m_j}$, definiert durch*

$$f\big([x]_m\big) = \big([x]_{m_1}, \ldots, [x]_{m_n}\big) \qquad \big([x]_m \in \mathbb{Z}_m\big),$$

ist (wohldefiniert und) bijektiv.

3. *(Chinesischer Restsatz) Sind $b_1, \ldots, b_n \in \mathbb{Z}$, so existiert ein $x \in \mathbb{Z}$ so, dass*

$$x \equiv b_j \mod m_j \qquad (j = 1, \ldots, n) \tag{4.2}$$

und die Lösungsmenge von (4.2) ist dann $[x]_m = x + m\mathbb{Z}$.

Beweis. 1. Sind $x, \tilde{x} \in \mathbb{Z}$, so gilt, da die m_j paarweise teilerfremd sind,

$$m_j|(x - \tilde{x}) \qquad (j = 1, \ldots, n)$$

genau dann, wenn

$$m|(x - \tilde{x})$$

($\Rightarrow$ ergibt sich induktiv mit S. 1.6.2 und S. 1.6.3; $\Leftarrow$ ist klar).
2. Nach 1. ist f wohldefiniert und injektiv. Da

$$|\mathbb{Z}_m| = \prod_{j=1}^{n} m_j = \prod_{j=1}^{n} |\mathbb{Z}_{m_j}|$$

gilt, ist f dann schon bijektiv.
3. Nach 2. existiert zu jedem Tupel $(b_1, \ldots, b_n) \in \mathbb{Z}^n$ genau ein $[x]_m \in \mathbb{Z}_m$ mit

$$([x]_{m_1}, \ldots, [x]_{m_n}) = f([x]_m) = ([b_1]_{m_1}, \ldots, [b_n]_{m_n}) \qquad (j = 1, \ldots, n)\ .$$

Damit ist $x \equiv b_j \mod m_j$ für $j = 1, \ldots, n$ (also x Lösung von (4.2)) und $y \in \mathbb{Z}$ ist genau dann Lösung von (4.2), wenn $y \in [x]_m$ gilt. □

Bemerkung 4.4 Ein Ansatz zur Berechnung einer Lösung von (4.2) ist der folgende: Man setzt

$$a_j := m/m_j \qquad (j = 1, \ldots, n).$$

Dann gilt $\mathrm{ggT}(a_j, m_j) = 1$ nach Satz 1.6.3 (induktiv angewandt). Also existiert nach Satz 4.1 ein $x_j \in \mathbb{Z}$ mit

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

Da $m_j|a_k$ für $k \neq j$ gilt, folgt

$$x := \sum_{k=1}^{n} a_k x_k \equiv a_j x_j \equiv b_j \mod m_j$$

für $j = 1, \ldots, n$, d.h. x ist eine Lösung von (4.2).

Wir betrachten das System

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

Nach obiger Überlegung kann man eine Lösung

$$x = a_1x_1 + a_2x_2 + a_3x_3$$

berechnen aus

$$\begin{aligned} a_1x_1 &= 35x_1 \equiv 2 \mod 3 \\ a_2x_2 &= 21x_2 \equiv 3 \mod 5 \\ a_3x_3 &= 15x_3 \equiv 2 \mod 7. \end{aligned}$$

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

$$x = 35 + 3 \cdot 21 + 2 \cdot 15 = 128\ .$$

Die Lösungsmenge ist gegeben durch

$$x \equiv 128 \equiv 23 \mod 105 = 3 \cdot 5 \cdot 7.$$

Bemerkung 4.5 In B./D. 3.14 hatten wir behauptet, dass etwa

$$n = 561 = 3 \cdot 11 \cdot 17$$

eine Carmichael-Zahl ist. Der Beweis wird jetzt nachgeliefert.
Wir zeigen allgemein: Ist $n \in \mathbb{N} \setminus \mathbb{P}$ quadratfrei, d.h. $n = \prod\limits_{p \in E(n)} p$, so ist n Carmichael-Zahl, wenn

$$(p-1)|(n-1) \qquad \big(p \in E(n)\big)$$

gilt.
(Denn: Aus dem kleinen Satz von Fermat erhält man für alle a mit $\mathrm{ggT}(a,n) = 1$ und alle $k \in \mathbb{N}$ sowie $p \in E(n)$

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

(man beachte $\mathrm{ggT}(a,p) = 1$ $(p \in E(n))$). Da $(p-1)|(n-1)$, folgt

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

für alle $p \in E(n)$. Nach S. 4.3.1 ist dann auch $a^{n-1} \equiv 1 \mod n$.)

Da für $n = 3 \cdot 11 \cdot 17 = 561$ offensichtlich $2|560, 10|560$ und $16|560$ gilt, ist 561 Carmichael-Zahl.

Bemerkung 4.6 Sind $m_1, \ldots, m_n$ paarweise teilerfremd, so gilt für die Abbildung $f : \mathbb{Z}_m \to \prod_{j=1}^{n} \mathbb{Z}_{m_j}$ aus S. 4.3.2:

$$f_{|\mathbb{Z}_m^*} : \mathbb{Z}_m^* \to \prod_{j=1}^{n} \mathbb{Z}_{m_j}^*$$

ist bijektiv.
(Denn: Dies ergibt sich aus der Bijektivität von f und daraus, dass nach S. 1.6.3 für $x \in \mathbb{Z}$

$$\mathrm{ggT}(m_j, x) = 1 \quad (j = 1, \ldots, n)$$

genau dann gilt, wenn

$$\mathrm{ggT}(m, x) = 1$$

ist.)
Für die Eulersche Phi-Funktion φ bedeutet dies

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

(denn $|\mathbb{Z}_m^*| = |\prod_{j=1}^{n} \mathbb{Z}_{m_j}^*| = \prod_{j=1}^{n} |\mathbb{Z}_{m_j}^*|$, da $f_{|\mathbb{Z}_m^*}$ bijektiv).

Hieraus folgt

Satz 4.7 *Für $n \in \mathbb{N}$ ist*

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

und insbesondere

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

Beweis. 1. Es sei zunächst $p \in \mathbb{P}, k \in \mathbb{N}$. Dann sind die $a \in \{1, \ldots, p^k\}$, die nicht teilerfremd zu p^k sind, genau die p^{k-1} Zahlen $p, 2p, 3p, \ldots, p^{k-1}p$. Also ist

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

2. Ist $n \in \mathbb{N}$, so gilt nach dem Fundamentalsatz der Arithmetik

$$n = \prod_{p \in E(n)} p^{\alpha_p(n)}.$$

Da die $p^{\alpha_p(n)}$ paarweise teilerfremd sind, gilt nach 1. und B. 4.6

$$\begin{aligned} \varphi(n) &= \prod_{p \in E(n)} \varphi(p^{\alpha_p(n)}) = \prod_{p \in E(n)} (p^{\alpha_p(n)} - p^{\alpha_p(n)-1}) \\ &= \Big(\prod_{p \in E(n)} p^{\alpha_p(n)} \Big) \prod_{p \in E(n)} \Big(1 - \frac{1}{p}\Big) = n \prod_{\substack{p \in \mathbb{P} \\ p \mid n}} \Big(1 - \frac{1}{p}\Big). \end{aligned}$$

□

Was kann man mit derartigen Dingen anfangen? Es ist höchst bemerkenswert, dass die heute üblichen Verschlüsselungsverfahren, wie sie etwa im Zahlungsverkehr via Internet genutzt werden, auf zahlentheoretischen Überlegungen beruhen. Wir wollen kurz hierauf eingehen:

Bemerkung 4.8 (RSA-Verfahren, 1977)
Das RSA-Kryptographie-Verfahren ist benannt nach den ,,Erfindern" Rivest, Shamir und Adleman. Es beruht auf folgender Beobachtung:
Sind $p, q \in \mathbb{P}$ (möglichst groß; heute > 200 Stellen), $p \neq q$, und ist $n = p \cdot q$, so gilt nach B. 4.6

$$\varphi(n) = (p-1)(q-1).$$

Weiter sei $a \in \mathbb{N}$ teilerfremd zu $\varphi(n)$. Nach S. 2.17 existiert ein $b \in \mathbb{Z}$ (ohne Einschränkung $b \in \mathbb{N}$) mit

$$ab \equiv 1 \mod \varphi(n).$$

Wir zeigen: *Für alle* $x \in \mathbb{N}$ *gilt*

$$(x^a)^b = x^{ab} \equiv x \mod n. \tag{4.3}$$

Denn:
Da $\varphi(n) = (p-1)(q-1)$ gilt, folgt aus $ab \equiv 1 \mod \varphi(n)$ auch $ab \equiv 1 \mod (p-1)$ und $ab \equiv 1 \mod (q-1)$. Also existieren $k, \ell \in \mathbb{N}$ mit

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

Damit erhält man aus dem kleinen Satz von Fermat (S. 3.13) im Falle, dass p kein Teiler von x ist,

$$[x^{ab}]_p = [x^{k(p-1)}x]_p = [x^{p-1}]_p^k[x]_p = [x]_p \ ,$$

d. h. $x^{ab} \equiv x \mod p$. Im Falle $p|x$ gilt natürlich auch

$$x^{ab} \equiv 0 \equiv x \mod p.$$

Entsprechend ergibt sich

$$x^{ab} \equiv x \mod q$$

und damit mit S. 4.3.1 auch

$$x^{ab} \equiv a \mod n = pq,$$

da p, q teilerfremd. •

Will man eine Nachricht, die ohne Einschränkung ein Vektor $(x_1, \ldots, x_N)$ natürlicher Zahlen $< n$ sein soll, von einem Sender B zu einem Empfänger A übermitteln, ohne dass Unbefugte die Nachricht verstehen können, so kann man, nachdem p, q, a, b wie oben durch A festgelegt wurden, die öffentlichen Schlüssel a und auch n an B übermitteln. B kann dann die verschlüsselte Nachricht $(x_1^a, \ldots, x_N^a)$ (modulo n) öffentlich übertragen. Die Originalnachricht $(x_1, \ldots, x_N)$ ist mit der Gleichung (4.3) für A leicht rekonstruierbar, da A zusätzlich b kennt.
Die Primfaktorzerlegung $n = pq$ ist eine sehr schwieriges Problem, das für genügend große p, q (mit den derzeit bekannten Methoden) praktisch unmöglich ist. Damit ist die Nachricht sicher verschlüsselt solange p und q (und damit $\varphi(n)$ sowie b) nur dem Empfänger bekannt sind.

5 Homomorphismen, Normalteiler, Faktorgruppen

Definition 5.1 Es seien $(G,*) = (G,*_G)$ und $(H,*) = (H,*_H)$ Gruppen (mit neutralen Elementen e_G bzw. e_H). Eine Abbildung $h : G \to H$ heißt *(Gruppen-) Homomorphismus*, falls

$$h(a * b) = h(a) * h(b) \qquad (a, b \in G).$$

Ein Homomorphismus heißt *(Gruppen-) Monomorphismus* (oder *Einbettung*), falls h injektiv ist. Ein bijektiver Homomorphismus heißt *(Gruppen-) Isomorphismus*. Existiert ein Isomorphismus $h : G \to H$, so nennt man G und H *isomorph* (Schreibweise: $G \simeq H$).
Schließlich heißt $\mathrm{Kern}(h) := h^{-1}\big(\{e_H\}\big)$ *Kern* von h.

Beispiele 5.2 1. Es sei $h : (\mathbb{Z},+) \to (\mathbb{Z}_m+)$ definiert durch

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

Dann ist h ein (surjektiver) Homomorphismus (denn

$$h(a+b) = [a+b] = [a] + [b] = h(a) + h(b)$$

für alle $a, b \in \mathbb{Z}$) jedoch kein Monomorphimus (etwa $h(0) = [0]_m = [m]_m = h(m)$). Hier gilt $\mathrm{Kern}(h) = m\mathbb{Z}$.
2. Die Abbiildung $h : (\mathbb{R},+) \to (\mathbb{C},+)$, definiert durch

$$h(a) := (a,0) = a + i0 \qquad (a \in \mathbb{R}),$$

ist eine Einbettung.
3. Genauso ist $h : (\mathbb{Z},+) \to (\mathbb{Q},+)$, definiert durch

$$h(a) := (a,1) = a/1 \qquad (a \in \mathbb{Z}),$$

eine Einbettung.
4. Es seien K ein Körper und

$$GL_n(K) := \{A \in M_n(K) : A \text{ invertierbar}\}.$$

Dann ist $GL_n(K)$ mit der Matrixmultiplikation eine Gruppe. Die Abbildung $h : GL_n(K) \to (K \setminus \{0\}, \cdot)$, definiert durch $h(A) := \det A$ für $A \in GL_n(K)$, ist ein Homomorphismus (da $\det(AB) = \det(A)\det(B)$).

Wir stellen einige elementare Eigenschaften von Homomorphismen zusammen (und schreiben im Weiteren meist kurz ab statt $a * b$).

Satz 5.3 *Es seien G und H Gruppen sowie $h : G \to H$ ein Homomorphismus. Dann gilt*

1. $h(e_G) = e_H$,
2. $h(a^{-1}) = \big(h(a)\big)^{-1}$ *für alle* $a \in G$.
3. *Ist $U \subset G$ eine Untergruppe, so ist $h(U) \subset H$ eine Untergruppe.*
4. *Ist $V \subset H$ eine Untergruppe, so ist $h^{-1}(V) \subset G$ eine Untergruppe. Insbesondere ist also* $\mathrm{Kern}(h) \subset G$ *eine Untergruppe.*
5. *h ist genau dann ein Monomorphismus, wenn* $\mathrm{Kern}(h) = \{e_G\}$ *gilt.*
6. *Ist h ein Isomorphismus, so ist auch $h^{-1} : H \to G$ ein Homomorphismus (und damit ein Isomorphismus). Sind F eine weitere Gruppe und $k : F \to G$ ein Isomorphismus, so ist auch $h \circ k$ ein Isomorphismus.*

Beweis. 1. Es gilt

$$h(e_G) = h(e_G e_G) = h(e_G)h(e_G),$$

also ist $e_H = h(e_G)\big(h(e_G)\big)^{-1} = h(e_G)h(e_G)\big(h(e_G)\big)^{-1} = h(e_G)$.
2. Nach 1. gilt für $a \in G$

$$h(a)h(a^{-1}) = h(aa^{-1}) = h(e_G) = e_H,$$

also $\big(h(a)\big)^{-1} = h(a^{-1})$.
3. und 4. (Ü)
5. $\Rightarrow$: Nach Voraussetzung ist $\mathrm{Kern}(h)$ höchstens einelementig. Da $\mathrm{Kern}(h)$ ein Unterraum von G ist, folgt $\mathrm{Kern}(h) = \{e_G\}$.
$\Leftarrow$: Aus $\mathrm{Kern}(h) = \{e_G\}$ folgt für alle $a, b \in G$ mit $h(a) = h(b)$ nach 2.

$$h(ab^{-1}) = h(a)\big(h(b)\big)^{-1} = h(a)\big(h(a)\big)^{-1} = e_H,$$

also $ab^{-1} = e_G$ und damit $a = ab^{-1}b = e_G b = b$.
6. Es seien $u, v \in H$. Dann existieren $a, b \in G$ mit $u = h(a), v = h(b)$. Also gilt

$$h^{-1}(uv) = h^{-1}\big(h(a)h(b)\big) = h^{-1}\big(h(ab)\big) = ab = h^{-1}(u)h^{-1}(v).$$

Schließlich gilt für $x, y \in F$

$$(h \circ k)(xy) = h(k(xy)) = h(k(x)k(y)) = h(k(x))h(k(y)) = (h \circ k)(x)(h \circ k)(y) \ .$$

□

Der folgende Satz zeigt, dass zyklische Gruppen im Wesentlichen von der Form $(\mathbb{Z}_m, +)$ sind.

Satz 5.4 *Es sei $(G, *)$ eine zyklische Gruppe. Dann gilt:*

1. *Ist $ord(G) = \infty$, so ist G isomorph zu $(\mathbb{Z}, +)$.*
2. *Ist $ord(G) := m < \infty$, so ist G isomorph zu $(\mathbb{Z}_m, +)$.*

Beweis. Es sei $G = <x>$, wobei $x \in G$. Wir definieren $h : \mathbb{Z} \to <x> = G$ durch

$$h(a) = x^a \qquad (a \in \mathbb{Z}).$$

Dann ist $h : \mathbb{Z} \to G$ ein surjektiver Homomorphismus.
(Denn: Für $a, b \in \mathbb{Z}$ gilt

$$h(a + b) = x^{a+b} = x^a * x^b = h(a) * h(b),$$

d. h. h ist ein Homomorphismus. Ist $y \in <x>$, so existiert ein $a \in \mathbb{Z}$ mit $y = x^a$, also $y = h(a)$.)
1. Fall: $|G| = \infty$. Dann ist $x^a \neq x^b$ für alle $a, b \in \mathbb{Z}, a \neq b$ (ansonsten wäre $x^{a-b} = e$ für gewisse $a, b \in \mathbb{Z}$ mit $a > b$ und damit G endlich nach S.3.11). Also gilt $h(a) \neq h(b)$ für alle $a, b \in \mathbb{Z}, a \neq b$, d. h. h ist injektiv und damit ein Isomorphismus.
2. Fall: $|G| = m$. Nach S. 3.11 ist $x^{a+mb} = x^a$ für alle $a, b \in \mathbb{Z}$. Also ist durch

$$k\big([a]_m\big) = h(a)(= x^a) \qquad \big([a]_m \in \mathbb{Z}_m\big)$$

eine Abbildung $k : (\mathbb{Z}_m, +) \to < x >= G$ wohldefiniert, die injektiv ist (beachte: $x^0, x^1, \ldots, x^{m-1}$ sind paarweise verschieden, da $\text{ord}(G) = m$). Da h ein surjektiver Homomorphismus ist, gilt dies auch für k. □

Bemerkung 5.5 1. Ist $p \in \mathbb{P}$, so ist jede Gruppe der Ordnung p isomorph zu $(\mathbb{Z}_p, +)$. (Denn: Es sei $x \in G \setminus \{e\}$. Nach S. 3.10 (Lagrange) ist $\operatorname{ord} x = p = \operatorname{ord}(G)$. Da $<x> \subset G$ ist, folgt $<x> = G$. Nach S. 5.4 ist G isomorph zu $(\mathbb{Z}_p, +)$.)
2. Für $m \in \mathbb{N}$ hat die (zyklische) Untergruppe $< e^{2\pi i/m} >$ von $(\mathbb{C} \setminus \{0\}, \cdot)$ die Ordnung m (denn $(e^{2\pi i/m})^m = e^{2\pi i} = 1$ und $e^{2\pi ij/m} \neq 1$ für $j = 1, \ldots, m-1$). Also ist $< e^{2\pi i/m} >$ isomorph zu $(\mathbb{Z}_m, +)$.

Allgemein kann man zeigen:

Satz 5.6 *Ist $n \in \mathbb{N}$, so ist jede Gruppe der Ordnung n isomorph zu einer Untergruppe der symmetrischen Gruppe S_n.*

Beweis. Es sei $G = \{x_1, \ldots, x_n\}$. Ist $a \in G$, so existiert zu jedem $j \in \{1, \ldots, n\}$ genau ein $\sigma_a(j) \in \{1, \ldots, n\}$ mit $ax_j = x_{\sigma_a(j)}$ (die Abbildung $G \ni x \mapsto ax \in G$ ist bijektiv). Damit ist $\sigma_a \in S_n$ und durch $h(a) := \sigma_a \, (a \in G)$ ist eine Abbildung $h : G \to S_n$ definiert.
Sind $a, b \in G$, so folgt aus $(ab)x_j = a(bx_j) = x_{\sigma_a(\sigma_b(j))}$

$$h(ab)(j) = \sigma_{ab}(j) = \sigma_a\big(\sigma_b(j)\big) = \big(h(a) \circ h(b)\big)(j)$$

für $j = 1, \ldots, n$. Also ist h ein Homomorphismus. Weiter folgt aus $\sigma_a = \mathrm{id}_{S_n}$ schon $ax_j = x_{\sigma_a(j)} = x_j$ für $j = 1, \ldots, n$. Für $x_j = e$ ergibt sich $a = e_G$. Folglich ist h injektiv, also eine Einbettung. Die Untergruppe $h(G) \subset S_n$ ist damit isomorph zu G. □

Der Satz zeigt, dass im Prinzip alle endlichen Gruppen als Untergruppe von S_n für ein n angesehen werden können. Es stellt sich allerdings die Frage, welche im konkreten Fall in Frage kommen – ein sehr schwieriges Problem. Wichtig in diesem Zusammenhang ist das Konzept der Normalteiler.

Definition 5.7 Es seien $(G, *)$ eine Gruppe und $H \subset G$ eine Untergruppe. Dann heißt H *Normalteiler* (oder *normale* Untergruppe) *von* (oder *in*) G, falls $Hg := H * g = g * H =: gH$ für alle $g \in G$ gilt (d. h., falls die Rechts- und Linksrestklassen bezüglich H übereinstimmen). Man schreibt dann

$$H \lhd G.$$

Beispiele 5.8 1. Ist $(G, *)$ abelsch, so ist jede Untergruppe Normalteiler. Ist $(G, *)$ beliebig, so sind jedenfalls G und $\{e\}$ Normalteiler.
2. Es sei $(G, *) = (S_3, \circ)$. Ist $H = \{id, (1,2)\}$, so existieren die drei Rechtsrestklassen

$$R_1 = H \cdot id\ , \quad R_2 = H \cdot (1,3) = \{(1,3),\ (1,3,2)\}\ ,$$
$$R_3 = H \cdot (2,3) = \{(2,3),\ (1,2,3)\}$$

und die drei Linksrestklassen

$$R_1 = id \cdot H\ , \quad R_2 = (1,3) \cdot H = \{(1,3), (1,2,3)\}\ ,$$
$$R_3 = (2,3) \cdot H = \{(2,3), (1,3,2)\}\ .$$

Hier stimmen die Rechts- und die Linksklassen zu $(1,3)$ und $(2,3)$ nicht überein. Also ist H kein Normalteiler in S_3.

Bemerkung und Definition 5.9 Es sei G eine Gruppe, und es sei H eine Untergruppe von G. Dann heißt für $g \in G$

$$H^g := gHg^{-1} := \{ghg^{-1} : h \in H\}$$

eine *konjugierte Untergruppe*. Man rechnet leicht nach, dass H^g stets eine Untergruppe von G ist ([Ü]). Äquivalent sind:

a) H ist Normalteiler in G,

b) $H^g = H$ für alle $g \in G$,

c) $H^g \subset H$ für alle $g \in G$.

a) $\Leftrightarrow$ b): Es gelte $gH = Hg$ für alle $g \in G$. Dann folgt

$$H^g = gHg^{-1} = (gH)g^{-1} = (Hg)g^{-1} = H\ .$$

Ist umgekehrt $gHg^{-1} = H$ für alle $g \in G$, so ergibt sich $gH = gHg^{-1}g = Hg$.
c) $\Rightarrow$ b): Es sei $g \in G$. Nach Voraussetzung ist $H^g \subset H$ und auch $H^{g^{-1}} \subset H$, also $H = (H^{g^{-1}})^g \subset H^g$.
b) $\Rightarrow$ c) ist klar.

Beispiel 5.10 1. Es seien K ein Körper und $(G,*) = (GL_n(K),\cdot)$ die Gruppe der invertierbaren $(n\times n)$ Matrizen über K mit der Matrix-Multiplikation (siehe B. 5.2.3). Dann ist

$$H := SL_n(K) := \{A \in GL_n(K) : \det A = 1\} = \text{Kern}(\det)$$

eine Untergruppe von $GL_n(K)$.
Ist $A \in GL_n(K)$, so gilt für alle $B \in SL_n(K)$:

$$\det(ABA^{-1}) = \det(A)\det(B)\det(A^{-1}) = \det(B) = 1\ ,$$

d. h. $ABA^{-1} \in SL_n(K)$. Damit gilt $H^A \subset H$, d h. H ist nach B. 5.9 Normalteiler in G.
2. Es seien $G = SL_2(K)$ und

$$H = \left\{ B = B_t = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} : t \in K \right\}\ .$$

Dann ist H eine Untergruppe von $SL_2(K)$.
(Denn: Es gilt
$(B_tB_s = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & s+t \\ 0 & 1 \end{pmatrix} = B_{s+t}$, also $(B_t)^{-1} = B_{-t}$.)
Für $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ gilt

$$AB_tA^{-1} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -t & 1 \end{pmatrix}$$

d. h. für $t \neq 0$ ist $AB_tA^{-1} \notin H$, also $H^A \not\subset H$. Damit ist H kein Normalteiler in $SL_2(K)$.

Satz 5.11 *Es seien G und H Gruppen und es sei $h : G \to H$ ein Homomorphismus. Ist $N \subset H$ ein Normalteiler von H, so ist $h^{-1}(N)$ ein Normalteiler von G. Insbesondere ist Kern(h) Normalteiler von G.*

Beweis. Es genügt, zu zeigen: Für alle $g \in G$ ist $(h^{-1}(N))^g \subset h^{-1}(N)$. Ist $g \in G$, so gilt

$$h(gh^{-1}(N)g^{-1}) = h(g)h(h^{-1}(N))(h(g))^{-1} \subset h(g)N(h(g))^{-1} = N$$

und damit auch $gh^{-1}(N)g^{-1} \subset h^{-1}(N)$.
Da $\{e_H\}$ ein Normalteiler von H ist, ist insbesondere

$$\mathrm{Kern}(h) = h^{-1}(\{e_H\})$$

Normalteiler von g. □

Die Normalteiler sind unter allen Untergruppen deswegen ausgezeichnet, weil die Restklassen von Normalteilern (wie die Restklassen von $m\mathbb{Z}$ in $\mathbb{Z}$) durch Definition einer Restklassenverknüpfung zu einer Gruppe gemacht werden können.

Satz 5.12 *Es seien G eine Gruppe und N ein Normalteiler in G. Dann ist auf*

$$G/N := G/_N := \{gN : g \in G\} \quad (= \{Ng : g \in G\} =_N \backslash G)$$

durch

$$Na * Nb := N(ab) \quad (a, b \in G) \ .$$

eine Abbildung $* = *_{G/N} : G/N \times G/N \to G/N$ (wohl-)definiert.

Beweis. Zu zeigen ist, dass die Definition unabhängig von den Repräsentanten a, b ist:
Es seien dazu a, b, a', b' mit $Na = Na'$ und $Nb = Nb'$ gegeben. Dann ist $b' \in Nb$. Da N Normalteiler in G ist, gilt auch $aN = a'N$ und damit ist $a' \in aN$. Also sind $a^{-1}a' \in N$ und $b'b^{-1} \in N$. Dann ist auch

$$a^{-1}a'b'b^{-1} \in N$$

und also

$$(a'b')(ab)^{-1} = (a'b')(b^{-1}a^{-1}) = a(a^{-1}a'b'b^{-1})a^{-1} \in aNa^{-1} = N^a = N \ .$$

Dies bedeutet wiederum $a'b' \in N(ab)$ bzw. $N(ab) = N(a'b')$. □

Bemerkung und Definition 5.13 Es seien G eine Gruppe, M eine nichtleere Menge und N ein Normalteiler in G.

1. Ist $*_M : M \times M \to M$ und ist $\pi : G \to M$ so, dass $\pi(ab) = \pi(a) *_M \pi(b)$ für alle $a, b \in G$, so ist $(\pi(G), *_M)$ eine Gruppe mit neutralem Element $\pi(e_G)$ und mit $(\pi(a))^{-1} = \pi(a^{-1})$ für alle $a \in G$ ([Ü]). Nach Definition ist dann $\pi : G \to h(G)$ ein (surjektiver) Homomorphismus.
2. Definiert man $\pi = \pi_N : G \to G/N$ durch

$$\pi_N(g) := Ng \qquad (g \in G),$$

so ist $(G/N, *_{G/N})$ nach S. 5.12 und 1. eine Gruppe und π_N ein surjektiver Homomorphismus. Dabei ist $\mathrm{Kern}(\pi_N) = N$. (Denn: Ist $\pi(a) = \pi(e_G) = N$, so ist $Na = N$ und damit $a \in N$. Umgekehrt folgt aus $a \in N$ auch wieder $Na = N$, also $\pi(a) = \pi(e_G)$.)
Die Gruppe $(G/N, *_{G/N})$ heißt *Faktorgruppe* (oder *Quotientengruppe*) von G nach N und die Abbildung π_N *kanonischer Homomorphismus*.
Nach Definition ist $\mathrm{ord}(G/N) = G : N$.
3. Die Aussage von 2. kann als eine gewisse Umkehrung von S. 5.11 gesehen werden, da jeder Normalteiler N in G der Kern eines Homomorphismus ist (nämlich etwa π_N).

Beispiele 5.14 1. Es seien $(G, *) = (\mathbb{Z}, +)$ und $N = m\mathbb{Z}$. Dann ist

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

und $\pi(a) = a + m\mathbb{Z} = [a]_m$ (vgl. B. 5.2.1) mit $\mathrm{Kern}(\pi) = m\mathbb{Z}$.
2. Es seien $(G, *) = (S_n, \circ)$ für $n \geq 2$ und $(H, *) = (\{\pm 1\}, \cdot)$. Dann ist durch

$$h(\sigma) := \mathrm{sign}(\sigma) \qquad (\sigma \in S_n)$$

ein Homomorpismus $h : S_n \to \{\pm 1\}$ definiert. Der Normalteiler

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

heißt alternierende Gruppe. Hier gilt

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

also $S_n : A_n = 2$. Aus $|S_n| = n!$ ergibt sich $\mathrm{ord}(A_n) = n!/2$ nach dem Satz von Lagrange.
Man kann zeigen: Für $n > 4$ ist A_n der einzige Normalteiler in S_n. Im Falle $n = 4$ ist auch noch die sog. Kleinsche Vierergruppe V_4 (siehe [Ü]) ein Normalteiler in S_4.

Der folgende Satz ist von zentraler Bedeutung für die Gruppentheorie.

Satz 5.15 *(Homomorphiesatz)*
Es seien G und H Gruppen, und es sei $h : G \to H$ ein surjektiver Homomorphismus mit $N := Kern(h)$. Dann ist durch $k \circ \pi_N = h$ ein Isomorphismus $k : G/N \to H$ (wohl-) definiert. Insbesondere sind also G/N und H isomorph.

Beweis. Wir zeigen: Durch $k(Na) := h(a)$ ist $k : G/N \to H$ wohldefiniert.
(Denn: Ist $Na = Na'$ für $a, a' \in G$, so gilt

$$a'a^{-1} \in N \ .$$

Also ist $e = h(a'a^{-1}) = h(a')(h(a))^{-1}$, d. h. $h(a') = h(a)$.)
Aus

$$k((Na) * (Nb)) = k(N(ab)) = h(ab) = h(a)h(b) = k(Na)k(Nb)$$

für alle $a, b \in G$ folgt, dass k ein Homomorphismus ist. Da h surjektiv ist, ist auch k surjektiv. Außerdem gilt $\text{Kern}(k) = \{N\}$, also besteht $\text{Kern}(k)$ genau aus dem neutralen Element in G/N. Damit ist k auch injektiv nach S. 5.3.5. □

Bemerkung 5.16 Es sei H eine zyklische Gruppe. Ist x ein erzeugendes Element, so ist $h : \mathbb{Z} \to H$, definiert durch $h(a) := x^a$, ein surjektiver Homomorphismus. Also ist H isomorph zu $\mathbb{Z}/\text{Kern}(h)$.
Im Falle $\text{ord}(H) = \infty$ ist $\text{Kern}(h) = \{0\}$ und im Falle $m := \text{ord}(H) < \infty$ ist $\text{Kern}(h) = m\mathbb{Z}$ (siehe S. 3.11). Damit ergibt sich wieder S. 5.4 (beachte: $\mathbb{Z}_m = \mathbb{Z}/(m\mathbb{Z})$).

Beispiele 5.17 1. Es seien K ein Körper und $G = GL_n(K)$. Dann ist $\det : G \to (K \setminus \{0\}, \cdot)$ ein surjektiver Homomorphismus mit $\text{Kern}(\det) = SL_n(K)$. Also ist $GL_n(K)/SL_n(K)$ isomorph zu $K \setminus \{0\}$.
2. Es seien $(G, *) = (\mathbb{R}^2, +)$ und $(H, *) = (\mathbb{R}, +)$. Dann ist durch

$$h(x, y) := x - y \quad ((x, y) \in \mathbb{R}^2)$$

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

$$\text{Kern}(h) = \{(x, x) : x \in \mathbb{R}\} =: U \ .$$

Nach dem Homomorphiesatz ist $\mathbb{R}^2/U$ isomorph zu $\mathbb{R}$.
3. In der Situation von B. 5.14.2 ist S_n/A_n isomorph zu $(\{\pm 1\}, \cdot)$.

6 Diedergruppen und Gruppen kleiner Ordnung

Wir beschäftigen uns nun – in Ansätzen – mit dem Zusammenspiel von Geometrie und Gruppentheorie.

Bemerkung und Definition 6.1 Es sei (X, d) ein metrischer Raum. Eine Abbildung $f : X \to X$ heißt *isometrisch* (oder *Bewegung*), falls

$$d\big(f(x), f(y)\big) = d(x, y) \qquad \text{für alle } x, y \in X.$$

Offensichtlich ist jedes isometrische f injektiv. Außerdem ist die Menge aller isometrischen und surjektiven f eine Untergruppe von $\big(S(X), \circ\big)$.

Bemerkung 6.2 Es sei $(X, d) = (\mathbb{R}^m, d_{|\cdot|})$, wobei $|\cdot|$ die euklidsche Norm bezeichnet. Sind $A \in \mathcal{O}(m)$ und $b \in \mathbb{R}^m$, wobei

$$\mathcal{O}(m) := \{A \in GL_m(\mathbb{R}) : A^{-1} = A^T\}$$

die sogenannte orthogonale Gruppe bezeichnet, so ist $T : \mathbb{R}^m \to \mathbb{R}^m$ mit

$$T(x) = Ax + b \qquad (x \in \mathbb{R}^m)$$

eine Bewegung.
(Denn: Für alle $x, y \in \mathbb{R}^m$ ist

$$\big|T(x) - T(y)\big|^2 = \big(A(x-y)\big)^T A(x-y) = (x-y)^T A^T A(x-y) = |x-y|^2.)$$

Man kann zeigen ($\to$ Lineare Algebra): Jede Bewegung $T : \mathbb{R}^m \to \mathbb{R}^m$ ist von dieser Form.
Wir betrachten den Fall $m = 2$ und zeigen unter Benutzung der multiplikativen Struktur von $\mathbb{C} = \mathbb{R}^2$:
$T : \mathbb{C} \to \mathbb{C}$ ist genau dann isometrisch, wenn T von der Form

$$T(z) = az + b \qquad (z \in \mathbb{C})$$

oder

$$T(z) = a\overline{z} + b \qquad (z \in \mathbb{C})$$

für ein $a \in \mathbb{C}$ mit $|a| = 1$ und ein $b \in \mathbb{C}$ ist.
(Denn: Klar ist, dass T von obiger Form isometrisch sind.

Es sei umgekehrt T isometrisch. Dann ist auch $T_1 : \mathbb{C} \to \mathbb{C}$ mit

$$T_1(z) = \frac{T(z) - T(0)}{T(1) - T(0)} \qquad (z \in \mathbb{C})$$

isometrisch (beachte: $\big|T(1) - T(0)\big| = |1 - 0| = 1$). Außerdem gilt $T_1(1) = 1$ und $T_1(0) = 0$. Hieraus folgt wiederum $T_1(i) = i$ oder $T_1(i) = -i$ ($\pm i$ sind die beiden Schnittpunkte der Kreise $\big\{|z| = 1\big\}$ und $\big\{|z - 1| = \sqrt{2}\big\}$).
Es seien $z = x + iy$ und $T_1(z) = u + iv$ mit $x, y, u, v \in \mathbb{R}$. Dann gilt

$$u^2 + v^2 = \big|T_1(z)\big|^2 = |z|^2 = x^2 + y^2$$

und damit auch

$$x^2 - 2x + 1 + y^2 = |z - 1|^2 = |T_1(z) - 1|^2 = x^2 - 2u + 1 + y^2,$$

d. h. $u = x$. Entsprechend ergibt sich $v = \pm y$, falls $T_1(i) = \pm i$. Also erhält man insgesamt: Entweder ist $T_1(z) = z$ für alle $z \in \mathbb{C}$ oder $T_1(z) = \overline{z}$ für alle $z \in \mathbb{C}$. Mit

$$a := T(1) - T(0), \qquad b := T(0)$$

ergibt sich die Behauptung.)

Bemerkung und Definition 6.3 Es sei $F \subset \mathbb{R}^m$. Eine Bewegung $T : \mathbb{R}^m \to \mathbb{R}^m$ heißt *Symmetrie* von F, falls $T(F) = F$ gilt. Wir setzen

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

Dann ist $\mathrm{Sym}(F)$ eine Untergruppe von $(S(\mathbb{R}^m), \circ)$ (Man beachte: Jede Bewegung $T : \mathbb{R}^m \to \mathbb{R}^m$ ist surjektiv, da von der Form $T(x) = Ax + b$ mit $A \in \mathcal{O}(m)$.)

Beispiel 6.4 Für $n \in \mathbb{N}, n \geq 2$, seien $\zeta = \zeta_n = e^{2\pi i/n}$ und $V_n := \{\zeta^0, \zeta, \ldots, \zeta^{n-1}\}$. Dann ist

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

das reguläre n-Eck mit den Eckpunkten $\zeta^k = e^{2\pi ik/n} (k = 0, 1 \ldots, n - 1)$. Die Gruppen

$$D_n := \mathrm{Sym}(R_n)$$

heißen *Diedergruppen.*
Wir wollen die Struktur von D_n etwas genauer beschreiben:
Ist $T \in D_n$, so ist notwendig $T(0) = 0$ (denn wäre $T(0) = b \neq 0$, so wäre $|\zeta^k - b| > 1$ für ein $k \in \{0, \ldots, n-1\}$. Für $z \in R_n$ mit $T(z) = \zeta^k$ ergäbe sich dann

$$1 < \big|T(z) - T(0)\big| = |z - 0| \leq 1,$$

Widerspruch.)
Damit ist T von der Form $T(z) = az$ oder $T(z) = a\overline{z}$ für ein $a(= T(1))$ mit $|a| = 1$.
Weiter folgt aus

$$|z| = 1, z \in R_n \Leftrightarrow z \in V_n,$$

dass $T(V_n) = V_n$ gilt. Ist $T(1) = \zeta^k$, so ist T von der Form $T(z) = \zeta^k z$ (Drehung um 0 mit Drehwinkel $2\pi k/n$) oder von der Form $T(z) = \zeta^k \overline{z}$ (Spiegelung an reeller Achse und anschließende Drehung mit Drehwinkel $2\pi k/n$).
Umgekehrt sind diese Abbildungen offensichtlich Symmetrien von R_n.
Mit $\tau(z) := \tau_n(z) := \zeta z$ und $\sigma(z) := \overline{z}$ gilt also

$$D_n = C_n \cup C_n\sigma = <\{\tau, \sigma\}>,$$

wobei

$$C_n := \{\tau^k : k = 0, \ldots, n-1\} = <\tau>$$

eine zyklische Gruppe der Ordnung n und ord $\sigma = 2$ (beachte $\overline{\overline{z}} = z$). Dabei ist

$$C_n\sigma = \{\tau^k \circ \sigma : k = 0, \ldots, n-1\}$$

die Rechtsrestklasse von C_n bezüglich σ. Also ist $|C_n| = n = |C_n\sigma|$ und $|D_n| = 2n$ (beachte: $\sigma \notin C_n$ und damit $C_n \cap C_n\sigma = \emptyset$).
Schließlich ist

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

Im Falle $n = 2$ (Strecke zwischen -1 und 1) ist

$$C_2 = \{\mathrm{id}, \tau_2\}, \quad C_2\sigma = \{\sigma, \tau_2 \circ \sigma\}$$

und für $n = 3$ (gleichseitiges Dreieck) ist $\zeta = e^{2\pi i/3}$ und

$$C_3 = \{\mathrm{id}, \tau_3, \tau_3^2\}, \quad C_3\sigma = \{\sigma, \tau_3 \circ \sigma, \tau_3^2 \circ \sigma\}.$$

Satz 6.5 *Bis auf Isomorphie ist D_n die einzige Gruppe der Ordnung $2n$, die von zwei Elementen a der Ordnung 2 und b der Ordnung n erzeugt wird mit $ab = b^{-1}a$.*

Beweis. Wie in B. 6.4 gesehen, hat D_n diese Eigenschaft. Es sei also G eine weitere solche Gruppe, also

$$G = <\{a, b\}>$$

mit ord $a = 2$, ord $b = n$ sowie $ab = b^{-1}a$. Wir betrachten

$$U := \{b^k a^j : k = 0, \ldots, n-1; j = 0, 1\} .$$

Da ord $a = 2$ ist, gilt $<a>= \{e, a\}$. Außerdem folgt aus ord $b = n$ genauso $<b>= \{e, b, \ldots, b^{n-1}\}$. Damit ist

$$U = <b> \cup <b>\, a .$$

Es seien $u, v \in U$, d. h. $u = b^k a^j, v = b^m a^\ell$ für $k, m \in \{0, \ldots, n-1\}, j, \ell \in \{0, 1\}$. Dann gilt

$$uv^{-1} = (b^k a^j)(b^m a^\ell)^{-1} = b^k a^j a^{-\ell} b^{-m}.$$

1. Fall: $a^{j-\ell} = e$. Dann ist $uv^{-1} = b^{k-m} \in <b> \subset U$.
2. Fall: $a^{j-\ell} = a$. Dann gilt

$$\begin{aligned} uv^{-1} &= b^k a b^{-m} = b^k a b b^{-m-1} = b^{k-1} a b^{-m-1} \\ &= \ldots = b^{k-(n-m)} a b^{-n} = b^{k-(n-m)} a \in <b>\, a \subset U. \end{aligned}$$

Nach B. 3.2.2 ist U eine Untergruppe von G.
Aus $\{a, b\} \subset U$ folgt $G = <\{a, b\}> \subset U$, also $G = U$. Sind σ, τ wie in B. 6.4, so ist durch

$$\tau^k \circ \sigma^j \mapsto b^k a^j \qquad (k = 0, \ldots, n-1, j = 0, 1)$$

ein Isomorphismus von D_n auf G definiert (beachte: $|G| = 2n = |D_n|$, also folgt aus „surjektiv" schon „bijektiv"). □

Weiter gilt

Satz 6.6 *Ist G eine endliche Gruppe mit der Eigenschaft, dass jedes $x \in G$, $x \neq e$ die Ordnung 2 hat, so ist G abelsch und* $\mathrm{ord}(G) = 2^m$ *für ein $m \in \mathbb{N}_0$.*

Beweis. 1. Nach Voraussetzung ist $a^2 = e$ für alle $a \in G$. Also folgt für alle $x, y \in G$

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

(übrigens auch in Fall einer unendlichen Gruppe).

2. Wir setzen

$$m := \min\{n \in \mathbb{N}_0 : \exists\, M \subset G,\ |M| = n,\ <M>= G\}$$

(wobei $<\emptyset>:= \{e\}$) und wählen $M \subset G$ mit $|M| = m$ so, dass $<M>= G$. Dann ist $e \notin M$ und aus 1. und S. 3.5.2 folgt

$$G = \left\{ \prod_{a \in F} a : F \subset M \right\}$$

(beachte: $<a>= \{e, a\}$). Da $|\mathrm{Pot}(M)| = 2^m$ gilt, reicht es, zu zeigen: Für $F, F' \subset M$ mit $F \neq F'$ ist

$$\prod_{a \in F} a \neq \prod_{a' \in F'} a' \ .$$

Angenommen, nicht. Ohne Einschränkung existiere also ein $a_0 \in F \setminus F'$. Dann ist

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

Damit ist schon $G = <M \setminus \{a_0\}>$ im Widerspruch zur Minimalität von m. □

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

Satz 6.7 *Ist $(G, *)$ eine Gruppe der Ordnung $2p$ für ein $p \in \mathbb{P}$, so ist entweder G zyklisch, also isomorph zu $(\mathbb{Z}_{2p}, +)$, oder isomorph zu D_p.*

Beweis. Nach S. 3.11 gilt ord $x \in \{2, p, 2p\}$ für alle $x \in G \setminus \{e\}$. Ist ord $x = 2p$ für ein $x \in G$, so ist $G = <x>$ und damit G zyklisch.
Es sei also ord $x \in \{2, p\}$ für alle $x \in G \setminus \{e\}$. Wir zeigen: G ist isomorph zu D_p.
Ist $p = 2$, so gilt also ord $x = 2$ für alle $x \neq e$. In diesem Fall ist G isomorph zu D_2 (Denn: Nach S. 6.6 ist G abelsch, also $ab = ba = b^{-1}a$ für alle $a, b \in G$. Sind $a, b \neq e$ mit $a \neq b$, so ist $\{a, b\}$ Erzeuger von G, da $ab \neq e$. Nach S. 6.5 ist G isomorph zu D_2.)
Es sei also $p \geq 3$. Dann existiert ein $b \in G$ mit ord $b = p$.
(Denn: Nach S. 6.6 existiert jedenfalls ein $e \neq b \in G$ mit ord $b \neq 2$, da $\mathrm{ord}(G) = 2p \neq 2^m$ für alle $m \in \mathbb{N}_0$. Also ist ord $b = p$).
Weiter existiert auch ein $a \in G$ mit ord $a = 2$ ([Ü]; man beachte, dass G gerade Ordnung hat).

Dabei gilt $a \notin <b>=: H$. (Denn: sonst wäre $a = b^n$ für ein $n \in \{1, \ldots, p-1\}$, also $e = a^2 = b^{2n}$, d. h. $p|2n$ nach S. 3.11. Da $p > 2$ ist, folgt $p|n$, also Widerspruch).
Damit ist $H \cap Ha = \emptyset (= H \cap aH)$, also (da $|G| = 2p$)

$$G = H \cup aH = H \cup Ha = <\{a, b\}> .$$

Hieraus ergibt sich auch $aH = Ha$, d. h. $H \lhd G$ und damit $aHa = aHa^{-1} = H^a = H$.
Folglich existiert ein $k \in \{0, \ldots, p-1\}$ mit

$$ab^k a = b$$

und damit auch $aba = a(ab^k a)a = b^k$ (da $a^2 = e$) sowie

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

Hieraus folgt

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

und damit $p|(k^2-1 = (k+1)(k-1))$. Da $p \in \mathbb{P}$ ist, erhält man $p|(k+1)$ oder $p|(k-1)$, also $k = p-1$ oder $k = 1$.
Ist $k = 1$, so ergibt sich $ab = ba^{-1} = ba$, also auch

$$(ab)^m = a^m b^m$$

für alle $m \in \mathbb{N}$ (Induktion).
Angenommen, $\mathrm{ord}(ab) = 2$. Dann gilt $e = (ab)^2 = a^2 b^2 = b^2$. Widerspruch zu $\mathrm{ord}(b) = p > 2$. Genauso führt die Annahme $\mathrm{ord}(ab) = p$ auf den Widerspruch $a^p = e$ (und p ungerade). Also bleibt nur die Möglichkeit $ab = e$. Dann ist aber $a = b^{-1} \in <b>$, also auch ein Widerspruch.
Damit erhalten wir $k = p-1$, d. h., $ab = b^{p-1}a = b^{-1}a$. Aus S. 6.5 folgt, dass G isomorph ist zu D_p. □

Bemerkung 6.8 Mit S. 6.7 können wir uns ein vollständiges Bild der Gruppen G der Ordnung ≤ 7 machen. Wir wissen bereits nach B. 5.5.1, dass jede Gruppe mit Primzahlordnung p zyklisch und damit isomorph zu $(\mathbb{Z}_p, +)$ ist. Es bleiben also die Fälle $n = 4$ bzw. $n = 6$. In diesen ist G entweder zyklisch oder isomorph zu D_2 bzw. D_3. Da $(\mathbb{Z}_p, +)$ und D_2 abelsch sind, sind insbesondere alle Gruppen der Ordnung ≤ 5 abelsch.

7 Weiteres zu Ringen und Körpern

In Abschnitt 3 haben wir u. A. auch Ringe und Körper definiert. Wir wollen noch einmal auf diese Strukturen zurückkommen.

Bemerkung und Definition 7.1 Es sei R ein Ring (bzw. ein Körper). Eine Menge $U \subset R$ heißt *Unterring* (bzw. *Unterkörper* oder *Teilkörper*), falls $(U, +_{|U\times U}, \cdot_{|U\times U})$ ein Ring (bzw. ein Körper) ist. Dann heißt R auch *Oberring* (bzw. *Oberkörper*) zu U. Es gilt (vgl. B. 3.2.2):
$U \neq \emptyset$ ist Unterring genau dann, wenn mit $x, y \in U$ auch $x - y \in U$ (also $U - U \subset U$) und $xy \in U$ (also $U \cdot U \subset U$). Gilt statt $U \cdot U \subset U$ dabei

$$R \cdot U \subset U \quad \text{und} \quad U \cdot R \subset U,$$

so heißt der Unterring U ein *Ideal* in R.
Ist R ein Körper, so ist U (mit $|U| \geq 2$) genau dann ein Teilkörper, wenn $U - U \subset U$ und $xy^{-1} \in U$ für $x, y \in U$, $y \neq 0$.

Bemerkung und Definition 7.2 Es seien R ein Ring und $M \subset R$. Dann heißen

$$<M> := <M>_R := \bigcap_{U \supset M \text{ Unterring}} U$$

$$\ll M \gg := \ll M \gg_R := \bigcap_{I \supset M \text{ Ideal}} I$$

der *von M erzeugte Unterring* bzw. das *von M erzeugte Ideal*. Entsprechend heißt für einen Körper K und $M \subset K$

$$<M> := <M>_K := \bigcap_{U \supset M \text{ Unterkörper}} U$$

der *der von M erzeugte Teilkörper*.
(Man beachte: Beliebige Schnitte von Unterringen bzw. Teilkörpern bzw. Idealen sind wieder Unterringe bzw. Teilkörper bzw. Ideale, wie sich unmittelbar aus B./D. 7.1 ergibt.)

Bemerkung und Definition 7.3 Es seien R ein kommutativer Ring mit Einselement und $x_1, \ldots, x_n \in R$. Dann ist

$$\ll x_1, \ldots, x_n \gg := \ll \{x_1, \ldots, x_n\} \gg = \left\{ \sum_{j=1}^{n} a_j x_j : a_j \in R \right\} \left(=: \sum_{j=1}^{n} Rx_j \right).$$

(Denn: Ist I die rechte Seite, so ist I ein Ideal, da $I - I \subset I$ und $R \cdot I \ (= I \cdot R) \subset I$. Außerdem ist $x_k = \sum_{j=1}^{n} \delta_{jk} x_j \in I$ für $k = 1, \ldots, n$. Also ist $\ll x_1, \ldots, x_n \gg \subset I$. Umgekehrt gilt für jedes Ideal $\widetilde{I}$ mit $\widetilde{I} \supset \{x_1, \ldots, x_n\}$ auch $\widetilde{I} \supset I$ und damit

$$\ll x_1, \ldots, x_n \gg \supset I.)$$

Insbesondere ist für $x \in R$

$$\ll x \gg = Rx \ (= xR)$$

das von x erzeugte Ideal. Ein solches, von einem Element erzeugte Ideal heißt ein *Hauptideal*. Speziell ist $\ll 1 \gg = R$ und damit stimmt ein Ideal, das 1 enthält, schon mit R überein.

Beispiel 7.4 Es sei $R = \mathbb{Z}$. Dann ist für $x \in \mathbb{Z}$

$$\ll x \gg = x\mathbb{Z}$$

und für $x_1, x_2 \in \mathbb{Z}$

$$\ll x_1, x_2 \gg = x_1\mathbb{Z} + x_2\mathbb{Z} = \mathrm{ggT}(x_1, x_2)\mathbb{Z} \ ,$$

also auch ein Hauptideal.

Wir setzen noch wie üblich

$$x^k := x \cdot x^{k-1}, \qquad x^0 := 1$$

für $k \in \mathbb{N}$.

Satz 7.5 *1. Es seien R ein kommutativer Ring mit Einselement 1 und $U \subset R$ ein Unterring mit $1 \in U$. Ferner seien $x_1, \ldots, x_n \in R$. Dann ist*

$$U[x_1, \ldots, x_n] := <U \cup \{x_1, \ldots, x_n\}>_R =$$
$$= \left\{ \sum_{\alpha \in E} a_\alpha x^\alpha : a_\alpha \in U, E \subset \mathbb{N}_0^n \ \textit{endlich} \right\}$$

(wobei $x^\alpha := x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ für $\alpha = (\alpha_1, \ldots, \alpha_n)$).

2. *Ist K ein Körper, so ist für jeden Unterring $U \subset K$ mit $1 \in U$ und für alle $x_1, \ldots, x_n \in K$*

$$U(x_1, \ldots, x_n) := <U \cup \{x_1, \ldots, x_n\}>_K = \\ = \left\{ \frac{\sum\limits_{\alpha \in E} a_\alpha x^\alpha}{\sum\limits_{\alpha \in F} b_\alpha x^\alpha} : \sum_{\alpha \in F} b_\alpha x^\alpha \neq 0, a_\alpha, b_\alpha \in U,\ E, F \subset \mathbb{N}_0^n \text{ endlich} \right\}.$$

Beweis. Ähnlich wie beim Beweis in B./D. 7.3 rechnet man nach, dass die rechte Seite in 1. ein Unterring ist, der U und $x_1, \ldots, x_n$ enthält. Andererseits enthält jeder Unterring, der U und $x_1, \ldots, x_n$ enthält, auch notwendigerweise die rechte Seite. Entsprechendes gilt in 2. mit Unterkörper statt Unterring. □

Bemerkung und Definition 7.6 Es sei R ein kommutativer Ring mit Einselement. Wir definieren

$$R^{[\mathbb{N}_0]} := \left\{(a_j) = (a_j)_{j=0}^\infty : a_j \in R, a_j = 0 \text{ bis auf endlich viele } j\right\}$$

(Menge der abbrechenden Folgen in R) und für $(a_j), (b_j) \in R^{[\mathbb{N}_0]}$

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

((c_j) heißt *Cauchy-Produkt* oder auch *Faltung* von (a_j) und (b_j)).
Damit ist $(R^{[\mathbb{N}_0]}, +, \cdot)$ ein kommutativer Ring mit Einselement $(1, 0, \ldots) = \left(\delta_{j0}\right)_{j=0}^\infty$ ([Ü]). Setzt man

$$X := (0, 1, 0, 0, \ldots) = \left(\delta_{j1}\right)_{j=0}^\infty,$$

so gilt für alle $k \in \mathbb{N}_0$

$$X^k = \left(\delta_{jk}\right)_{j=0}^\infty.$$

Also ist mit $n \in \mathbb{N}_0$ so, dass $a_j = 0$ für $j > n$,

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

(Hierbei ist $\lambda(a_j) := (\lambda a_j)$ für $\lambda \in R$ und $(a_j) \in R^{[\mathbb{N}_0]}$.)
Man nennt $P = (a_j) = \sum_{j=0}^{n} a_j X^j$ ein *Polynom über* R und schreibt auch

$$R[X] := R^{[\mathbb{N}_0]} \ \big(= \{P : P \text{ Polynom über } R\}\big).$$

Dabei gilt für $P = \sum_{j=0}^{m} a_j X^j$ und $Q = \sum_{j=0}^{n} b_j X^j$ nach obiger Definition

$$P \cdot Q = \sum_{j=0}^{n+m} c_j X^j = \sum_{j=0}^{m+n} \left(\sum_{k=0}^{j} a_k b_{j-k} \right) X^j$$

(beachte: $c_j = 0$ für $j > n + m$, da dann $j - k > n$ für $k \leq m$ gilt).
Ist weiterhin $U \subset R$ ein Unterring mit $1 \in U$, so setzen wir für $x \in R$

$$P(x) := \sum_{j=0}^{n} a_j x^j \ (\in R),$$

falls $P = \sum_{j=0}^{n} a_j X^j \in U[X]$. Ist dabei $P(x) = 0$, so heißt x eine *Wurzel* oder auch *Nullstelle* von P.
Nach. S. 7.5 ergibt sich für $x \in R$ damit

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

und im Falle eines Körpers R auch

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

Beispiel 7.7 1. Es seien $R = \mathbb{R}$ und $U = \mathbb{Z}$. Dann ist für $x \in \mathbb{R}$

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

also etwa

$$\mathbb{Z}[\sqrt{2}] = \big\{P(\sqrt{2}) : P \in \mathbb{Z}[X]\big\} = \{a + \sqrt{2}\, b : a, b \in \mathbb{Z}\} = \mathbb{Z} + \sqrt{2}\, \mathbb{Z}$$

(beachte: $(\sqrt{2})^j \in \mathbb{Z} \cup \sqrt{2}\, \mathbb{Z}$ für alle $j \in \mathbb{N}_0$).
2. Sind $R = \mathbb{C}$ und $U = \mathbb{R}$, so ist entsprechend

$$\mathbb{R}[i] = \{P(i) : P \in \mathbb{R}[X]\} = \{a + ib : a, b \in \mathbb{R}\} = \mathbb{R} + i\mathbb{R} = \mathbb{C} \ .$$

Bemerkung und Definition 7.8 Es seien R ein kommutativer Ring mit Einselement und $P = \sum_{j=0}^{n} a_j X^j \in R[X]$ mit $a_n \neq 0$. Dann heißt $\deg P := n$ *Grad* von P. Ist $P = 0$, so setzen wir $\deg P := -\infty$.
Mit $(-\infty) + a = a + (-\infty) := -\infty$ gilt: sind $P, Q \in R[X]$, so ist

$$\deg (P + Q) \leq \max(\deg P, \deg Q)$$
$$\deg (PQ) \leq \deg P + \deg Q$$

und im Falle eines Integritätsrings R genauer

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

Ist der Grad von $P \leq 0$, d. h. $P = a_0 X^0$ mit $a_0 \in R$, so schreiben wir kurz $P = a_0$ und nennen P auch ein *konstantes* Polynom.

Satz 7.9 *(Division mit Rest)*
Es seien K ein Körper und $B, P \in K[X], P \neq 0$. Dann existieren $Q, R \in K[X]$ mit $\deg R < \deg P$ und

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

Beweis. Ohne Einschränkung sei $\deg B \geq \deg P$ (sonst sind $R = B, Q = 0$ geeignet). Wir zeigen die Behauptung per Induktion nach $n = \deg B$.
$n = 0$: Ist $B = b_0$, so ist $P = a_0 \neq 0$, also sind $R = 0$ und $Q = b_0/a_0$ geeignet.
$n - 1 \to n$: Die Behauptung gelte für alle $0 \leq k < n$. Sind

$$P = \sum_{j=0}^{m} a_j X^j, \qquad B = \sum_{j=0}^{n} b_j X^j$$

mit $\deg B = n$ und $\deg P = m \leq n$, so hat

$$C := B - \frac{b_n}{a_m} X^{n-m} P \in K[X]$$

Grad $< n$ (führende Koeffizienten heben sich weg).
Ist $\deg C < m$, so sind $R = C$ und $Q = \dfrac{b_n}{a_m} X^{n-m}$ geeignet. Ist $\deg C \geq m$, so existieren nach Induktionsvoraussetzung $\widetilde{Q}, R \in K[X]$ mit $\deg R < \deg P$ und

$$C = \widetilde{Q} P + R.$$

Dann ist

$$B = C + \frac{b_n}{a_m} X^{n-m} P = \left(\widetilde{Q} + \frac{b_n}{a_m} X^{n-m} \right) P + R.$$

□

Bemerkung 7.10 Es seien K ein Körper und $B = \sum_{j=0}^{n} b_j X^j \in K[X]$. Ist $a \in K$ eine Wurzel von B, so existiert nach Satz 7.9 ein $Q = Q_a \in K[X]$ mit

$$B = Q(X - a).$$

Dabei ist das Polynom Q eindeutig bestimmt und es gilt $\deg(Q) + 1 = \deg(B)$ nach B./D. 7.8.
(Denn: $P := X - a$ hat Grad 1. Division mit Rest ergibt

$$B = Q(X - a) + R$$

mit $\deg R \in \{-\infty, 0\}$, d.h. $R = r_0$ mit einem $r_0 \in K$. Aus $0 = B(a) = R(a)$ folgt $r_0 = 0$. Eindeutigkeit: [Ü])
Induktiv ergibt sich daraus auch: Sind $a_1 \ldots, a_m \in K$ (paarweise verschiedene) Wurzeln von B, so existiert genau ein $Q = Q_{a_1,\ldots,a_m} \in K[X]$ mit

$$B = Q(X - a_1) \cdots (X - a_m) \, .$$

Aus $\deg(Q) + m = \deg(B)$ folgt insbesondere, dass jedes Polynom $B \neq 0$ nur endlich viele Wurzeln hat (nämlich nicht mehr als der Grad von B).

Definition 7.11 Es seien R und S Ringe. Eine Abbildung $f : R \to S$ heißt *(Ring-) Homomorphismus*, falls für alle $x, y \in R$

$$f(x + y) = f(x) + f(y) \text{ und } f(xy) = f(x)f(y)$$

gilt. Wieder heißt ein Ringhomomorphismus f

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

Existiert ein Isomorphismus $f : R \to S$, so heißen R, S isomorph (Schreibweise $R \simeq S$). Ist dabei R ein Körper, so ist auch S ein Körper.
Schließlich setzen wir wieder

$$\mathrm{Kern}(f) := f^{-1}\big(\{0_S\}\big) \, .$$

Bemerkung 7.12 Für Ringhomomorphismen $f : R \to S$ gelten natürlich sämtliche Aussagen von S. 5.3 für den Gruppenhomomorphismus $f : (R, +) \to (S, +)$. Mit ähnlichen Überlegungen ergibt sich zudem

(i) Die Verknüpfung zweier Isomorphismen und die Inverse eines Isomorphismus sind wieder Isomorphismen.

(ii) Ist $U \subset R$ ein Unterring (bzw. ein Ideal), so ist $f(U) \subset S$ ein Unterring (bzw. ein Ideal). Ist 1_R ein Einselement in R, so ist $f(1_R)$ Einselement in $f(U)$.

(iii) Ist $V \subset S$ ein Unterring (bzw. ein Ideal), so ist $f^{-1}(V) \subset R$ ein Unterring (bzw. ein Ideal). Insbesondere ist $\mathrm{Kern}(f)$ stets ein Ideal.

Ist R ein Körper, so ist f injektiv oder es ist $f(R) = \{0\}$.
(Denn: Ist f nicht injektiv, so existiert ein $0 \neq x \in \mathrm{Kern}(f)$. Damit ist

$$f(1) = f(xx^{-1}) = f(x)f(x^{-1}) = 0,$$

also auch

$$f(y) = f(y1) = f(y)f(1) = 0 \qquad (y \in R)).$$

Ideale entsprechen in vielerlei Hinsicht den Normalteilern in Gruppen. Wir wollen dies genauer beleuchten.

Bemerkung und Definition 7.13 Es seien R ein Ring und $I \subset \mathbb{R}$ ein Ideal.
1. Durch

$$(x + I) \cdot (y + I) := (xy) + I \qquad (x, y \in R).$$

ist eine Multiplikation $\cdot = \cdot_{R/I} : R/I \times R/I \to R/I$ auf der Menge der Restklassen

$$R/I = \{x + I : x \in R\} \quad \big(= \{I + x : x \in R\}\big)$$

wohldefiniert.
(Denn: Es seien $x, x', y, y' \in R$ mit $x' \in x + I, y' \in y + I$. Dann gilt

$$xy - x'y' = x\underbrace{(y - y')}_{\in I} + \underbrace{(x - x')}_{\in I}y' \in xI + Iy' \subset I + I \subset I,$$

also $x'y' \in xy + I$.)

2. Ist $(R/I, +)$ wie in B./D. 5.13, so ist $(R/I, +, \cdot)$ ein Ring. Außerdem ist die Abbildung $\pi = \pi_I : R \to R/I$, definiert durch

$$\pi(x) := x + I \qquad (x \in R),$$

ist ein surjektiver Ringhomomorphismus mit Kern $(\pi) = I$.
(Denn: Nach B./D. 5.13 ist $(R/I, +)$ ist eine (offensichtlich kommutative) Gruppe. Außerdem ist $\pi : (R, +) \to (R/I, +)$ ein surjektiver Gruppenhomomorphismus mit Kern $(\pi) = I$.
Aus der repräsentantenweisen Definition von $+$ und $\cdot$ in R/I folgen unmittelbar die Bedingungen (R.2) und (R.3), also ist R/I ein Ring. Außerdem gilt auch $\pi(xy) = \pi(x)\pi(y)$ für $x, y \in R$, d. h. π ist ein Ringhomomorphismus.)
Der Ring $(R/I, +, \cdot)$ heißt *Restklassenring von R modulo I* (oder *von R nach I*). Im Falle $R = \mathbb{Z}$ und $I = m\mathbb{Z}$ ergibt sich der ,,klassische" Restklassenring $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$ (vgl. S. 2.15).

Bemerkung 7.14 Wie im Falle von Gruppen sieht man mit B. 7.12 und B./D. 7.13: Ideale sind genau die Kerne von Ringhomomorphismen.
Weiter ergibt sich durch Anwendung von S. 5.15 folgender Homomorphiesatz für Ringe: *Sind R, S Ringe und ist $f : R \to S$ ein surjektiver Homomorphismus, so ist für $I := Kern(f)$ durch $g \circ \pi_I = f$ ein Isomorphismus $g : R/I \to S$ definiert.*

Wir wollen nun zeigen, dass jeder Ring mit Einselement eine ,,Kopie" von $\mathbb{Z}_q$ für ein geeignetes $q \in \mathbb{N}_0$ enthält.

Satz 7.15 *Es seien R ein Ring mit Einselement 1_R und $\mathbb{Z}1_R := \{n1_R : n \in \mathbb{Z}\}$. Dann gilt*

1. *$\mathbb{Z}1_R$ ist Unterring von R und isomorph zu $(\mathbb{Z}_q, +, \cdot)$, wobei*

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

2. *$\mathbb{Z}1_R$ ist genau dann nullteilerfrei, wenn $q \in \{0, 1\} \cup \mathbb{P}$.*

Beweis. 1. Nach der Definition von nx für $n \in \mathbb{Z}, x \in R$, ist klar, dass $\mathbb{Z}1_R$ ein Unterring $f : \mathbb{Z} \to \mathbb{Z}1_R$, $f(n) := n1_R$, ein (surjektiver) Homomorphismus ist. Dabei gilt $\mathrm{Kern}(f) = q\mathbb{Z}$. Nach dem Homomorphiesatz (B./D. 7.14) ist $\mathbb{Z}1_R \simeq \mathbb{Z}/(q\mathbb{Z}) = \mathbb{Z}_q$.
2. Nach 1. ist $\mathbb{Z}1_R$ genau dann nullteilerfrei, wenn $(\mathbb{Z}_q, +, \cdot)$ nullteilerfrei ist. (Man beachte: Sind S_1 und S_2 isomorphe Ringe, so ist S_1 genau dann nullteilerfrei, wenn S_2 nullteilerfrei ist.)
Ist $q \notin \{0, 1\} \cup \mathbb{P}$, so ist $(\mathbb{Z}_q, +, \cdot)$ nicht nullteilerfrei (denn dann ist $q = rs$ mit $1 < r, s < q$, also $[rs]_q = [q]_q = [0]_q$, aber $[r]_q, [s]_q \neq [0]_q$).
Andererseits sind $(\mathbb{Z} = \mathbb{Z}_0, +, \cdot)$ und $(\mathbb{Z}_1 = \{[0]_1\}, +, \cdot)$ nullteilerfrei, und im Falle $q \in \mathbb{P}$ ist $(\mathbb{Z}_q, +, \cdot)$ sogar ein Körper (B. 2.21.2). □

Bemerkung und Definition 7.16 Ist R ein Ring mit Einselement 1_R, so heißt die Zahl $q \in \mathbb{N}_0$ aus S. 7.15 *Charakteristik* von R. Ist dabei $K = R$ ein Körper, so ist $q \in \{0\} \cup \mathbb{P}$. Im Fall $q \in \mathbb{P}$ ist also $\mathbb{Z}1_K$ isomorph zum Körper $(\mathbb{Z}_q, +, \cdot)$, d. h. K enthält eine ,,Kopie" von $\mathbb{Z}_q$. Wir werden im Weiteren sehen, dass im Falle $q = 0$ der Körper K eine ,,Kopie" von $(\mathbb{Q}, +, \cdot)$ enthält.

Wir beweisen zunächst, dass jeder Integritätsring durch ,,Quotientenbildung" zu einem Körper erweitert werden kann.

Bemerkung und Definition 7.17 Es sei R ein Integritätsring. In Analogie zur Definition von $\mathbb{Q}$ aus $\mathbb{Z}$ definiert man den Körper $K =: \mathrm{Quot}(R)$ der Quotienten durch Äquivalenzklassenbildung in $R \times \big(R \setminus \{0\}\big)$:
Sind (a, b) und $(a', b') \in R \times \big(R \setminus \{0\}\big)$, so setzt man

$$(a, b) \sim (a', b') :\Longleftrightarrow ab' = a'b.$$

Dann ist $\sim$ eine Äquivalenzrelation (denn: Reflexivität und Kommutativität sind klar; aus $(a, b) \sim (a', b')$ und $(a', b') \sim (a'', b'')$ folgt

$$b'ab'' = a'bb'' = a''b'b,$$

also mit der Kürzungsregel aus B. 2.8 auch $ab'' = a''b$).
Damit setzt man

$$\frac{a}{b} := a/b := \big\{(x, y) \in R \times \big(R \setminus \{0\}\big) : (x, y) \sim (a, b)\big\} = \big[(a, b)\big]_\sim$$

und $K = \mathrm{Quot}(R) := \{a/b : a \in R, b \in R \setminus \{0\}\}$. Außerdem definiert man $+ : K \times K \to K$ und $\cdot : K \times K \to K$ durch

$$\frac{a}{b} + \frac{c}{d} := \frac{ad + cb}{bd}$$

$$\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$$

(wichtig wie immer: Definition ist unabhängig von der Wahl der Repräsentanten!).
Durch Nachrechnen sieht man: $(K, +, \cdot)$ ist ein Körper mit $0_K = 0_R/1_R$, $1_K = 1_R/1_R$ und $(a/b)^{-1} = b/a$, falls $a \neq 0_R$. Außerdem ist durch $j(a) := a/1_R$ eine Einbettung $j : R \to K$ definiert. Damit ist $R \simeq j(R) \subset K$. Indem man $j(R)$ mit R identifiziert kann man R als Unterring von K auffassen.
Schließlich gilt dabei noch: Ist E ein weiterer Körper und ist $f : R \to E$ ein Monomorphismus, so ist durch

$$F\left(\frac{a}{b}\right) := \frac{f(a)}{f(b)} \qquad \left(\frac{a}{b} \in K\right)$$

ein (Körper-)Homomorphismus $F : K \to E$ definiert mit $f = F \circ j$ (oder kurz $F_{|R} = f$ bei Identifikation von R und $j(R)$). Dabei ist F auch injektiv (siehe B. 7.12). Außerdem ist F durch f eindeutig bestimmt (d. h. ist $\widetilde{F} : K \to E$ ein Homomorphismus mit $\widetilde{F} \circ j = f$, so ist $\widetilde{F} = F$). Wir nennen F die *kanonische Erweiterung* von f.

Bemerkung 7.18 Es sei E ein Körper mit Charakteristik 0. Ist $f : \mathbb{Z} \to E$ definiert durch $f(n) := n1_E$ für $n \in \mathbb{Z}$, so ist f nach dem Beweis zu S. 7.15 injektiv. Also ist die kanonische Erweiterung $F : \mathbb{Q} = \mathrm{Quot}(\mathbb{Z}) \to E$ von $f : \mathbb{Z} \to E$ gemäß B./D. 7.17 eine Einbettung. Damit ist $\mathbb{Q}$ isomorph zum Teilkörper $F(\mathbb{Q})$ von E.

Bemerkung und Definition 7.19 Ist K ein beliebiger Körper, so heißt

$$P(K) := \bigcap_{U \subset K \text{ Teilkörper}} U$$

Primkörper von K. Es gilt damit: Hat K die Charakteristik $q \in \{0\} \cup \mathbb{P}$, so ist $P(K)$ isomorph zu $(\mathbb{Z}_q, +, \cdot)$ im Falle $q \in \mathbb{P}$ und zu $(\mathbb{Q}, +, \cdot)$ im Falle $q = 0$.
(Denn: Zunächst hat jeder Teilkörper nach Definition die gleiche Charakteristik und es gilt $P(K) \supset \mathbb{Z}1_K$. Ist $q \in \mathbb{P}$, so ist $\mathbb{Z}1_K$ isomorph zu $(\mathbb{Z}_q, +, \cdot)$, also ein Körper und damit auch $P(K) = \mathbb{Z}1_K$. Ist $q = 0$, so enthält jeder Teilkörper U von K nach B. 7.18 die „Kopie" $F(\mathbb{Q})$ von $(\mathbb{Q}, +, \cdot)$. Damit ist $P(K) = F(\mathbb{Q})$.)

8 Körpererweiterungen

Wir untersuchen einfache Aspekte der Körpertheorie, die wir im Weiteren nutzen werden, um einige klassische Fragen zur Konstruktion mit Zirkel und Lineal zu beantworten.

Bemerkung und Definition 8.1 1. Es seien K und E Körper. Ist $0 \neq j : K \to E$ ein Homomorphismus, so ist j nach B. 7.12 schon eine Einbettung. Man nennt $j : K \to E$ *(Körper-)Erweiterung* und spricht auch von E als *(Körper-)Erweiterung* von K. Im Fall $E \supset K$ sei stets $j : K \to E$ definiert durch $j(x) := x$ ür $x \in K$.
2. Ist $j : K \to E$ eine Erweiterung, so kann man E als K-Vektorraum auffassen, indem man die Skalarmultiplikation $\cdot = \cdot_j : K \times E \to E$ durch

$$x \cdot y := j(x) \cdot y \qquad (x \in K, y \in E)$$

definiert. Wir setzen

$$[E : K] := [E : K]_j := \dim_K(E) = \dim_K((E, +, \cdot_j)).$$

Dabei heißt die Erweiterung *endlich*, falls $[E : K] < \infty$. Außerdem heißt $[E : K]$ dann *Grad* der Erweiterung.

Beispiele 8.2 Nach B. A.10 ist $[\mathbb{C} : \mathbb{R}] = 2$ und $[\mathbb{R} : \mathbb{Q}] = \infty$.

Satz 8.3 *Es seien $j : K \to E$ und $k : E \to F$ Erweiterungen. Sind j und k endlich, so ist $k \circ j$ endlich und es gilt*

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

Beweis. Es seien B eine Basis von E als K-Vektorraum und C eine Basis von F als E-Vektorraum.
Ist $z \in F$, so existieren $\mu_y \in E$ mit

$$z = \sum_{y \in C} \mu_y y \quad \left(= \sum_{y \in C} j(\mu_y) y \right).$$

Weiter existieren zu jeden $y \in C$ Skalare $\lambda_{xy} \in K$ mit $\mu_y = \sum\limits_{x \in B} \lambda_{xy} x$. Also ist

$$z = \sum_{y \in C} \sum_{x \in B} \lambda_{xy} xy \quad \left(= \sum_{y \in C} \sum_{x \in B} (k \circ j)(\lambda_{xy}) k(x) y \right).$$

Also ist $BC = \{xy : x \in B, y \in C\}$ ein Erzeugendensystem von F als K-Vektorraum. Ist $z = 0$ in obiger Darstellung, so folgt zunächst $\mu_y = 0$ für $y \in C$ und damit auch $\lambda_{xy} = 0$ für $x \in B$, $y \in C$. Damit ist BC eine Basis von F als K-Vektorraum. Aus $|BC| = |B \times C| = |B| \cdot |C|$ folgt

$$[F : K] = |BC| = |B| \cdot |C| = [F : E][E : K].$$

□

Definition 8.4 Es seien $j : K \to E$ eine Erweiterung und $x \in E$. Dann heißt x *algebraisch* über K, falls ein Polynom $P = \sum\limits_{\nu=0}^{n} a_\nu X^\nu \in K[X]$, $P \neq 0$, existiert mit

$$0 = P(x) := \sum_{\nu=0}^{n} a_\nu x^\nu \ (:= \sum_{\nu=0}^{n} j(a_\nu) x^\nu)$$

(m. a. W. falls $\left(x^n\right)_{n=0}^{\infty}$ linear abhängig in E als K-Vektorraum ist). Wir nennen x dann auch eine *Wurzel* von P. Existiert kein solches Polynom, so heißt x *transzendent* über K.
Die Erweiterung $j : K \to E$ heißt *algebraisch*, falls jedes $x \in E$ algebraisch über K ist. Ist $E \supset K$. so sagt man auch, E sei *algebraisch über* K.

Beispiele 8.5 1. $\mathbb{C}$ ist algebraisch üeber $\mathbb{R}$, denn ist $z = x + iy \in \mathbb{C}$, so ist $P(z) = 0$ etwa für

$$P = (X - x)^2 + y^2 = X^2 - 2xX + (x^2 + y^2) \in \mathbb{R}[X].$$

2. $\sqrt{2}$ ist algebraisch über $\mathbb{Q}$, da $P(\sqrt{2}) = 0$ etwa für

$$P = X^2 - 2 \in \mathbb{Q}[X].$$

$\mathbb{R}$ ist jedoch nicht algebraisch über $\mathbb{Q}$, da $\mathbb{Q}[X]$ abzählbar ist und damit auch die Menge $\mathbb{A}$ der reellen algebraischen Zahlen über $\mathbb{Q}$ (jedes Polynom hat nur endlich viele Nullstellen).
Wir werden später sehen, dass e und π transzendent über $\mathbb{Q}$ sind.

Bemerkung und Definition 8.6 Es sei $j : K \to E$ eine Erweiterung. Ist $x \in E$, so ist durch $\varphi_x : K[X] \to E$

$$\varphi_x(P) := P(x) \qquad (P \in K[X])$$

sowohl ein Ring- als auch ein Vektorraum-Homomorphismus definiert. Daher ist

$$K_j[x] := \varphi_x\big(K[X]\big) = \big\{P(x) : P \in K[X]\big\}$$

ein Unterring und ein linearer Teilraum von E (genauer eine K-Algebra). Die Abbildung φ_x heißt *Einsetzungshomomorphismus* bzgl. x. Nach Definition ist φ_x genau dann eine Einbettung (also injektiv), wenn x transzendent über K ist. Im Falle $E \supset K$ ist $K[x] = K_j[x]$ wie in S. 7.5. Wir schreiben daher auch kurz $K[x]$ statt $K_j[x]$.

Ein Polynom $P = \sum_{\nu=0}^{n} a_\nu X^\nu$ heißt *normiert*, falls $a_n = 1$. Es gilt damit

Satz 8.7 *Es seien $j : K \to E$ eine Erweiterung und $x \in E$.*

1. *Ist x transzendent über K, so ist $\dim_K \big(K[x]\big) = \infty$.*
2. *Ist x algebraisch über K, so existiert genau ein normiertes Polynom $P = P_x$ minimalen Grades in $K[X]$ mit $P(x) = 0$, und jedes Polynom $B \in K[X]$ mit $B(x) = 0$ ist Vielfaches von P (d. h. $B = QP$ für ein $Q \in K[X]$). Außerdem ist $\{x^{k-1} : k = 1, \ldots, \deg P\}$ eine Basis des K-Vektorraumes $K[x]$.*

Beweis. 1. Ist x transzendent über K, so sind nach Definition $(x^n)_{n\in\mathbb{N}_0}$ linear unabhängig in E (als K-Vektorraum). Damit ist $\dim_K \big(K[x]\big) = \infty$.
2. Es sei x algebraisch über K. Wir setzen

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

und wählen $P = \sum_{\nu=0}^{m} a_\nu X^\nu \in K[X]$ mit $\deg P = m, P(x) = 0$ und ohne Einschränkung so, dass $a_m = 1$.
Es sei $B \in K[X]$. Nach S. 7.9 existieren $Q, R \in K[X]$ mit $B = QP + R$ und $\deg R < \deg P$. Ist dabei $B(x) = 0$, so folgt

$$R(x) = B(x) - Q(x)P(x) = 0.$$

Nach Definition von m ist $R = 0$, also $B = QP$. Ist zudem B normiert mit $\deg B = \deg P$, so ist $Q = 1$ mit B./D. 7.8.
Es sei $K_{<m}[X]$ die Menge der Polynome in $K[X]$ vom Grad $\leq m-1$. Dann ist nach obigen Überlegungen $\varphi_{x|K_{<m}[X]}$ injektiv. Außerdem ist $\varphi_x\big(K_{<m}[X]\big) = K[x]$.
(Denn: Ist $y \in K[x]$ so ist $y = \varphi_x(B)$ für ein $B \in K[X]$. Sind Q, R wie oben, so ist $R \in K_{<m}[X]$ und

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

Damit sind $K_{<m}[X]$ und $K[x]$ isomorph als K-Vektorräume. Da $\{X^{k-1}, k = 1, \ldots, m\}$ eine Basis von $K_{<m}[X]$ ist, ist $\{\varphi_x(X^{k-1}) = x^{k-1}, k = 1, \ldots, m\}$ eine Basis von $K[x]$.
□

Bemerkung und Definition 8.8 1. Es seien K ein Körper und $P \in K[X]$. Dann heißt P *irreduzibel* (über K), falls gilt: Ist $P = QR$ mit $Q, R \in K[X]$, so ist grad $Q \leq 0$ oder grad $R \leq 0$ (also Q oder R konstant).
2. Ist $j : K \to E$ eine Erweiterung und ist x algebraisch über K, so heißt das Polynom P_x aus S. 8.7.2 *Minimalpolynom von x bezüglich K*. Ist $m = \deg P_x$, so heißt m auch *Grad von x über K*.
Es gilt damit: Ist $B \in K[X]$ normiert mit $B(x) = 0$, so ist B genau dann irreduzibel, wenn $B = P_x$ gilt.
(Denn: $\Rightarrow$: Nach S. 8.7 ist $B = QP_x$ mit einem $Q \in K[X]$. Da B irreduzibel ist, gilt $\deg Q \leq 0$ und da B normiert ist damit $Q = 1$.
$\Leftarrow$: Ist $P_x = QR$, so gilt $Q(x)R(x) = 0$, also $Q(x) = 0$ oder $R(x) = 0$. Aus $\deg Q + \deg R = \deg P_x$ und der Minimalität von $\deg P_x$ folgt $\deg Q \leq 0$ oder $\deg R \leq 0$.)

Beispiel 8.9 1. Das Minimalpolynom von i bzgl. $\mathbb{R}$ ist gegeben durch $P = X^2 + 1$. Insbesondere ist i vom Grad 2 über $\mathbb{R}$. Nach B. 8.5.1 ist jedes $z \in \mathbb{C} \setminus \mathbb{R}$ vom Grad 2 über $\mathbb{R}$.
2. Das Minimalpolynom von $\sqrt{2}$ bzgl. $\mathbb{Q}$ ist gegeben durch $P = X^2 - 2$. Also ist $\sqrt{2}$ vom Grad 2 über $\mathbb{Q}$. Nach S. 8.7 ist $\{1, \sqrt{2}\}$ eine Basis von $\mathbb{Q}[\sqrt{2}]$, also insbesondere $\mathbb{Q}[\sqrt{2}] = \mathbb{Q} + \sqrt{2} \cdot \mathbb{Q}$.

Satz 8.10 *Es seien $j : K \to E$ eine Erweiterung und $x \in E$, $x \neq 0$. Dann sind äquivalent:*

a) x ist algebraisch über K.

b) $K[x]$ ist ein Teilkörper von E.

Beweis. b) $\Rightarrow$ a) Aus $x \in K[x]$ folgt nach Voraussetzung die Existenz eines $P \in K[X]$ mit $1/x = P(x)$. Damit ist x Wurzel des Polynoms $1 - XP \in K[X]$, also algebraisch über K.
a) $\Rightarrow$ b): Da $K[x]$ ein Unterring von E ist, genügt es, zu zeigen: Für $y \in K[x]$, $y \neq 0$ ist $1/y \in K[x]$.
Ist $P(y) = \sum_{\nu=r}^{d} a_\nu y^\nu = 0$ mit $a_r \neq 0$, so gilt auch

$$\sum_{\nu=r}^{d} \frac{a_\nu}{a_r}\, y^{\nu-r-1} = 0,$$

also

$$\frac{1}{y} = \sum_{\nu=r+1}^{d} -\frac{a_\nu}{a_r}\, y^{\nu-r-1} = \sum_{k=0}^{d-r-1} \underbrace{-\frac{a_{k+r+1}}{a_r}}_{\in K} y^k.$$

Da $K[x]$ eine K-Algebra ist, folgt $1/y \in K[x]$. □

Bemerkung 8.11 Es sei $j : K \to E$ eine endliche Erweiterung. Ist $x \in E$, so ist x nach S. 8.7.1 algebraisch über K, also $K[x]$ nach S. 8.10 ein Teilkörper von E. Offensichtlich ist durch $K \ni a \mapsto ax^0 (= j(a)x^0) \in K[x]$ eine Einbettung definiert. Dabei ist $\big[K[x] : K\big]$ nach S. 8.7.2 der Grad von x über K. Außerdem gilt nach S. 8.3

$$[E : K] = \big[E : K[x]\big] \cdot \big[K[x] : K\big]$$

(aus $[E : K] < \infty$ folgt auch $\big[E : K[x]\big] < \infty$). Insbesondere ist also $\big[K[x] : K\big]$ ein Teiler von $[E : K]$.

Satz 8.12 *Es sei $j : K \to E$ eine Erweiterung. Dann ist die Menge $A \subset E$ der algebraischen Elemente über K ein Teilkörper von E.*

Beweis. Nach S. 8.10 ist mit $0 \neq x \in A$ auch $1/x \in K[x]$. Also genügt es (nach B./D. 7.1) zu zeigen: A ist ein Unterring von E, d.h. mit $x, y \in A$ sind auch $x - y$ und $x \cdot y$ in A (beachte: dann ist auch $K[x] \subset A$ für jedes $x \in A$).
Es seien $x, y \in A$. Sind $\{x^{\nu-1} : \nu = 1, \ldots, n\}$ und $\{y^{\mu-1} : \mu = 1, \ldots, m\}$ Basen von $K[x]$ und $K[y]$ gemäß S. 8.7, so ist $\{x^{\nu-1}y^{\mu-1} : \nu = 1, \ldots, n;\ \mu = 1, \ldots, m\}$ ein Erzeugendensystem von

$$K[x, y] := K_j[x, y] := \operatorname{span}\{x^N y^M : M, N \in \mathbb{N}_0\} .$$

(Denn: Für beliebige $M, N \in \mathbb{N}_0$ ist

$$x^M = \sum_{\nu=1}^{n} a_\nu x^{\nu-1}, \qquad y^N = \sum_{\mu=1}^{m} b_\mu y^{\mu-1}$$

für gewisse $a_\nu, b_\mu \in K$. Damit ist

$$x^M y^N = \sum_{\nu=1}^{n} \sum_{\mu=1}^{m} a_\nu b_\mu x^{\nu-1} y^{\mu-1}.)$$

Insbesondere ist $\dim_K(K[x, y]) < \infty$. Aus $K[x - y] \subset K[x, y]$ und $K[xy] \subset K[x, y]$ folgt $\dim_K K[x-y] < \infty$ und $\dim_K K[xy] < \infty$. Nach S. 8.7.1 sind $x-y, x\cdot y \in A_K$. □

9 Konstruktionen mit Zirkel und Lineal

Zu den klassischen Fragen der Mathematik gehört die Konstruierbarkeit reeller Zahlen mit Zirkel und Lineal. Was versteht man unter einer solchen Konstruktion?

Definition 9.1 Es sei S eine Menge in $\mathbb{R}^2$. Ein Punkt $P \in \mathbb{R}^2$ heißt *konstruierbar (mit Zirkel und Lineal) aus* S, falls ein $n \in \mathbb{N}$ und Punkte $P_1, \ldots, P_n$ in $\mathbb{R}^2$ existieren mit $P_n = P$ und so, dass für $S_0 := S$ und $S_j := S_{j-1} \cup \{P_j\}$, $(j = 1, \ldots, n)$ eine der folgenden Bedingungen erfüllt ist:

(i) Es existieren $A, B, A', B' \in S_{j-1}$ so, dass P_j der Schnittpunkt der beiden (nichtparallelen) Geraden durch A, B und A', B' ist.

(ii) Es existieren $A, B, C, D \in S_{j-1}$ so, dass P_j einer der (höchstens 2) Schnittpunkte der Gerade durch A, B und des Kreises mit Mittelpunkt C und einem Randpunkt D ist.

(iii) Es existieren $C, D, C', D' \in S_{j-1}$ so, dass P_j einer der (höchstens 2) Schnittpunkte der Kreise mit Mittelpunkt C und Randpunkt D sowie Mittelpunkt $C'(\neq C)$ und Randpunkt D' ist.

Weiter heißt ein $x \in \mathbb{R}$ *konstruierbar* aus $S \subset \mathbb{R}$, falls der Punkt $(x, 0)$ konstrierbar aus $S \times \{0\}$ ist. Für $S \subset \mathbb{R}$ setzen wir $\mathrm{kon}(S) := \{x \in \mathbb{R} : x \text{ konstruierbar aus } S\}$.

Bemerkung 9.2 Es sei $S \subset \mathbb{R}$ mit $0, 1 \in S$. Dann gilt:

1. Der Punkt $(0, 1)$ ist konstruierbar aus $S \times \{0\}$.
2. Sind P, Q konstruierbar aus $S \times \{0\}$, so sind auch $P \pm Q$ konstruierbar aus $S \times \{0\}$.
3. Ist (x, a) konstruierbar aus $S \times \{0\}$ für ein $a \in \mathbb{R}$, so ist $x \in \mathrm{kon}(S)$.

Satz 9.3 *Es sei $S \subset \mathbb{R}$ mit $\{0, 1\} \subset S$. Dann sind mit $x, y \in kon(S)$ auch $x \pm y, xy \in kon(S)$ und im Falle $y \neq 0$ auch $1/y$. Außerdem ist für $x > 0$ auch $\sqrt{x} \in kon(S)$.*

Beweis. Siehe Vorlesung. □

Bemerkung 9.4 Aus S. 9.3 folgt insbesondere, dass kon(S) im Falle $\{0,1\} \subset S$ ein Teilkörper von $\mathbb{R}$ ist. Damit ist schon $\mathbb{Q} \subset \text{kon}(S)$. Also ist $\text{kon}(\mathbb{Q}) \subset \text{kon}\big(\text{kon}(S)\big) = \text{kon}(S)$ (und damit im Falle $S \subset \mathbb{Q}$ auch „=").

Satz 9.5 *Es seien K ein Körper und E ein Oberkörper von K. Ist $[E : K] = 2$, so existiert ein $a \in E \setminus K$ mit $a^2 \in K$ und $E = span\ \{1, a\} = K + Ka$.*

Beweis. Es sei $x \in E \setminus K$. Dann sind $1, x$ linear unabhängig und damit eine Basis von E als K-Vektorraum. Also existieren $p, q \in K$ mit

$$x^2 + px + q = 0,$$

d. h.

$$\left(x + \frac{p}{2}\right)^2 = \frac{p^2}{4} - q\ (\in K).$$

Für $a := x + \frac{p}{2}$ gilt $a^2 \in K$ und $a \in E \setminus K$. Insbesondere sind auch $1, a$ linear unabhängig (über K). Damit ist $\{1, a\}$ eine Basis von E und folglich

$$E = \text{span}\{1, a\} = K + Ka.$$

□

Damit beweisen wir

Satz 9.6 *Es sei K ein Teilkörper von $\mathbb{R}$. Für $x \in \mathbb{R}$ sind äquivalent:*

a) $x \in kon(K)$.

b) Es existieren ein $n \in \mathbb{N}_0$ und Teilkörper

$$K = K_0 \subset K_1 \subset \ldots \subset K_n$$

von $\mathbb{R}$ mit $x \in K_n$ und $[K_j : K_{j-1}] = 2$ für $j = 1, \ldots, n$ (falls $n > 0$).

Beweis. a) $\Rightarrow$ b): 1. Wir zeigen: Ist U ein Teilkörper von $\mathbb{R}$ und wird ein Punkt $(x, y) \in \mathbb{R}^2$ durch einen der drei Konstruktionsschritte aus D. 9.1 aus Punkten erzeugt, deren Koordinaten in U liegen, so gilt $x, y \in U[\sqrt{\delta}]$ für ein $\delta \in U$.

Denn: Geraden durch 2 Punkte mit Koordinaten U sind gegeben durch Gleichungen der Form

$$ax + by + c = 0, \tag{9.1}$$

wobei $a, b, c \in U$ (Normalenform). Der Schnittpunkt zweier solcher Geraden hat dann wieder Koordinaten $x, y \in U$ als Lösung eines (2×2)-Gleichungssystems mit Koeffizientenmatrix in $GL_2(U)$ und rechter Seite in $U \times U$.
Entsprechend sind Gleichungen von Kreisen, bei denen der Mittelpunkt und ein Randpunkt Koordinaten in U haben, von der Form

$$x^2 + y^2 + dx + ey + f = 0 \tag{9.2}$$

mit gewissen $d, e, f \in U$.
(Denn: Ist $C = (u, v)$ der Mittelpunkt und $D = (w, z)$ ein Randpunkt, so hat die Kreisgleichung die Form

$$(x - u)^2 + (y - v)^2 = (w - u)^2 + (z - v)^2.$$

Durch Ausmultiplizieren ergibt sich obige Form.)
Damit sieht man: Die Schnittpunkte einer Geraden mit einem Kreis ergeben sich durch Auflösen von (9.1) etwa nach y und Einsetzen in (9.2). Die dann resultierende quadratische Gleichung für x hat eine Diskriminante $\delta \in U$ (mit $\delta \geq 0$, falls Schnittpunkte existieren). Damit ist $x \in U[\sqrt{\delta}]$ und mit (9.1) auch y.
Schließlich lässt sich der Fall von Schnittpunkten zweier Kreise wie oben durch Subtraktion der beiden Kreisgleichungen auf den Fall ,,Kreis und Gerade" zurückführen.
In allen Fällen ist also $x, y \in U[\sqrt{\delta}]$ für ein $\delta \in U$.
2. Es gilt $U = U[\sqrt{\delta}]$ (falls $\sqrt{\delta} \in U$) oder $[U[\sqrt{\delta}] : U] = 2$ (falls $\sqrt{\delta} \notin U$).
Denn: Der erste Fall ist klar. Ist $\sqrt{\delta} \notin U$, so ist $U[\sqrt{\delta}]$ nach S. 8.10 ein Körper. Dabei ist $X^2 - \delta \in U[X]$ das Minimalpolynom von $\sqrt{\delta}$, also $[U[\sqrt{\delta}] : U] = 2$ nach B. 8.11.
3. Durch sukzessive Anwendung von 1. und 2. (startend mit $U = K$) ergibt sich für $x \in \mathrm{kon}(K)$ die Eigenschaft aus b).

b) $\Rightarrow$ a): Es reicht zu zeigen: Für alle $j \in \{1, \ldots, n\}$ ist

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

Aus $[K_j : K_{j-1}] = 2$ folgt mit S. 9.5 die Existenz eines $a \in K_j \setminus K_{j-1}$ mit $a^2 \in K_{j-1}$ und $K_j = \mathrm{span}(1, a) = K_{j-1} + K_{j-1}a$. Nach S. 9.3 ist dann $a(= \pm\sqrt{a^2}) \in \mathrm{kon}(K_{j-1})$ $(\{1, 0\} \subset K_{j-1})$. Da $K_j = \mathrm{span}(1, a)$ ist, folgt $K_j \subset \mathrm{kon}(K_{j-1})$ wieder aus S. 9.3. $\square$

Der folgende Satz liefert die für das Weitere zentrale Einschränkung an konstruierbare Zahlen.

Satz 9.7 *Es sei K ein Teilkörper von $\mathbb{R}$. Ist $x \in \mathrm{kon}(K)$, so ist x algebraisch über K vom Grad 2^m für ein $m \in \mathbb{N}_0$.*

Beweis. Es seien $K = K_0 \subset \ldots \subset K_n$ wie in S. 9.6 mit $x \in K_n$. Dann gilt nach S. 8.3 (induktiv angewandt)

$$[K_n : K] = \prod_{j=1}^{n} [K_j : K_{j-1}] = 2^n$$

(mit $\prod_{\emptyset} := 1$). Weiter ist mit B. 8.11 $[K[x] : K]$ Teiler von $[K_n : K]$, also $[K[x] : K] = 2^m$ für ein $m \in \mathbb{N}_0$. □

Um den vorhergehenden Satz auf verschiedene klassische Probleme der (Nicht-)Konstruierbarkeit anwenden zu können, benötigen wir noch einige einfache Aussagen über Polynome.

Bemerkung 9.8 Es sei K ein Körper.
1. Hat $P \in K[X]$ eine Wurzel $a \in K$, so ist $P = (X - a)Q$ mit einem $Q \in K[X]$ nach B. 7.10. Also ist P in Falle $\deg P \geq 2$ reduzibel.
2. Ist $P \in K[X]$ ein Polynom vom Grad 2 oder 3 und ist P reduzibel, so hat P eine Wurzel in K.
(Denn: Ist P reduzibel, so ist $P = QR$ mit $Q, R \in K[X]$ nicht konstant. Also ist $\deg Q = 1$ oder $\deg R = 1$. Damit hat Q oder R (und folglich P) eine Wurzel in K.)
3. Es sei $P \in \mathbb{Z}[X]$ normiert, also P ein Polynom mit ganzzahligen Koeffizienten und führenden Koeffizienten 1. Dann gilt ([Ü]): Ist x eine rationale Wurzel von P, so ist schon x ganzzahlig (oder, mit anderen Worten, ist $x \in \mathbb{R} \setminus \mathbb{Z}$ eine Wurzel von P, so ist x irrational). Insbesondere ergibt sich daraus ([Ü]): Sind $a, n \in \mathbb{N}$, so ist entweder $\sqrt[n]{a} \in \mathbb{N}$ oder $\sqrt[n]{a} \notin \mathbb{Q}$.

Satz 9.9 *Ist $a \in \mathbb{N}$, so ist entweder $\sqrt[3]{a} \in \mathbb{N}$ oder $\sqrt[3]{a}$ von Grad 3 über $\mathbb{Q}$.*

Beweis. Da $\sqrt[3]{a}$ Wurzel von $X^3 - a$ ist, ist der Grad ≤ 3. Es sei $\sqrt[3]{a} \notin \mathbb{N}$. Nach B. 8.8.2 reicht es, zu zeigen: $X^3 - a \in \mathbb{Z}[X] \subset \mathbb{Q}[X]$ ist irreduzibel (in $\mathbb{Q}[X]$). Angenommen, nicht. Dann hat $X^3 - a$ nach B. 9.8.2. eine Wurzel in $\mathbb{Q}$ und damit nach B. 9.8.3 in $\mathbb{Z}$. Die einzige reelle Wurzel ist aber $\sqrt[3]{a}$. □

Beispiel 9.10 (Delisches Problem; Würfelverdopplung)
$\sqrt[3]{2}$ ist nicht konstruierbar aus $\mathbb{Q}$.
(Denn. Nach S. 9.7 reicht es zu zeigen, dass der Grad von $\sqrt[3]{2}$ über $\mathbb{Q}$ keine Zweierpotenz ist. Nach S. 9.9 ist der Grad 3, also keine Zweierpotenz.)

Wir untersuchen das Problem der Winkeldreiteilung, also die Frage, ob der Punkt $\big(\cos(\alpha/3), \sin(\alpha/3)\big)$ konstruierbar ist aus $S = \big\{(0,0), (1,0), (\cos\alpha, \sin\alpha)\big\}$. Aus den Überlegungen in B. 9.2, S. 9.3 und B. 9.4 ergibt sich, dass dies äquivalent ist zu

$$\cos(\alpha/3) \in \operatorname{kon}\big(\mathbb{Q}(\cos\alpha)\big)$$

(Wichtig dabei: es gilt $\sin^2\alpha = 1 - \cos^2\alpha$, also ist $\sin\alpha \in \operatorname{kon}\big(\mathbb{Q}(\cos\alpha)\big)$ nach S. 9.3.)

Satz 9.11 *Es sei $\alpha \in \mathbb{R}$. Dann sind äquivalent*

a) $\cos(\alpha/3) \in \operatorname{kon}\big(\mathbb{Q}(\cos\alpha)\big)$;

b) $P = X^3 - 3X - 2\cos\alpha$ *hat eine Wurzel in* $\mathbb{Q}(\cos\alpha)$.

Beweis. Wir setzen $K := \mathbb{Q}(\cos\alpha)$.
Für beliebige $\varphi \in \mathbb{R}$ gilt

$$\cos(3\varphi) = 4\cos^3\varphi - 3\cos\varphi,$$

also

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

Folglich ist $2\cos(\alpha/3)$ Wurzel von

$$P = X^3 - 3X - 2\cos\alpha \in K[X]$$

und damit $2\cos(\alpha/3)$ (also auch $\cos(\alpha/3)$) vom Grad ≤ 3 über K. Aus S. 9.6 und S. 9.7 folgt, dass $\cos(\alpha/3)$ genau dann konstruierbar aus K ist, wenn der Grad 1 oder 2 ist. Nach B. 8.8.2 ist dies genau dann der Fall, wenn $P \in K[X]$ reduzibel ist. Mit B. 9.8.1./2. ergibt sich, dass dies wiederum äquivalent dazu ist, dass P eine Wurzel in K hat. □

Beispiel 9.12 Es sei $\alpha = \pi/3$. Dann ist $\cos(\alpha) = 1/2$, also ist $P = X^3 - 3X - 1$ in S. 9.11. Wir zeigen

$$\cos(\pi/9) = \cos(\alpha/3) \notin \text{kon}\big(\mathbb{Q}(\cos\alpha)\big),$$

d. h., die Dreiteilung des Winkels $\pi/3 = 60^o$ ist nicht möglich.
Denn: $P = X^3 - 3X - 1 \in \mathbb{Z}[X]$. Also hat P nach B. 9.8.3 nur dann eine Wurzel in $\mathbb{Q}(\cos\alpha) = \mathbb{Q}(1/2) = \mathbb{Q}$, wenn eine Wurzel in $\mathbb{Z}$ existiert. Wir betrachten die Polynomfunktion $f : \mathbb{R} \to \mathbb{R}$ mit $f(x) := P(x) = x^3 - 3x - 1$. Aus

$$f'(x) = 3(x^2 - 1) \begin{cases} > 0 & \text{für } |x| > 1 \\ < 0 & \text{für } |x| < 1 \end{cases}$$

folgt

$$f \begin{cases} \nearrow & \text{in } (-\infty, -1) \\ \searrow & \text{in } (-1, 1) \\ \nearrow & \text{in } (1, \infty) \end{cases} .$$

Da $f(-2) = -3$, $f(-1) = 1$, $f(0) = -1$, $f(1) = -3$, $f(2) = 1$ gilt, hat P keine Wurzel in $\mathbb{Z}$.

Das bekannteste (Nicht-)Konstruierbarkeitsproblem ist die Quadratur des Kreises, also die Frage, ob aus einem gegebenen Kreis ein flächengleiches Rechteck konstruiert werden kann. Das Problem reduziert sich auf die Frage, ob

$$\sqrt{\pi} \in \text{kon}\big(\{0, 1\}\big) = \text{kon}(\mathbb{Q})$$

gilt. F. Lindemann bewies 1882, dass $\sqrt{\pi}$ (bzw. π) transzendent (über $\mathbb{Q}$) ist. Nach S. 9.7 ist damit $\sqrt{\pi}$ nicht konstruierbar aus $\mathbb{Q}$.

10 Spezielle irrationale und transzendente Zahlen

Im letzten Abschnitt haben wir bemerkt, dass die Unmöglichkeit der Quadratur des Kreises eine Folge der Transzendenz von π ist. Wir werden zumindest die Irrationalität von π nachweisen.

Satz 10.1 *1. Für alle $a \in \mathbb{N}$ ist $e^a \notin \mathbb{Q}$.*

2. $\pi^2 \notin \mathbb{Q}$.

Beweis. 1. Es sei $m \in \mathbb{N}$. Für die Polynomfunktion $f_m : \mathbb{R} \to \mathbb{R}$, $f_m(x) = x^m(1-x)^m$ gilt

$$f_m^{(k)}(0),\ f_m^{(k)}(1) \in (m!)\mathbb{Z} \qquad (k \in \mathbb{N}_0).$$

(Denn: Aus $X^m(1-X)^m = \sum_{k=m}^{2m} c_k X^k \in \mathbb{Z}[X]$ folgt

$$f_m^{(k)}(0) = \left\{ \begin{array}{ll} 0, & \text{falls } k < m \text{ oder } k > 2m \\ k!c_k, & \text{falls } m \le k \le 2m \end{array} \right\} \in (m!)\mathbb{Z}$$

und aus Symmetriegründen gilt auch $f_m^{(k)}(1) \in (m!)\mathbb{Z}$.)
Angenommen, $e^a = p/q$ mit $p, q \in \mathbb{N}$. Wir betrachten

$$F_m(x) := \sum_{k=0}^{2m} (-1)^k a^{2m-k} f_m^{(k)}(x) \qquad (x \in \mathbb{R}).$$

Dann ist $F_m(0), F_m(1) \in (m!)\mathbb{Z}$ und (da $f_m^{(2m+1)} = 0$)

$$\begin{aligned} F_m'(x) &= \sum_{k=0}^{2m} (-1)^k a^{2m-k} f_m^{(k+1)}(x) = (-a) \sum_{k=1}^{2m} (-1)^k a^{2m-k} f_m^{(k)}(x) \\ &= -aF_m(x) + a^{2m+1} f_m(x) \end{aligned}$$

und damit

$$\big(e^{ax} F_m(x)\big)' = e^{ax}\big(aF_m(x) + F_m'(x)\big) = e^{ax} a^{2m+1} f_m(x).$$

Also ist einerseits (da $f_m(x) > 0$ für $x \in (0,1)$)

$$\begin{aligned} 0 < q \int_0^1 e^{ax} a^{2m+1} f_m(x)dx &= qe^{ax} F_m(x)\big|_0^1 = \\ &= qe^a F_m(1) - qF_m(0) = pF_m(1) - qF_m(0) \in (m!)\mathbb{Z} \end{aligned}$$

und andererseits (da $f_m(x) < 1$ für $x \in [0,1]$)

$$q \int_0^1 e^{ax} a^{2m+1} f_m(x) dx \leq q e^a a^{2m+1} < m!$$

für m genügend groß. Widerspruch!
2. Angenommen, $\pi^2 = p/q$ mit $p, q \in \mathbb{N}$. Wir betrachten

$$G_m(x) := q^m \sum_{k=0}^{m} (-1)^k \pi^{2m-2k} f_m^{(2k)}(x) \qquad (x \in \mathbb{R}).$$

Dann gilt $G_m(0), G_m(1) \in (m!)\mathbb{Z}$ (beachte: $q^m \pi^{2(m-k)} = q^k p^{m-k}$) und

$$\begin{aligned} &\big(G_m'(x)\sin(\pi x) - \pi G_m(x)\cos(\pi x)\big)' = \\ &\quad = G_m''(x)\sin(\pi x) + \pi^2 G_m(x)\sin(\pi x) \\ &\quad = \sin(\pi x)\big(q^m \pi^{2m+2} f_m(x)\big) = p^m \pi^2 \sin(\pi x) f_m(x). \end{aligned}$$

Also ist einerseits

$$\begin{aligned} 0 < \pi p^m \int_0^1 \sin(\pi x) f_m(x) dx &= \Big(G_m'(x)\,\frac{\sin(\pi x)}{\pi} - G_m(x)\cos(\pi x)\Big)\Big|_0^1 \\ &= G_m(1) + G_m(0) \in (m!)\mathbb{Z} \end{aligned}$$

und andererseits

$$\pi p^m \int_0^1 \sin(\pi x) f_m(x) dx < \pi p^m < m!$$

für m genügend groß. Widerspruch! □

Bemerkung 10.2 Aus S. 10.1.1 folgt leicht, dass e^x irrational ist für alle $0 \neq x \in \mathbb{Q}$.

Satz 10.3 *e ist transzendent.*

Beweis. Angenommen, e ist algebraisch (vom Grad n). Dann existiert ein $c \in \mathbb{Z}$, $c \neq 0$ so, dass $P = \sum_{j=0}^{n} a_j X^j = cP_e \in \mathbb{Z}[X]$, wobei P_e das Minimalpolynoms P_e von e bzgl. $\mathbb{Q}$ bezeichnet. Da P_e (und damit auch P) irreduzibel über $\mathbb{Q}$ ist, gilt $a_0 \neq 0$.

Für $p \in \mathbb{P}$ sei $f_p : \mathbb{R} \to \mathbb{R}$ definiert durch

$$f_p(x) := x^{p-1}(x-1)^p \dots (x-n)^p \qquad (x \in \mathbb{R}).$$

Dann gilt

$$f_p^{(k)}(0) \begin{cases} = (p-1)!(-1)^p \dots (-n)^p, & \text{falls } k = p-1 \\ \in (p!)\mathbb{Z}, & \text{sonst} \end{cases}$$

und

$$f_p^{(k)}(j) \in (p!)\mathbb{Z} \qquad \text{für alle } k \in \mathbb{N}_0, j \in \{1, \dots, n\}.$$

(Denn: $X^{p-1}(X-1)^p \dots (X-n)^p = \sum\limits_{j=p-1}^{np+p-1} c_j X^j \in \mathbb{Z}[X]$ mit $c_{p-1} = (-1)^p \cdots (-n)^p$.
Also ist ($\to$ Analysis, Potenzreihenentwicklung)

$$f_p^{(k)}(0) = \begin{cases} (p-1)!c_{p-1}, & \text{falls } k = p-1 \\ 0, & \text{falls } k < p-1 \text{ oder } k > np+p-1 \\ k!c_k \in (p!)\mathbb{Z}, & \text{sonst} \end{cases}.$$

Mit einer entsprechenden Überlegung (Potenzreihenentwicklung mit Entwicklungsmitte ν) ergibt sich $f_p^{(k)}(\nu) \in (p!)\mathbb{Z}$ für $\nu = 1, \dots, n$.
Wir setzen

$$F_p(x) := \sum_{k=0}^{np+p-1} f_p^{(k)}(x) \qquad (x \in \mathbb{R}).$$

Dann gilt (da $f_p^{(np+p)} \equiv 0$)

$$\big(e^{-x}F_p(x)\big)' = e^{-x}\big(F_p'(x) - F_p(x)\big) = -e^{-x}f_p(x) \qquad (x \in \mathbb{R}),$$

also für $j = 1, \dots, n$

$$-\int_0^j e^{-x}f_p(x)dx = e^{-x}F_p(x)\big|_0^j = e^{-j}F_p(j) - F_p(0).$$

Folglich ist (da p Teiler von $F_p(j)$ für $j = 1, \dots, n$ und $f_p^{(k)}(0)$ für $k \neq p-1$)

$$D_p := -\sum_{j=1}^n (a_j e^j \int_0^j e^{-x}f_p(x)dx\big) = \sum_{j=1}^n a_j F_p(j) - F_p(0)\underbrace{\sum_{j=1}^n a_j e^j}_{=-a_0}$$

$$\equiv a_0 f_p^{(p-1)}(0) = a_0(p-1)!(-1)^p \cdots (-n)^p \mod p.$$

Aus $a_0 \neq 0$ folgt für $p > \max\big(n, |a_0|\big)$, dass p kein Teiler von $a_0 f_p^{(p-1)}(0)$ ist (sonst müsste p nach S. 1.6.1 einen der Faktoren teilen, was nicht der Fall ist). Damit ist insbesondere $D_p \neq 0$.
Aus $a_0, \ldots, a_n \in \mathbb{Z}$ folgt weiter $D_p \in ((p-1)!)\mathbb{Z}$, also $|D_p| \geq (p-1)!$.
Andererseits gilt (mit $\big|f_p(x)\big| \leq n^{np+p-1}$ für $0 \leq x \leq n$)

$$\begin{aligned} |D_p| &\leq \sum_{j=1}^{n} \Big(|a_j| e^j \int_0^j e^{-x} \big|f_p(x)\big| dx \Big) \\ &\leq \sum_{j=1}^{n} |a_j| e^j j \cdot n^{np+p-1} \leq e^n n^{np+p} \sum_{j=1}^{n} |a_j| < (p-1)! \end{aligned}$$

für p genügend groß. Widerspruch! □

Wir wollen zum Abschluss zeigen, dass algebraische Zahlen in gewissem Sinne schlecht durch rationale approximierbar sind. Dies führt wiederum auf die Transzendenz einer ganzen Klasse von Zahlen.

Satz 10.4 *(Liouville)*
Es sei $\alpha \in \mathbb{R}$ algebraisch vom Grad $d \geq 2$ über $\mathbb{Q}$. Dann existiert ein $c > 0$ so, dass für alle $p \in \mathbb{Z}$ und $q \in \mathbb{N}$ gilt

$$\Big|\alpha - \frac{p}{q}\Big| \geq \frac{c}{q^d}.$$

Beweis. Es sei $P = cP_\alpha \in \mathbb{Z}[X]$ mit $c \neq 0$ Vielfaches des Minimalpolynoms $P_\alpha \in \mathbb{Q}[X]$ von α. Ist $f(x) := P(x)$ $(x \in \mathbb{R})$, so folgt aus $f(\alpha) = 0$ die Existenz eines $\delta > 0$ mit $f(x) \neq 0$ in $[\alpha - \delta, \alpha + \delta] \setminus \{\alpha\}$. Wir definieren

$$M := \max_{[\alpha-\delta, \alpha+\delta]} \big|f'(x)\big|, \qquad c := \min(\delta, 1/M).$$

1. Fall: $|\alpha - p/q| \geq \delta$. Dann ist $|\alpha - p/q| \geq c \geq c/q^d$.
2. Fall: $|\alpha - p/q| < \delta$. Dann gilt nach dem Mittelwertsatz

$$\big|f(p/q)\big| = \big|f(\alpha) - f(p/q)\big| \leq M|\alpha - p/q|.$$

Aus $P \in \mathbb{Z}[X]$ folgt $f(p/q) \in (1/q^d)\mathbb{Z}$ und aus $f(p/q) \neq 0$ damit $\big|f(p/q)\big| \geq 1/q^d$. Also ist

$$|\alpha - \frac{p}{q}| \geq \frac{1}{M} \frac{1}{q^d} \geq \frac{c}{q^d}.$$

□

Bemerkung 10.5 Ist $\alpha = a/b \in \mathbb{Q}$ und $c := 1/|b|$, so gilt sogar $|\alpha - p/q| \geq c/q$ für alle $p \in \mathbb{Z}$, $q \in \mathbb{N}$ mit $\alpha \neq p/q$. In diesem Sinne sind rationale Zahlen (also algebraische vom Grad 1) besonders schlecht durch (andere) rationale approximierbar.

Satz 10.6 *Es sei (λ_n) eine Folge in $\mathbb{N}$ mit $\lambda_{n+1}/\lambda_n \to \infty$. Dann ist $\sum_{n=1}^{\infty} 1/q^{\lambda_n}$ transzendent für alle $q \in \mathbb{N}$, $q > 1$.*

Beweis. Für alle $n \in \mathbb{N}$ gilt mit $\alpha := \sum_{k=1}^{\infty} 1/q^{\lambda_k}$

$$\left|\alpha - \sum_{k=1}^{n} \frac{1}{q^{\lambda_k}}\right| \leq \sum_{k=n+1}^{\infty} \frac{1}{q^{\lambda_k}} \leq \frac{1}{q^{\lambda_{n+1}}} \sum_{\nu=0}^{\infty} \frac{1}{q^{\nu}} = \frac{q}{(q-1)q^{\lambda_{n+1}}} \leq \frac{2}{q^{\lambda_{n+1}}}.$$

Dabei ist $\sum_{k=0}^{n} 1/q^{\lambda_k} = p_n/q^{\lambda_n} \in \mathbb{Q} \setminus \{\alpha\}$. Sind $d \in \mathbb{N}, c > 0$, so ist

$$|\alpha - p_n/q^{\lambda_n}| \leq \frac{2}{(q^{\lambda_n})^{\frac{\lambda_{n+1}}{\lambda_n}}} \leq \frac{c}{(q^{\lambda_n})^d}$$

für n genügend groß. Nach S. 10.4 und B. 10.5 ist α transzendent. □

Beispiel 10.7 Für $\lambda_n = n!$ gilt $\lambda_{n+1}/\lambda_n = n + 1 \to \infty$ $(n \to \infty)$. Also ist etwa

$$\sum_{n=1}^{\infty} \frac{1}{10^{n!}} = \frac{1}{10} + \frac{1}{100} + \frac{1}{10^6} + \frac{1}{10^{24}} + \dots$$

transzendent.

A Etwas Lineare Algebra

Wir sammeln in diesem Anhang einige Grundbegriffe der Linearen Algebra.

Definition A.1 Es sei V ein K-Vektorraum. Dann heißt $U \subset V$ ein *Untervektorraum* oder *(linearer) Teilraum*, falls $(U, +_{|U\times U}, \cdot_{|K\times U})$ ein K-Vektorraum ist.
Es gilt: $\emptyset \neq U \subset V$ ist genau dann Teilraum, falls für alle $x, y \in U, \lambda \in K$ auch $x+y \in U$ und $\lambda x \in U$ gilt, d. h. $U+U \subset U$ und $K \cdot U \subset U$. (Man beachte: mit $y \in U$ ist dann auch $-y = (-1)y \in U$, also $U - U \subset U$).
Ist $M \subset V$, so heißt

$$<M> := <M>_V := \text{span } M := \text{linspan } M := \bigcap_{U \supset M \text{ Teilraum}} U$$

lineare Hülle oder *linearer Spann* von M. Außerdem heißt M dann *Erzeugendensystem* von span M. Man beachte: $<M>$ ist als Schnitt von Teilräumen wieder ein Teilraum.

Satz A.2 *Sind V ein K-Vektorraum und $M \subset V$, so ist*

$$\text{span } M = \{\sum_{x\in F} \lambda_x x : \lambda_x \in K, F \subset M \text{ endlich}\}.$$

Ist speziell $M = \{x_1, \ldots, x_n\}$, so ist auch

$$\text{span}(x_1, \ldots, x_n) := \text{span } M = \left\{ \sum_{j=1}^{n} \lambda_j x_j : \lambda_j \in K \right\} \quad \left(=: \sum_{j=1}^{n} K x_j \right).$$

Beweis. vgl. Beweis zu S. 3.5, B./D. 7.3, S. 7.5. □

Beispiel A.3 Es sei K ein Körper. Ist $S \neq \emptyset$ eine Menge, so ist

$$K^S := \{f : S \to K\}$$

mit den üblichen punktweisen Definitionen von $+$ und $\cdot$ ein K-Vektorraum (siehe B. 2.10). Ist speziell $S = \mathbb{N}_0$, so ist $K^{\mathbb{N}_0} = \left\{(a_j)_{j=0}^{\infty} : a_j \in K\right\}$ und $K^{[\mathbb{N}_0]} = K[X] =$

$\operatorname{span}\{X^j : j \in \mathbb{N}_0\}$ ein Teilraum. Damit ist der Polynomring über K auch ein K-Vektorraum und folglich auch eine K-Algebra (offensichtlich gilt $\lambda(PQ) = (\lambda P)Q = P(\lambda Q)$ für $P, Q \in K[X], \lambda \in K$.)
Weiter gilt auch: Sind $\emptyset \neq M \subset K$ und $p_k : M \to K$ mit

$$p_k(x) := x^k \qquad (x \in M,\ k \in \mathbb{N}_0)\ ,$$

so ist

$$\operatorname{span}\ \{p_j : j \in \mathbb{N}_0\} = \left\{ \sum_{j=1}^{n} a_j p_j : a_j \in K, n \in \mathbb{N} \right\}$$

(also die Menge der Polynomfunktionen auf M) ein Teilraum von K^M.

Definition A.4 Es sei V ein K-Vektorraum.
Eine Familie $(x_\alpha)_{\alpha\in I}$ in V (wobei $(x_\alpha)_{\alpha\in\emptyset} =: \emptyset$) heißt *linear unabhängig*, falls für alle $J \subset I$ endlich und alle $(\lambda_j)_{j\in J} \in K^J$ mit $\sum\limits_{j\in J} \lambda_j x_j = 0$ schon $\lambda_j = 0$ $(j \in J)$ gilt.
Sind speziell $x_1, \ldots, x_n \in V$, so heißen $x_1, \ldots, x_n$ *linear unabhängig*, falls $(x_1, \ldots, x_n)$ linear unabhängig ist. Dies ist genau dann der Fall, wenn aus $\sum\limits_{j=1}^{n} \lambda_j x_j = 0$ für $\lambda_1, \ldots, \lambda_n \in K$ schon $\lambda_1 = \ldots = \lambda_n = 0$ folgt.

Beispiele A.5 Es sei K ein Körper.
1. Die Familie $\left(X^k = \left(\delta_{jk}\right)_{j=0}^{\infty}\right)_{k\in\mathbb{N}_0}$ aus B./D. 7.6 ist linear unabhängig in $K[X]$.
2. Ist $|M| = \infty$, so ist die Familie $(p_k)_{k\in\mathbb{N}_0}$ der Monome aus B. A.3 linear unabhängig in K^M.
(Beachte: Nach B. 7.10 hat jedes Polynom in $K[X] \setminus \{0\}$ nur endlich viele Wurzeln in K. Also folgt aus

$$\sum_{j=0}^{n} a_j x^j = 0 \qquad (x \in M)$$

für $a_j \in K$ schon $a_j = 0$ $(j = 0, \ldots, n)$.)
Ist $n := |M| < \infty$, so ist $(p_k)_{k=0,\ldots,n}$ linear abhängig in K^M.
(Denn: ist $M = \{x_1, \ldots, x_n\}$ und

$$P = (X - x_1) \cdot (X - x_n) \in K[X],$$

so gilt $P = \sum\limits_{j=0}^{n} a_j X^j$ mit $a_n = 1 \neq 0$ und

$$0 = P(x) = \sum_{j=0}^{n} a_j x^j = 0 \qquad (x \in M)\ .)$$

Definition A.6 Es sei V ein K-Vektorraum. Dann heißt

$$\dim V := \dim_K(V) := \min\{n \in \mathbb{N}_0 : \exists\, M \subset V \text{ mit } |M| = n, \text{span } M = V\}$$

(wobei $\min \emptyset := \infty$ und $\text{span}(\emptyset) := \{0\}$) die *Dimension* von V.

Bemerkung A.7 Ist $\dim V < \infty$ und M ein minimales Erzeugendensystem von V, d. h. $M \subset V$ mit $|M| = \dim V$ und span $M = V$, so ist $(x)_{x\in M}$ linear unabhängig.
(Denn: Im Fall $\dim V = 0$ ist $(x)_{x\in\emptyset}$ linear unabhängig.
Es seien also $\dim V > 0$ und $\lambda_x \in K$ mit $\sum\limits_{x\in M} \lambda_x x = 0$. Angenommen, $\lambda_y \neq 0$ für ein $y \in M$. Dann ist (mit $\sum\limits_{\emptyset} := 0$)

$$y = \sum_{M\ni x\neq y} \left(-\frac{\lambda_x}{\lambda_y}\right) x,$$

also $y \in \text{span}\big(M \setminus \{y\}\big)$ (beachte: $\text{span}(\emptyset) = \{0\}$) und damit auch

$$V = \text{span } M = \text{span}\big(\text{span}\big(M \setminus \{y\}\big) = \text{span}\big(M \setminus \{y\}\big).$$

Dies widerspricht der Minimalität von $|M|$.)

Definition A.8 Es seien V ein K-Vektorraum und $B \subset V$. Dann heißt B *Basis* von V, falls span $B = V$ gilt und $(x)_{x\in B}$ linear unabhängig ist.

Bemerkung A.9 Nach B. A.7 hat jeder K-Vektorraum mit $n := \dim V < \infty$ eine Basis.
Weiter kann man zeigen ($\to$ LA):
Ist $M \subset V$ mit $(x)_{x\in M}$ linear unabhängig in V, so ist $|M| \leq n$. Außerdem gilt dann: Ist $|M| = n$, so ist M eine Basis.
Insbesondere ergibt sich daraus, dass $|B| = n$ für jede Basis von V gilt (denn: es ist $|B| \geq n$, da span $B = V$ und $|B| \leq n$, da $(x)_{x\in B}$ linear unabhängig ist).

Beispiel A.10 Es sei K ein Körper.
1. $\{e^{(k)} := (\delta_{jk})_{j=1,\ldots,n} : k = 1, \ldots, n\}$ ist eine Basis von K^n. Also ist $\dim K^n = n$.
2. $\{X^k : k \in \mathbb{N}_0\}$ ist eine Basis von $K[X]$. Damit ist $\dim K[X] = \infty$ (denn sonst könnte nach B. A.9 das Tupel $(X^k)_{k\in\mathbb{N}_0}$ nicht linear unabhängig sein).

3. Ist E ein Oberkörper von K, so kann man E auch als K-Vektorraum auffassen (indem man die Multiplikation auf $K \times E$ einschränkt). Insbesondere sind etwa $\mathbb{C}$ ein $\mathbb{R}$-Vektorraum und $\mathbb{R}$ ein $\mathbb{Q}$-Vektorraum. Dabei ist $\{1, i\}$ eine Basis des $\mathbb{R}$-Vektorraumes $\mathbb{C}$. Also ist

$$\dim_{\mathbb{R}}(\mathbb{C}) = 2.$$

Weiter ist

$$\dim_{\mathbb{Q}}(\mathbb{R}) = \infty,$$

denn ist $M \subset \mathbb{R}$ endlich, so ist $\text{span}\,(M) = \left\{ \sum_{x \in M} \lambda_x x : \lambda_x \in \mathbb{Q} \right\}$ abzählbar (da $\mathbb{Q}$ abzählbar ist). Da $\mathbb{R}$ überabzählbar ist, ist M kein Erzeugendensystem von $\mathbb{R}$. Da auch abzählbare Vereinigungen abzählbarer Mengen abzählbar sind, sieht man, dass genauer jede Basis von $\mathbb{R}$ überabzählbar sein muss.

Bemerkung und Definition A.11 Es seien V, W K-Vektorräume. Eine Abbildung $T : V \to W$ heißt *linear* (oder *(Vektorraum-)Homomorphismus*), falls für alle $x, y \in V, \lambda \in K$,

$$T(x + y) = Tx + Ty, \qquad T(\lambda x) = \lambda Tx$$

gilt (man schreibt hier auch kurz Tx statt $T(x)$).
Wie üblich werden wieder *Monomorphismen* (bzw. kurz *Einbettungen*) und *Isomorphismen* definiert. Existiert ein Isomorphismus $T : V \to W$, so heißen auch hier V, W *isomorph*. In diesem Fall gilt: $B \subset V$ ist genau dann eine Basis von V, wenn $T(B) \subset W$ eine Basis von W ist.
Schließlich ergibt sich noch (siehe LA): Ist $n := \dim V < \infty$, so sind V und W genau dann isomorph, wenn sie gleiche Dimension haben. Insbesondere ist V isomorph zu K^n.