Kapitel 6

Algebraische Strukturen

6.1 Modulare Arithmetik

Teilbarkeit und Divison mit Rest

Folie 318

Definition 6.1. Sei $x \in \mathbb{R}$.

(a) Der *Betrag* von x ist definiert als

$$|x| := \begin{cases} x & \text{falls } x \geqslant 0 \\ (-1) \cdot x & \text{falls } x < 0. \end{cases}$$

(b) Wir schreiben $\lfloor x \rfloor$ für die größte Zahl $z \in \mathbb{Z}$ mit $z \leqslant x$.

(c) Wir schreiben $\lceil x \rceil$ für die kleinste Zahl $z \in \mathbb{Z}$ mit $z \geqslant x$.

Beispiel: Für $x := 3,7$ ist $|x| = 3,7$ und $\lfloor x \rfloor = 3$ und $\lceil x \rceil = 4$.
Für $x := -7$ ist $|x| = 7$ und $\lfloor x \rfloor = -7$ und $\lceil x \rceil = -7$.

Folie 319

Definition 6.2. Sei $b \in \mathbb{Z}$.
Ein (ganzzahliger) *Teiler* von b ist eine Zahl $a \in \mathbb{Z}$ mit $a \neq 0$, so dass es ein $c \in \mathbb{Z}$ mit $a \cdot c = b$ gibt.
Wir sagen dann auch: b ist ein (ganzzahliges) *Vielfaches* von a.
Wir schreiben $a \,|\, b$ um auszudrücken, dass a ein Teiler von b ist.

Definition 6.3. Eine *Primzahl* ist eine eine Zahl $p \in \mathbb{N}$ mit $p \geqslant 2$, deren einzige Teiler die Zahlen 1 und p sind.

Folie 320

Teilbarkeitsregeln

Bemerkung 6.4. Für alle $a, b, c \in \mathbb{Z}$ gilt:

(a) Aus $a \mid b$ folgt für alle $d \in \mathbb{Z}$, dass $a \mid bd$.

(b) *Transitivität:* Aus $a \mid b$ und $b \mid c$ folgt $a \mid c$.

(c) Aus $a \mid b$ und $a \mid c$ folgt für alle $s, t \in \mathbb{Z}$, dass $a \mid (sb + tc)$.

(d) Aus $a \mid (b + c)$ und $a \mid b$ folgt $a \mid c$.

(e) Ist $c \neq 0$, so gilt: $a \mid b \iff ac \mid bc$.

(f) Aus $a \mid b$ und $b \mid a$ folgt: $a = b$ oder $a = (-1) \cdot b$.

Beweis. Dies folgt ganz leicht aus Definition 6.2. Details: Übungsaufgabe. □

Folie 321

Division mit Rest

Satz 6.5. *Seien $a, b \in \mathbb{Z}$ mit $b \neq 0$.*
Dann gibt es $q, r \in \mathbb{Z}$ mit $0 \leqslant r < |b|$ so dass $a = qb + r$.
Diese Zahlen q, r sind eindeutig bestimmt.

Die Zahl r wird der Rest von a modulo b genannt;
die Zahl q wird Ganzzahlquotient von a bzgl. b genannt.

Beweis. Sei $S := \{a - qb \ : \ q \in \mathbb{Z} \text{ so dass } (a - qb) \in \mathbb{N} \text{ ist }\}$.
Wegen $b \neq 0$ ist $S \neq \emptyset$. Sei r das *kleinste* Element in S (bzgl. der linearen Ordnung $\leqslant$ der natürlichen Zahlen).
Wegen $r \in S$ gilt: Es gibt ein $q \in \mathbb{Z}$ mit $r = a - qb$. Somit ist $a = qb + r$.

Behauptung 1: $0 \leqslant r < |b|$

Beweis: Wegen $r \in \mathbb{N}$ ist $r \geqslant 0$.
Wir führen einen Beweis durch Widerspruch und nehmen an, r wäre $\geqslant |b|$.
Dann ist $0 \leqslant r - |b| = a - qb - |b|$.
Falls $b > 0$ ist, setzen wir $\tilde{q} := q+1$ und erhalten $r - |b| = a - \tilde{q}b \in S$.
Falls $b < 0$ ist, setzen wir $\tilde{q} := q-1$ und erhalten $r - |b| = a - \tilde{q}b \in S$.

In beiden Fällen ist $\tilde{r} := r - |b| \in S$ und $\tilde{r} < r$ — was ein Widerspruch zur Minimalität von r ist. $\square_{Beh.1}$.

Somit haben wir Zahlen $q, r \in \mathbb{Z}$ mit $0 \leqslant r < |b|$ gefunden, so dass $a = qb + r$ ist.

Behauptung 2: Für alle $r', q' \in \mathbb{Z}$ mit $0 \leqslant r' < |b|$ und $a = q'b + r'$ gilt: $q' = q$ und $r' = r$.
Beweis: Es gilt: $0 = a - a = qb + r - q'b - r'$. Also ist $r - r' = q'b - qb = (q'-q)b$.
Somit ist b ein Teiler von $(r-r')$.
Außerdem gilt wegen $0 \leqslant r < |b|$ und $0 \leqslant r' < |b|$, dass $|r-r'| < |b|$. Wegen $b \,|\, (r-r')$ muss daher gelten: $r - r' = 0$.
D.h.: $r = r'$ und $qb = q'b$. Da $b \neq 0$ ist, können wir durch b teilen und erhalten: $q = q'$. $\square_{Beh.2}$

Dies beendet den Beweis von Satz 6.5 $\square$

Folie 322

Kongruenz modulo n

Definition 6.6. Sei $n \in \mathbb{N}_{\geqslant 1}$.
Zwei Zahlen $a, b \in \mathbb{Z}$ heißen *kongruent modulo* n, kurz:

$$a \equiv b \mod n$$

falls der Rest von a modulo n und der Rest von b modulo n identisch sind.

Bemerkung 6.7. Für alle $n \in \mathbb{N}_{\geqslant 1}$ und alle $a, b \in \mathbb{Z}$ gilt:

$$a \equiv b \mod n \quad \Longleftrightarrow \quad n \,|\, (a - b)\,.$$

Beweis. Seien $q, r, q', r' \in \mathbb{Z}$ mit $0 \leqslant r < n$ und $0 \leqslant r' < n$ gemäß Satz 6.5 gewählt, so dass $a = qn + r$ und $b = q'n + r'$. Es gilt:

$$\begin{aligned} a \equiv b \mod n \quad &\Longleftrightarrow \quad r = r' \quad \Longleftrightarrow \quad a-b \;=\; qn - q'n \;=\; (q-q')n \\ &\Longleftrightarrow \quad n \,|\, (a-b)\,. \end{aligned}$$

$\square$

Folie 323

Regeln zum Rechnen mit Kongruenzen

Lemma 6.8. *Sei $n \in \mathbb{N}_{\geqslant 1}$. Seien $a, b, x, y \in \mathbb{Z}$, so dass gilt:*

$$x \equiv y \mod n \qquad \text{und} \qquad a \equiv b \mod n\,.$$

Dann gilt:

(a) $x + a \equiv y + b \mod n$.

(b) $x - a \equiv y - b \mod n$.

(c) $xa \equiv yb \mod n$.

(d) Für jedes $d \in \mathbb{N}$ gilt: $x^d \equiv y^d \mod n$.

Beweis. Dies folgt leicht aus Definition 6.6 und Bemerkung 6.7. Details: Übungsaufgabe. □

Teilerfremde Zahlen und der ggT

Folie 324

Definition 6.9. Seien $a, b \in \mathbb{Z} \setminus \{0\}$.

(a) Der *größte gemeinsame Teiler* $\mathrm{ggT}(a, b)$ der Zahlen a und b ist die größte Zahl $t \in \mathbb{N}_{\geqslant 1}$, für die gilt: $t \mid a$ und $t \mid b$.

Beispiel: $\mathrm{ggT}(8, 12) = 4$, $\mathrm{ggT}(-21, 7) = 7$, $\mathrm{ggT}(8, 9) = 1$.

(b) Die Zahlen a und b heißen *teilerfremd* (oder: *relativ prim*), falls gilt: $\mathrm{ggT}(a, b) = 1$.

Folie 325

Linearkombinationen

Definition 6.10. Eine (ganzzahlige) *Linearkombination* zweier Zahlen $a, b \in \mathbb{Z}$ ist eine Zahl der Form $xa + yb$ mit $x, y \in \mathbb{Z}$.
Eine Linearkombination ist *positiv* falls sie > 0 ist.

Satz 6.11 (*Vielfachsummendarstellung des ggT, Lemma von Bézout*)**.**
Seien $a, b \in \mathbb{Z} \setminus \{0\}$.
$\mathrm{ggT}(a, b)$ ist die kleinste positive Linearkombination von a und b.
Insbesondere gibt es Zahlen $x, y \in \mathbb{Z}$ so dass $ax + by = \mathrm{ggT}(a, b)$.

Beweis. Sei $t := \text{ggT}(a,b)$.
Sei $S := \{ax + by \ : \ x, y \in \mathbb{Z},\ ax + by > 0\}$. Wegen $a, b \neq 0$ ist $S \neq \emptyset$. Sei k das kleinste Element von S und seien $x, y \in \mathbb{Z}$ so dass $k = ax + by$.
Wegen $t \,|\, a$ und $t \,|\, b$ gilt: $t \,|\, k$.
Unser Ziel ist, zu zeigen, dass $k = t$ ist.
Wegen $t \,|\, k$ und $t, k \geqslant 0$ genügt es zu zeigen, dass $k \,|\, t$; dann folgt gemäß Bemerkung 6.4(f) nämlich, dass $t = k$ ist.

Behauptung 1: $k \,|\, a$.

Beweis: Seien $q, r \in \mathbb{Z}$ mit $a = qk + r$ und $0 \leqslant r < k$. Es gilt:

$$r \ = \ a - qk \ = \ a - q(ax + by) \ = \ a(1 - qx) + b(-qy)\,.$$

Wegen $(1 - qx) \in \mathbb{Z}$ und $-qy \in \mathbb{Z}$ ist also r eine Linearkombination von a und b.
Falls $r > 0$, so ist $r \in S$. Da k das kleinste Element in S ist, ist $r \geqslant k$. *Widerspruch* zu $r < k$.
Somit ist also $r = 0$. D.h.: $a = qk$. Somit gilt: $k \,|\, a$. $\square_{\text{Beh.1}}$

Auf die gleiche Weise lässt sich Folgendes beweisen:

Behauptung 2: $k \,|\, b$.

Wegen $k \,|\, a$ und $k \,|\, b$ und $t = \text{ggT}(a,b)$ gilt: $k \,|\, t$. $\square$

Folie 326

Satz 6.12 (Euklid'scher Hilfssatz)**.** *Seien $a, b \in \mathbb{Z} \setminus \{0\}$ und sei $n \in \mathbb{N}_{\geqslant 1}$. Wenn $n \,|\, ab$ und $\text{ggT}(a,n) = 1$, dann gilt: $n \,|\, b$.*

Insbes. gilt für jede Primzahl p: Falls $p \,|\, ab$, so gilt: $p \,|\, a$ oder $p \,|\, b$.

Beweis. Gemäß Voraussetzung gilt: $n \,|\, ab$ und $\text{ggT}(a,n) = 1$.
Gemäß der Vielfachsummendarstellung des ggT gibt es $x, y \in \mathbb{Z}$ so dass $xa + yn = \text{ggT}(a,n) = 1$.
Multiplizieren mit b liefert: $bxa + byn = b$.
Wegen $n \,|\, bxa$ (da $n \,|\, ab$) und $n \,|\, byn$ gilt: $n \,|\, bxa + byn = b$.

Sei nun p eine Primzahl mit $p \,|\, ab$. Falls[1] $p \nmid a$, so gilt: $\text{ggT}(a,p) = 1$ (da p eine Primzahl ist). Gemäß des eben Gezeigten folgt für $n := p$, dass $p \,|\, b$. $\square$

Folie 327

[1] Wir schreiben $a \nmid b$ um auszudrücken, dass a *kein* Teiler von b ist, d.h. dass *nicht* gilt: $a \,|\, b$.

Einfache Folgerungen

Satz 6.13.

(a) Für $n \in \mathbb{N}_{\geqslant 1}$ und $a, b \in \mathbb{Z} \setminus \{0\}$ mit $\text{ggT}(n, a) = \text{ggT}(n, b) = 1$ gilt: $\text{ggT}(n, ab) = 1$.

(b) Sei p eine Primzahl und sei $k \in \mathbb{N}$ mit $1 \leqslant k < p$. Es gilt: $p \mid \binom{p}{k}$.

(c) Für jede Primzahl p gilt: $\sqrt{p}$ ist irrational, d.h. $\sqrt{p} \notin \mathbb{Q}$.

Beweis. (a): Sei $t := \text{ggT}(n, ab)$. Angenommen, $t \geqslant 2$. Laut Voraussetzung ist $\text{ggT}(n, a) = \text{ggT}(n, b) = 1$. Somit ist auch $\text{ggT}(t, a) = 1$. Aus $t \mid ab$ und $\text{ggT}(t, a) = 1$ folgt gemäß dem Euklid'schen Hilfssatz, dass $t \mid b$.
Widerspruch zu $\text{ggT}(n, b) = 1$.

(b): Setze $a := \binom{p}{k}$, $b := k!$ und $x := (p)_k$. Es gilt: $a = \frac{x}{b}$, d.h. $ab = x$.
Wegen $p \mid x$ (da $x = (p)_k = p \cdot (p-1) \cdots (p-k+1)$) gilt $p \mid ab$ und da p eine Primzahl ist, folgt aus dem Euklid'schen Hilfssatz: $p \mid a$ oder $p \mid b$.
Gemäß Voraussetzung ist $k < p$, und daher ist auch jeder einzelne Faktor von $b = k! = k \cdot (k-1) \cdots 1$ kleiner als p. Somit gilt: $p \nmid b$. Also gilt: $p \mid a = \binom{p}{k}$.

(c): Gemäß Voraussetzung ist p eine Primzahl. Angenommen, $\sqrt{p} \in \mathbb{Q}$. Dann können wir $\sqrt{p}$ als "gekürzten Bruch" schreiben, d.h. es gibt Zahlen $a, b \in \mathbb{Z} \setminus \{0\}$ und $\text{ggT}(a, b) = 1$, so dass $\sqrt{p} = \frac{a}{b}$.
Es gilt: $p = \frac{a^2}{b^2}$, d.h. $b^2 p = a^2$.
Also gilt: $p \mid a^2$. Aus dem Euklid'schen Hilfssatz folgt: $p \mid a$. Somit gibt es ein $x \in \mathbb{Z}$ so dass $a = px$.

Aus $a^2 = b^2 p$ und $a = px$ folgt: $p^2 x^2 = b^2 p$.
Teilen durch p liefert: $px^2 = b^2$. Somit gilt: $p \mid b^2$. Aus dem Euklid'schen Hilfssatz folgt: $p \mid b$.

Wir haben gezeigt: $p \mid a$ und $p \mid b$. Somit gilt: $\text{ggT}(a, b) \geqslant p$. *Widerspruch* zu $\text{ggT}(a, b) = 1$. □

Folie 328

Bemerkung 6.14 (Kürzungsregel)**.**
Sei $n \in \mathbb{N}_{\geqslant 1}$ und sei $a \in \mathbb{Z} \setminus \{0\}$ so dass $\text{ggT}(n, a) = 1$.
Für alle $x, y \in \mathbb{Z}$ mit $ax \equiv ay \mod n$ gilt: $x \equiv y \mod n$.

Beweis. Wegen $ax \equiv ay \mod n$ gilt: $n \,|\, (ax - ay) = a(x-y)$.
Wegen $\text{ggT}(n, a) = 1$ folgt aus dem Euklid'schen Hilfssatz: $n \,|\, x-y$. Somit gilt: $x \equiv y \mod n$. □

Folie 329

Repräsentantenmengen modulo n

Sei $n \in \mathbb{N}_{\geqslant 1}$. Für jedes $i \in \mathbb{N}$ setze

$$n\mathbb{Z} + i \quad := \quad \{nz + i \;:\; z \in \mathbb{Z}\}\,. \tag{6.1}$$

Die Menge $n\mathbb{Z} + i$ wird auch *Restklasse modulo n* genannt.
An Stelle von $n\mathbb{Z} + 0$ schreiben wir auch kurz $n\mathbb{Z}$.

Aus Satz 6.5 folgt:

$$\mathbb{Z} \quad = \quad \bigcup_{\substack{r \in \mathbb{N} \text{ mit} \\ 0 \leqslant r < n}} n\mathbb{Z} + r$$

und die Mengen $n\mathbb{Z} + r$ für $0 \leqslant r < n$ sind paarweise disjunkt.
Wir sagen auch: $(n\mathbb{Z} + r)_{0 \leqslant r < n}$ ist eine *Zerlegung* der Menge $\mathbb{Z}$.

Eine *Repräsentantenmenge modulo n* ist eine Menge $R \subseteq \mathbb{Z}$ mit $|R| = n$, so dass es für jedes $r \in \mathbb{N}$ mit $0 \leqslant r < n$ genau ein Element $x_r \in R$ gibt mit $x_r \equiv r \mod n$.

Beispiel: Für $n = 5$ sind $R := \{0, 1, 2, 3, 4\}$ und $R' := \{0, 1, -1, 2, -2\}$ Repräsentantenmengen modulo 5.

Für jedes $n \in \mathbb{N}_{\geqslant 1}$ gilt: Die Menge

$$\mathbb{Z}_n \quad := \quad \{r \in \mathbb{N} \;:\; 0 \leqslant r < n\} \tag{6.2}$$

ist eine Repräsentantenmenge modulo n.

Folie 330

Lemma 6.15. *Sei $n \in \mathbb{N}_{\geqslant 1}$, sei R eine Repräsentantenmenge modulo n und sei $a \in \mathbb{Z} \setminus \{0\}$ mit $\text{ggT}(a, n) = 1$. Dann ist auch $aR := \{ar \;:\; r \in R\}$ eine Repräsentantenmenge modulo n.*

Beweis. Wegen $|R| = n$ und $a \neq 0$ ist $|aR| = n$.

Behauptung: Für alle $X, Y \in aR$ mit $X \neq Y$ gilt: $X \not\equiv Y \mod n$.

Beweis: Wegen $X, Y \in aR$ gibt es $x, y \in R$ so dass $X = ax$ und $Y = ay$ und $x \neq y$. Da R eine Repräsentantenmenge modulo n ist, gilt: $x \not\equiv y \mod n$.

Angenommen, es würde gelten: $X \equiv Y \mod n$, also $ax \equiv ay \mod n$. Dann folgt aus der Kürzungsregel, dass $x \equiv y \mod n$. *Widerspruch.* $\square_{\text{Beh.}}$

Aus der Behauptung sowie der Tatsache, dass $|aR| = n$ ist, folgt, dass aR eine Repräsentantenmenge modulo n ist. $\square$

Folgerung 6.16. *Für jede Primzahl p und jedes $a \in \mathbb{Z} \setminus \{0\}$ ist die folgende Abbildung $f : a\mathbb{Z}_p \to \mathbb{Z}_p$ bijektiv:*

$$f(x) := r \quad \textit{wobei } r \textit{ der Rest von } x \textit{ modulo } p \textit{ ist,}$$

für alle $x \in a\mathbb{Z}_p$; und $a\mathbb{Z}_p$ ist eine Repräsentantenmenge modulo p.

Beispiel: Für $n := 5$ ist $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.
Für $a := 3$ ist $3\mathbb{Z}_5 = \{0, 3, 6, 9, 12\}$ eine Repräsentantenmenge modulo 5. Es gilt:

$$\begin{aligned} 0 &\equiv 0 \mod 5\,, \\ 3 &\equiv 3 \mod 5\,, \\ 6 &\equiv 1 \mod 5\,, \\ 9 &\equiv 4 \mod 5\,, \\ 12 &\equiv 2 \mod 5\,. \end{aligned}$$

Folie 331

Lösen einer Gleichung modulo n

Satz 6.17. *Sei $n \in \mathbb{N}_{\geqslant 1}$ und sei $a \in \mathbb{Z} \setminus \{0\}$.*

(a) Wenn $\text{ggT}(a, n) = 1$ ist, dann gilt für jedes $b \in \mathbb{Z}$: Die Gleichung

$$ax \equiv b \mod n$$

besitzt eine eindeutig bestimmte Lösung $x \in \mathbb{Z}_n$.

(b) Die Gleichung

$$ax \equiv 1 \mod n$$

besitzt genau dann eine Lösung $x \in \mathbb{Z}_n$, wenn $\text{ggT}(a, n) = 1$ ist.

Falls $\text{ggT}(a, n) = 1$ ist, so wird die (eindeutig bestimmte) Zahl $a' \in \mathbb{Z}_n$ mit $aa' \equiv 1 \mod n$ *multiplikatives Inverses von a modulo n* genannt und mit $a^{-1} \mod n$ bezeichnet.

Beweis. (a): Gemäß der Voraussetzung gilt: $\text{ggT}(a,n) = 1$.
Gemäß Lemma 6.15 ist $a\mathbb{Z}_n$ eine Repräsentantenmenge modulo n. Somit gibt es ein $B \in a\mathbb{Z}_n$ so dass $B \equiv b \mod n$. Wegen $B \in a\mathbb{Z}_n$ gibt es ein $x \in \mathbb{Z}_n = \{0, \ldots, n-1\}$ so dass $B = ax$.
Somit ist $x \in \mathbb{Z}_n$ eine Lösung der Gleichung $ax \equiv b \mod n$.

Angeonmmen, diese Gleichung besitzt eine weitere Lösung $x' \in \mathbb{Z}_n$. Dann gilt: $ax \equiv ax' \mod n$. Gemäß der Kürzungsregel gilt dann: $x \equiv x' \mod n$. Wegen $x, x' \in \mathbb{Z}_n = \{0, \ldots, n-1\}$ ist dann $x = x'$. Somit ist die Lösung eindeutig.

(b): Falls $\text{ggT}(a,n) = 1$ ist, so können wir (a) für $b := 1$ anwenden und erhalten, dass die Gleichung $ax \equiv 1 \mod n$ eine eindeutig bestimmte Lösung besitzt.

Betrachte nun den Fall, dass $\text{ggT}(a,n) \neq 1$ *ist.* Dann ist $t := \text{ggT}(a,n) \geqslant 2$.
Angenommen, es gäbe ein $x \in \mathbb{Z}_n$, so dass $ax \equiv 1 \mod n$. Dann gilt: $n \mid ax-1$. Und wegen $t \mid n$ gilt dann auch: $t \mid ax-1$.
Wegen $t \mid a$ folgt dann gemäß Bemerkung 6.4(d): $t \mid -1$. Aber dann muss gelten: $t = 1$. *Widerspruch.* □

Folie 332

Beispiel 6.18. Löse die Gleichung

$$2x \equiv 3 \mod 7\,.$$

Wir nutzen Satz 6.17 für $n = 7$ und $a = 2$.
Wegen $\text{ggT}(n,a) = 1$ erhalten wir, dass die Gleichung eine eindeutige Lösung $x \in \mathbb{Z}_7$ besitzt.
Zum Finden der Lösung betrachten wir die folgende Tabelle:

$x \in \mathbb{Z}_7$	$2x$	Rest von $2x$ modulo 7
0	0	0
1	2	2
2	4	4
3	6	6
4	8	1
5	10	3
6	12	5

Somit löst $x := 5$ die Gleichung $2x \equiv 3 \mod 7$.

Euklidischer Algorithmus

Folie 333

Effizientes Berechnen von ggT(a, b)

Um bei gegebenen Zahlen $a, b \in \mathbb{N}_{\geqslant 1}$ den größten gemeinsamen Teiler $\mathrm{ggT}(a, b)$ zu berechnen, kann man das folgende Verfahren verwenden.

Euklidischer Algorithmus
Eingabe: $a, b \in \mathbb{N}$ mit $a > b \geqslant 1$.
Ausgabe: $\mathrm{ggT}(a, b)$

1. Sei $x := a$, sei $y := b$ und sei r der Rest von x modulo y.
2. Falls $r = 0$, so STOPP mit Ausgabe y.
3. Falls $r \neq 0$, so setze $x := y$, $y := r$ und sei r der Rest von x modulo y.
4. Mach weiter in Zeile 2.

Die Korrektheit des Algorithmus (also die Tatsache, dass die vom Algorithmus ausgegebene Zahl tatsächlich $\mathrm{ggT}(a, b)$ ist), folgt aus den beiden folgenden Fakten:

- Wenn $y \mid x$, so ist $\mathrm{ggT}(x, y) = y$.
- Wenn $x = qy + r$ für ein $q \in \mathbb{Z}$, so ist $\mathrm{ggT}(x, y) = \mathrm{ggT}(y, r)$.

  Beweis: Sei $t := \mathrm{ggT}(x, y)$ und $t' := \mathrm{ggT}(y, r)$.

  Wegen $t \mid x$ und $t \mid y$ und $x = qy + r$ folgt: $t \mid r$.

  Somit gilt: $t \mid y$ und $t \mid r$. Also: $t \mid \mathrm{ggT}(y, r) = t'$.

  Andererseits gilt wegen $t' \mid y$ und $t' \mid r$ und $x = qy + r$ auch: $t' \mid x$.
  Somit gilt: $t' \mid x$ und $t' \mid y$. Also: $t' \mid \mathrm{ggT}(x, y) = t$.

  Wir haben gezeigt: $t \mid t'$ und $t' \mid t$. Wegen $t, t' \geqslant 1$ folgt: $t = t'$. □

Folie 334

Beispiel 6.19. Wir wenden den Euklisischen Algorithmus an, um Folgendes zu berechnen:

(a) $\mathrm{ggT}(348, 124)$.

$$\begin{array}{rcll} 348 & = & 2 \cdot 124 + 100 & \text{also: } x = 348,\ y = 124,\ r = 100 \\ 124 & = & 1 \cdot 100 + 24 & \text{also: } x = 124,\ y = 100,\ r = 24 \\ 100 & = & 4 \cdot 24 + 4 & \text{also: } x = 100,\ y = 24,\ r = 4 \\ 24 & = & 6 \cdot 4 + 0 & \text{also: } x = 24,\ y = 4,\ r = 0 \end{array}$$

Dies liefert die Ausgabe 4, d.h.: $\mathrm{ggT}(348, 124) = 4$.

(b) $\mathrm{ggT}(4864, 3458)$.

$$\begin{array}{rcll} 4864 & = & 1 \cdot 3458 + 1406 & \text{also: } x = 4864,\ y = 3458,\ r = 1406 \\ 3458 & = & 2 \cdot 1406 + 646 & \text{also: } x = 3458,\ y = 1406,\ r = 646 \\ 1406 & = & 2 \cdot 646 + 114 & \text{also: } x = 1406,\ y = 646,\ r = 114 \\ 646 & = & 5 \cdot 114 + 76 & \text{also: } x = 646,\ y = 114,\ r = 76 \\ 114 & = & 1 \cdot 76 + 38 & \text{also: } x = 114,\ y = 76,\ r = 38 \\ 76 & = & 2 \cdot 38 + 0 & \text{also: } x = 76,\ y = 38,\ r = 0 \end{array}$$

Dies liefert die Ausgabe 38, d.h.: $\mathrm{ggT}(4864, 3458) = 38$.

Primzahlen

Folie 335

Satz 6.20 (*Fundamentalsatz der Arithmetik*)**.**
Für jede Zahl $n \in \mathbb{N}$ mit $n \geqslant 2$ gibt es eine eindeutige Primfaktorzerlegung, d.h. es gibt eindeutig bestimmte Zahlen $k \in \mathbb{N}_{\geqslant 1}$, Primzahlen $p_1 < \cdots < p_k$ und Zahlen $s_1, \ldots, s_k \in \mathbb{N}_{\geqslant 1}$ so dass

$$n \quad = \quad p_1^{s_1} \cdots p_k^{s_k} \,.$$

Beweis.

Schritt 1: Zunächst beweisen wir per Induktion nach n, dass jedes $n \in \mathbb{N}$ mit $n \geqslant 2$ eine Primfaktorzerlegung besitzt.

Induktionsanfang: $n = 2$.
Wir wählen $k = 1$, $p_1 = 2$ und $s_1 = 1$. Es gilt: $n = 2 = p_1^{s_1}$.

Induktionsschritt: $n \to n{+}1$. Sei $n \geqslant 2$ beliebig.

Induktionsannahme: Jedes $n' \in \mathbb{N}$ mit $2 \leqslant n' \leqslant n$ besitzt eine Primfaktorzerlegung.

Behauptung: $n{+}1$ besitzt eine Primfaktorzerlegung.

Beweis: Falls $n{+}1$ eine Primzahl ist, so wählen wir $k = 1$, $p_1 = n{+}1$ und $s_1 = 1$ und sind fertig, da $n{+}1 = p_1^{s_1}$ ist.
Falls $n{+}1$ keine Primzahl ist, so gibt es Zahlen $a, b \in \mathbb{N}$ mit $a, b \geqslant 2$ so dass $n{+}1 = ab$ ist. Insbesondere gilt dann: $a, b < n{+}1$.
Gemäß der Induktionsannahme besitzt jede der Zahlen a und b eine Primfaktorzerlegung. Daraus erhalten wir eine Primfaktorzerlegung des Produkts ab, also der Zahl $n{+}1$. $\square_{\text{Schritt 1}}$

Schritt 2: Sein nun $n \in \mathbb{N}$ mit $n \geqslant 2$ beliebig gewählt. Gemäß Schritt 1 besitzt n eine Primfaktorzerlegung, d.h. es gibt eine Zahl $k \in \mathbb{N}_{\geqslant 1}$, Primzahlen $p_1 < \cdots < p_k$ und Zahlen $s_1, \ldots, s_k \in \mathbb{N}_{\geqslant 1}$ so dass $n = p_1^{s_1} \cdots p_k^{s_k}$.
Angenommen es gäbe eine weitere Primfaktorzerlegung von n, d.h. eine Zahl $\ell \in \mathbb{N}_{\geqslant 1}$, Primzahlen $q_1 < \cdots < q_\ell$ und Zahlen $t_1, \ldots, t_\ell \in \mathbb{N}_{\geqslant 1}$ so dass $n = q_1^{t_1} \cdots q_\ell^{t_\ell}$ ist.
O.B.d.A. betrachten wir den Fall, dass $k \leqslant \ell$ ist.

Per Induktion nach j kann man für alle $j \in [k]$ zeigen, dass $p_j = q_j$ und $s_j = t_j$ gilt. *Details: Übungsaufgabe.*

Dann gilt also:

$$1 \;=\; \frac{n}{n} \;=\; \frac{q_1^{t_1} \cdots q_\ell^{t_\ell}}{p_1^{s_1} \cdots p_k^{s_k}} \;=\; \prod_{i=k+1}^{\ell} q_i^{t_i},$$

und daher muss gelten: $k = \ell$. Somit ist die Primfaktorzerlegung eindeutig. $\square$

Folie 336

Satz 6.21 (*Kleiner Satz von Fermat*)**.**
Für jede Primzahl p und jedes $a \in \mathbb{N}$ gilt:

$$a^p \;\equiv\; a \mod p\,.$$

Falls $p \nmid a$, so gilt insbesondere:

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

Beweis. Wir führen den Beweis per Induktion nach a.

Induktionsanfang: $a = 0$.
Offensichtlicherweise gilt: $0^0 = 0 \equiv 0 \mod p$.

Induktionsschritt: $a \to a{+}1$.

Induktionsannahme: $a^p \equiv a \mod p$.
Behauptung: $(a{+}1)^p \equiv a{+}1 \mod p$.
Beweis: Wir nutzen die binomische Formel:

$$(a{+}1)^p \;=\; \sum_{k=0}^{p} \tbinom{p}{k} \cdot a^k \cdot 1^{p-k} \;=\; \tbinom{p}{0} \cdot a^0 \;+\; \tbinom{p}{p} \cdot a^p \;+\; \sum_{k=1}^{p-1} \tbinom{p}{k} \cdot a^k \,.$$

Gemäß Satz 6.13(b) gilt $p \mid \binom{p}{k}$ für alle k mit $1 \leqslant k < p$.
Somit gilt: $\sum_{k=1}^{p-1} \binom{p}{k} \cdot a^k \equiv 0 \mod p$.
Außerdem gilt: $\binom{p}{0} = 1 = \binom{p}{p}$ und $a^0 = 1$.
Somit gilt:

$$(a{+}1)^p \;\equiv\; 1 + a^p \mod p\,.$$

Gemäß der Induktionsannahme ist $a^p \equiv a \mod p$. Daher gilt:
$1 + a^p \equiv 1 + a \mod p$. Somit erhalten wir: $(a{+}1)^p \equiv a{+}1 \mod p$.
Dies beendet den Induktionsbeweis.

Für denn Fall, dass $p \nmid a$ gilt, müssen wir noch zeigen, dass $a^{p-1} \equiv 1 \mod p$ ist. Gemäß dem gerade bereits Gezeigten gilt: $a^p \equiv a \mod p$.
Wegen $p \nmid a$ und da p eine Primzahl ist, gilt: $\mathrm{ggT}(p, a) = 1$. Wir wenden die Kürzungsregel (Bemerkung 6.14) an für $x := a^{p-1}$ und $y := 1$. Wegen $a^p \equiv a \mod p$ gilt also: $ax \equiv ay \mod p$. Die Kürzungsregel liefert:
$x \equiv y \mod p$, d.h. $a^{p-1} \equiv 1 \mod p$. □

Der Chinesische Restsatz

Folie 337

Satz 6.22 (*Chinesischer Restsatz*)**.**
Sei $k \in \mathbb{N}_{\geqslant 1}$, seien $m_1, \ldots, m_k \in \mathbb{N}_{\geqslant 1}$ mit $\mathrm{ggT}(m_i, m_j) = 1$ für alle $i, j \in [k]$ mit $i \neq j$, und sei $n := \prod_{i=1}^{k} m_i$.
Seien $a_1, \ldots, a_k \in \mathbb{Z}$ beliebig. Es gibt ein eindeutig bestimmtes $x \in \mathbb{Z}_n$ so dass

$$x \;\equiv\; a_i \mod m_i \quad \textit{für alle } i \in [k].$$

Beweis. Für jedes $i \in [k]$ setze $n_i := \frac{n}{m_i}$; d.h.: $n = m_i \cdot n_i$.
Aus der Voraussetzung folgt: $\text{ggT}(m_i, n_i) = 1$. Wir wenden Satz 6.17(b) an (für $a := n_i$, $n := m_i$) und erhalten das *multiplikative Inverse* n_i^{-1} von n_i *modulo* m_i, d.h. es gilt: $n_i^{-1} \in \mathbb{Z}_{m_i}$ und $n_i \cdot n_i^{-1} \equiv 1 \mod m_i$.
Wir setzen

$$X \;:=\; \sum_{i=1}^{k} a_i n_i n_i^{-1} \,.$$

Behauptung: Für alle $i \in [k]$ gilt: $X \equiv a_i \mod m_i$.

Beweis: Betrachte ein beliebiges $i \in [k]$.
Wegen $m_i \,|\, n_j$ für alle $j \in [k] \setminus \{i\}$ gilt: $X \equiv a_i n_i n_i^{-1} \mod m_i$.
Da n_i^{-1} das multiplikative Inverse von n_i modulo m_i ist, folgt:
$X \equiv a_i \mod m_i$. $\square_{\text{Beh.}}$

Wir wählen nun $x \in \mathbb{Z}_n$ so dass $x \equiv X \mod n$. Wegen $m_i \,|\, n$ folgt aus der obigen Behauptung, dass $x \equiv a_i \mod m_i$ gilt (für alle $i \in [k]$).

Wir müssen nur noch zeigen, dass dieses x eindeutig bestimmt ist.
Angenommen, es gibt ein weiteres $x' \in \mathbb{Z}_n$ so dass $x' \equiv a_i \mod m_i$ für alle $i \in [k]$ gilt.
Dann gilt für alle $i \in [k]$: $x - x' \equiv a_i - a_i \mod m_i$, d.h. $x - x' \equiv 0 \mod m_i$, also gilt: $m_i \,|\, (x - x')$.
Da die Zahlen $m_1, \ldots, m_k$ paarweise teilerfremd sind und $n = \prod_{i=1}^{k} m_i$ ist, folgt aus dem Fundamentalsatz der Arithmetik (Satz 6.20): $n \,|\, (x - x')$, d.h. $x \equiv x' \mod n$. Wegen $x, x' \in \mathbb{Z}_n = \{0, \ldots, n-1\}$ muss dann gelten:
$x = x'$. $\square$

Folie 338

Anwendung des Chinesischen Restsatzes

Der Chinesische Restsatz ermöglicht es, eine große Zahl durch mehrere kleinere Zahlen eindeutig zu repräsentieren.

Seien p_1 und p_2 zwei große Primzahlen mit $p_1 \neq p_2$. Sei $n := p_1 \cdot p_2$.
Eine Zahl $z \in \mathbb{N}$ mit $0 \leqslant z < n$ können wir durch das Tupel (a_1, a_2) repräsentieren, wobei a_i der Rest von z modulo p_i sei, für jedes $i \in [2]$.

Es gilt nämlich für $x := z$, dass $x \equiv a_i \mod p_i$ für jedes $i \in [2]$; und gemäß der Aussage des Chinesichen Restsatzes gibt es kein weiteres $x \neq z$ mit $x \in \mathbb{Z}_n$ und $x \equiv a_i \mod p_i$ für jedes $i \in [2]$.

Dieses Prinzip wird im folgenden Satz verallgemeinert:

Satz 6.23 (Fingerabdrucksatz). *Sei $k \in \mathbb{N}_{\geqslant 1}$, seien $p_1 \ldots, p_k$ paarweise verschiedene Primzahlen und sei $n := \prod_{i=1}^{k} p_i$. Für alle $a, b \in \mathbb{Z}_n$ gilt:*

$$a \equiv b \mod p_i \quad \textit{für alle } i \in [k] \qquad \Longleftrightarrow \qquad a = b\,.$$

Somit können wir $b \in \mathbb{Z}_n$ eindeutig aus seinem "Fingerabdruck" $(b_1, \ldots, b_k)$ rekonstruieren, wobei b_i der Rest von b modulo p_i ist, für jedes $i \in [k]$.

Beweis. Die Richtung "$\Longleftarrow$" ist offensichtlich.
Für die Richtung "$\Longrightarrow$" nutzen wir den Chinesischen Restsatz für $a_i := b$ und $m_i := p_i$ für alle $i \in [k]$. Gemäß Aussage des Chinesischen Restsatzes gibt es ein eindeutig bestimmtes $x \in \mathbb{Z}_n$ so dass $x \equiv b \mod p_i$ für alle $i \in [k]$ gilt. Da sowohl $x = a$ also auch $x = b$ Lösungen für alle $i \in [k]$ sind, muss gelten: $a = b$. □

Anwendung in der Kryptgraphie: RSA-Verfahren

Folie 339

RSA-Verschlüsselung

Beim *RSA-Verfahren*[2] handelt es sich um ein asymmetrisches kryptographisches Verfahren, mit dem man Nachrichten sowohl verschlüsseln als auch digital signieren kann.
"Asymmetrisch" bedeutet, dass es einen geheimen Schlüssel und einen öffentlichen Schlüssel gibt.
Um für mich selbst solche Schlüssel zu erhalten, wähle ich zwei sehr große Primzahlen p_1 und p_2 mit $p_1 \neq p_2$ und setze $n := p_1 \cdot p_2$.
Die Zahl n *gebe ich öffentlich bekannt*; die beiden Primzahlen p_1, p_2 *halte ich geheim.*
Nachrichten, die man verschlüsselt an mich schicken kann, sind Zahlen in $\mathbb{Z}_n$.
Ich berechne die Zahl $m := (p_1 - 1) \cdot (p_2 - 1)$ (die ich geheim halte) und wähle eine kleine Zahl k, die teilerfremd ist zu m (d.h.: $\mathrm{ggT}(k, m) = 1$). Diese Zahl k gebe ich als meinen *"öffentlichen Schlüssel"* (engl.: public key) bekannt.
Ich berechne *das multiplikative Inverse $\ell := k^{-1}$ von k modulo m* und halte dieses als meinen *"privaten Schlüssel" geheim.*

Wenn jemand mir eine verschlüsselte Nachricht x schicken will, berechnet er den Rest y von x^k modulo n und schickt mir die Zahl y zu.

[2] benannt nach seinen Erfindern Rivest, Shamir, Adleman

Um y zu entschlüsseln, berechne ich den Rest r von y^ℓ modulo n.

Behauptung: $r = x$.

Beweis. Gemäß dem Fingerabdrucksatz (Satz 6.23) genügt es zu zeigen, dass $r \equiv x \mod p_i$ für jedes $i \in [2]$ gilt.
Wir betrachten p_1 (für p_2 folgt die Aussage analog).
Wegen $p_1 \mid n$ und $y \equiv x^k \mod n$ gilt: $y \equiv x^k \mod p_1$. Daher gilt auch: $y^\ell \equiv x^{k\ell} \mod p_1$, d.h. $r \equiv x^{k\ell} \mod p_1$.
Fall 1: $p_1 \mid x$.
Dann gilt auch: $p_1 \mid (x^{k\ell} - x)$, d.h. $x^{k\ell} \equiv x \mod p_1$. Somit gilt: $r \equiv x \mod p_1$.
Fall 2: $p_1 \nmid x$.
Dann folgt aus dem kleinen Satz von Fermat (Satz 6.21): $x^{p_1-1} \equiv 1 \mod p_1$.
Gemäß unserer Wahl von k und ℓ gilt: $k \cdot \ell \equiv 1 \mod m$. Somit gilt: $m \mid (k \cdot \ell - 1)$, d.h. es gibt ein $c \in \mathbb{Z}$ so dass $k \cdot \ell - 1 = c \cdot m = c \cdot (p_1 - 1) \cdot (p_2 - 1)$.
Somit gilt: $x^{k\ell-1} = x^{c \cdot m} = \left(x^{p_1-1}\right)^{c \cdot (p_2-1)}$.
Wegen $x^{p_1-1} \equiv 1 \mod p_1$ folgt also: $x^{k\ell-1} \equiv 1^{c \cdot (p_2-1)} \mod p_1$, d.h. $x^{k\ell-1} \equiv 1 \mod p_1$. Daher ist $x^{k\ell} \equiv x \mod p_1$, d.h. $r \equiv x \mod p_1$. □

Folie 340

RSA-Signierung

Falls ich jemandem eine Nachricht $x \in \mathbb{Z}_n$ schicken will, kann ich diese mit einer "Signatur" versehen, so dass der Empfänger sicher sein kann, dass die Nachricht tatsächlich von mir stammt. Dazu kann ich wie folgt vorgehen:

Ich berechne den Rest z von x^ℓ modulo n und schicke dem Empfänger die Zahlen x und z.

Der Empfänger berechnet den Rest r von z^k modulo n und überprüft, ob $r = x$ ist. Falls ja, kann er davon ausgehen, dass die Nachricht tatsächlich von mir an ihn geschickt worden ist.

Behauptung: $r = x$.

Beweis. Es gilt: $r \equiv z^k \mod n$ und $z \equiv x^\ell \mod n$. Also gilt: $r \equiv x^{k\ell} \mod n$.
Wir sind also genau in derselben Situation wie oben bei der RSA-Verschlüsselung. Dort haben wir bereits gezeigt, dass $r = x$ ist. □

6.2 Gruppen, Ringe und Körper

Gruppen

Folie 341

Verknüpfungen

Definition 6.24. Sei M eine Menge.

(a) Eine *Verknüpfung* auf M ist eine Abbildung $\circ : M \times M \to M$.

Für $a, b \in M$ schreiben wir statt $\circ(a, b)$ oft $a \circ b$. Insbesondere bedeutet $(a \circ b) \circ c$ dann: $\circ(\circ(a, b), c)$.

(b) Eine Verknüpfung $\circ$ auf M heißt *assoziativ*, wenn für alle $a, b, c \in M$ gilt: $(a \circ b) \circ c = a \circ (b \circ c)$.

(c) Eine Verknüfung $\circ$ auf M heißt *kommutativ*, wenn für alle $a, b \in M$ gilt: $a \circ b = b \circ a$.

Beispiel: Betrachte $M := \mathbb{Q}$ und die Verknüfung

- $+$ (Addition auf $\mathbb{Q}$): diese Verknüpfung ist assoziativ und kommutativ
- $-$ (Subtraktion auf $\mathbb{Q}$): diese Verknüpfung ist nicht assoziativ (denn: $(2-3)-4 = -1-4 = -5$, aber $2-(3-4) = 2-(-1) = 3$) und nicht kommutativ (denn: $2-3 = -1$, aber $3-2 = 1$)
- $\cdot$ (Multiplikation auf $\mathbb{Q}$): diese Verknüpfung ist assoziativ und kommutativ
- $:$ (Division auf $\mathbb{Q}$): diese Verknüpfung ist nicht assoziativ (denn: $(18:3):3 = 6:3 = 2$, aber $18:(3:3) = 18:1 = 18$) und nicht kommutativ (denn: $2:1 = 2$, aber $1:2 = \frac{1}{2}$)

Folie 342

Halbgruppen, Monoide und neutrale Elemente

Definition 6.25. Sei M eine Menge und sei $\circ$ eine Verknüpfung auf M.

(a) $(M, \circ)$ ist eine *Halbgruppe*, falls $\circ$ assoziativ ist.

$(M, \circ)$ ist eine *kommutative Halbgruppe*, falls $\circ$ assoziativ und kommutativ ist.

(b) Ein *neutrales Element* für $(M, \circ)$ ist ein $e \in M$ so dass für alle $a \in M$ gilt: $a \circ e = e \circ a = a$.

(c) $(M, \circ)$ ist ein *Monoid*, falls $(M, \circ)$ eine Halbgruppe ist, die ein neutrales Element besitzt.

Ein *kommutatives Monoid* ist eine kommutative Halbgruppe, die ein neutrales Element besitzt.

Bemerkung 6.26. Sei M eine Menge und sei $\circ$ eine Verknüpfung auf M. Wenn $(M, \circ)$ ein neutrales Element besitzt, so ist dieses eindeutig bestimmt.

Beweis: Seien e und e' neutrale Elemente für $(M, \circ)$. Dann gilt für alle $a \in M$: $a \circ e = e \circ a = a = a \circ e' = e' \circ a$.
Indem wir $a := e'$ wählen, erhalten wir: $e' \circ e = e'$.
Indem wir $a := e$ wählen, erhalten wir: $e = e' \circ e$.
Somit gilt: $e = e'$. □

Folie 343

Beispiele 6.27.

(a) Sei Σ ein Alphabet (d.h. eine nicht-leere Menge).

Sei $\circ$ die *Konkatenation* auf Σ^*, d.h. für alle Worte $v, w \in \Sigma^*$ ist $v \circ w$ das Wort vw.

Dann ist $(\Sigma^*, \circ)$ ein Monoid, dessen neutrales Element e das leere Wort ε ist. Falls $|\Sigma| \geqslant 2$ ist, so ist diese Monoid *nicht* kommutativ.

(b) Betrachte $\mathbb{N}$ mit der Verknüpfung

- $+$ (Addition auf $\mathbb{N}$): Dann ist $(\mathbb{N}, +)$ ein kommutatives Monoid, dessen neutrales Element e die Zahl 0 ist.
- $\cdot$ (Multiplikation auf $\mathbb{N}$): Dann ist $(\mathbb{N}, \cdot)$ ein kommutatives Monoid, dessen neutrales Element e die Zahl 1 ist.

(c) Betrachte $\mathbb{N}_{\geqslant 1}$ mit der Verknüpfung $+$ (Addition): Dann ist $(\mathbb{N}_{\geqslant 1}, +)$ eine kommutative Halbgruppe, die kein neutrales Element besitzt.

Folie 344

Inverse Elemente und Gruppen

Definition 6.28. Sei $(M, \circ)$ ein Monoid und sei e dessen neutrales Element. Ein *Inverses* von $a \in M$ ist ein $a' \in M$ so dass gilt: $a \circ a' = e = a' \circ a$.

Bemerkung 6.29. Sei $(M, \circ)$ ein Monoid. Wenn ein $a \in M$ ein Inverses besitzt, so ist dieses eindeutig bestimmt.

Beweis: Sei e das neutrale Element des Monoids $(M, \circ)$. Seien $a', a'' \in M$ Inverse von a. Dann gilt: $a \circ a' = e = a' \circ a$ und $a \circ a'' = e = a'' \circ a$.
Somit gilt: $(a'' \circ a) \circ a' = e \circ a' = a'$. Und es gilt:
$(a'' \circ a) \circ a' = a'' \circ (a \circ a') = a'' \circ e = a''$. Somit gilt: $a' = a''$. □

Definition 6.30. Eine *Gruppe* ist ein Monoid $(M, \circ)$, bei dem jedes Element $a \in M$ ein Inverses besitzt.

D.h.: M ist eine Menge und $\circ$ ist eine Verknüpfung auf M, für die gilt:

(1) $\circ$ ist assoziativ, d.h. für alle $a, b, c \in M$ gilt: $(a \circ b) \circ c = a \circ (b \circ c)$,

(2) $(M, \circ)$ besitzt ein neutrales Element e, d.h.: $e \in M$ und für alles $a \in M$ gilt: $a \circ e = e \circ a = a$, und

(3) jedes $a \in M$ besitzt ein Inverses, d.h. es gibt ein $a' \in M$ so dass $a \circ a' = a' \circ a = e$.

Definition 6.31. Eine *kommutative Gruppe* bzw. *abelsche Gruppe* ist eine Gruppe $(M, \circ)$, deren Verknüpfung $\circ$ kommutativ ist.

Folie 345

Beispiele 6.32.

(a) $(\mathbb{N}, +)$ ist keine Gruppe, da kein $n \in \mathbb{N}$ mit $n \neq 0$ ein Inverses besitzt.

(b) $(\mathbb{Z}, +)$ ist eine abelsche Gruppe mit neutralem Element 0; für jedes $z \in \mathbb{Z}$ gilt: das Inverse von z ist die Zahl $(-1) \cdot z$.

(c) $(\mathbb{Z} \setminus \{0\}, \cdot)$ ist ein kommutatives Monoid mit neutralem Element 1; aber keine Gruppe, da z.B. die Zahl $2 \in \mathbb{Z}$ kein Inverses besitzt.

(d) $(\mathbb{Q} \setminus \{0\}, \cdot)$ ist eine abelsche Gruppe mit neutralem Element 1; für jedes $q \in \mathbb{Q}$ gilt: das Inverse von q ist die Zahl $\frac{1}{q}$.

(e) $(\mathbb{Q}, \cdot)$ ist keine Gruppe, da die Zahl 0 kein Inverses besitzt, denn es gibt kein $q \in \mathbb{Q}$ so dass $0 \cdot q = 1$.

Folie 346

Die *symmetrische Gruppe* S_n

Beispiel 6.33. Sei $n \in \mathbb{N}_{\geqslant 1}$ und betrachte die Menge $[n] = \{1, \ldots, n\}$. Sei S_n die Menge aller Permutationen von $[n]$, d.h. die Menge aller bijektiven Abbildungen $f : [n] \to [n]$.
Für alle $f, g \in S_n$ sei $f \circ g$ die Abbildung $h : [n] \to [n]$ mit $h(i) := f(g(i))$ für alle $i \in [n]$. Da f und g bijektiv sind, ist auch h bijektiv.
Somit ist $\circ$ eine Verknüpfung auf S_n.

Behauptung: $(S_n, \circ)$ ist eine Gruppe.

Beweis: Man kann leicht nachrechnen, dass $\circ$ assoziativ ist, dass die Identitätsfunktion $\mathrm{id}_{[n]}$ das neutrale Element von $(S_n, \circ)$ ist, und dass für jedes $f \in S_n$ gilt: das Inverse von f ist die *Umkehrabbildung* f^{-1} mit $f^{-1}(j) = i$ für alle $j \in [n]$ und dasjenige $i \in [n]$ mit $f(i) = j$. Details: Übungsaufgabe. □

Die Gruppe $(S_n, \circ)$ wird die *symmetrische Gruppe* S_n genannt. Es gilt: $|S_n| = n!$. Für $n \geqslant 3$ ist die symmetrische Gruppe S_n ist nicht kommutativ, denn: Sei $f \in S_n$ mit $f(1) = 2$, $f(2) = 3$ und $f(3) = 1$ — wir schreiben dafür kurz: $f = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{smallmatrix}\right)$. Sei $g = \left(\begin{smallmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{smallmatrix}\right)$, d.h. $g(1) = 3$, $g(2) = 2$ und $g(3) = 1$. Dann ist $f \circ g \neq g \circ f$, denn $(f \circ g)(2) = f(g(2)) = f(2) = 3$ und $(g \circ f)(2) = g(f(2)) = g(3) = 1$, also $(f \circ g)(2) \neq (g \circ f)(2)$, also $f \circ g \neq g \circ f$.

Folie 347

Verknüpfungen auf $\mathbb{Z}_n$

Beispiele 6.34. Sei $n \in \mathbb{N}$ mit $n \geqslant 2$. Betrachte $\mathbb{Z}_n = \{0, \ldots, n-1\}$.

(a) Sei $+_n$ die "Addition modulo n", d.h. für alle $a, b \in \mathbb{Z}_n$ sei $a +_n b$ der Rest der Zahl $(a+b)$ modulo n.

Dann ist $(\mathbb{Z}_n, +_n)$ eine abelsche Gruppe mit neutralem Element 0. Das Inverse von $a \in \mathbb{Z}_n \setminus \{0\}$ ist die Zahl $a' := n-a$, und das Inverse von 0 ist die Zahl 0.

(b) Sei $\cdot_n$ die "Multiplikation modulo n", d.h. für alle $a, b \in \mathbb{Z}_n$ sei $a \cdot_n b$ der Rest der Zahl $(a \cdot b)$ modulo n.

Dann ist $(\mathbb{Z}_n, \cdot_n)$ ein kommutatives Monoid mit neutralem Element 1; aber es ist keine Gruppe, da $0 \in \mathbb{Z}_n$ kein Inverses besitzt.

(c) Sei $\mathbb{Z}_n^\times := \{a \in \mathbb{Z}_n \ : \ a \neq 0 \text{ und } \mathrm{ggT}(a,n) = 1\}$.

Dann ist $(\mathbb{Z}_n^\times, \cdot_n)$ eine abelsche Gruppe mit neutralem Element 1.

Beweis:

- $\cdot_n$ ist eine Verknüpfung auf $\mathbb{Z}_n^\times$, denn: Seien $a, b \in \mathbb{Z}_n^\times$ und sei $c := a \cdot_n b$. Zu zeigen: $c \in \mathbb{Z}_n^\times$, d.h. $\mathrm{ggT}(c,n) = 1$.
  Wegen $a, b \in \mathbb{Z}_n^\times$ gilt: $\mathrm{ggT}(a,n) = 1 = \mathrm{ggT}(b,n)$. Gemäß Satz 6.13(a) gilt: $\mathrm{ggT}(ab,n) = 1$.
  Wegen $c = a \cdot_n b$ gilt: $c \in \mathbb{Z}_n$ und $c \equiv a \cdot b \mod n$. Somit gibt es ein $k \in \mathbb{N}$ so dass $c + kn = ab$. Aus $\mathrm{ggT}(ab,n) = 1$ folgt dann: $\mathrm{ggT}(c,n) = 1$ (denn: angenommen $t := \mathrm{ggT}(c,n) \geqslant 2$, dann gilt: $t \,|\, c$ und $t \,|\, n$, also: $t \,|\, c{+}kn$, d.h. $t \,|\, ab$, also $t \,|\, \mathrm{ggT}(ab,n)$. Widerspruch zu $\mathrm{ggT}(ab,n) = 1$).
- Wir wissen bereits, dass $\cdot_n$ assoziativ und kommutativ ist, und dass 1 das neutrale Element ist. Es gilt: $1 \in \mathbb{Z}_n^\times$.
  Um zu zeigen, dass $(\mathbb{Z}_n^\times, \cdot_n)$ eine abelsche Gruppe ist, müssen wir nur noch zeigen, dass jedes $a \in \mathbb{Z}_n^\times$ ein Inverses besitzt, d.h. dass es ein $x \in \mathbb{Z}_n^\times$ gibt, so dass $a \cdot_n x = 1$ ist.
  Da $\mathrm{ggT}(a,n) = 1$ ist, erhalten wir von Satz 6.17(b), dass es ein $x \in \mathbb{Z}_n$ gibt, so dass $ax \equiv 1 \mod n$ ist. Indem wir nochmals Satz 6.17(b) anwenden und dabei die Rollen von a und x vertauschen, erhalten wir aus der Gleichung $xa \equiv 1 \mod n$, dass $\mathrm{ggT}(x,n) = 1$ ist. Also ist $x \in \mathbb{Z}_n^\times$. □

Eigenschaften von Gruppen

Bemerkung 6.35. Sei $(G, \circ)$ eine Gruppe. Wir wissen bereits, dass es genau ein neutrales Element $e \in G$ gibt und dass es für jedes $g \in G$ genau ein Inverses gibt; wir schreiben im Folgenden g^{-1} um das Inverse von g zu bezeichnen.
Folgende Sachverhalte lassen sich leicht beweisen (Details: Übungsaufgabe):

1. Für alle $g \in G$ gilt: $(g^{-1})^{-1} = g$.
2. Für alle $g, h \in G$ gilt: $(g \circ h)^{-1} = h^{-1} \circ g^{-1}$.

   Man beachte die vertauschte Reihenfolge! Eselsbrücke, um sich dies zu merken: Sei h die Operation "ziehe die Socken an" und sei g die

Operation "ziehe die Schuhe an". Dann ist $g \circ h$ die Operation "ziehe erst die Socken und dann die Schuhe an". Das Inverse $(g \circ h)^{-1}$ soll die Operation $g \circ h$ rückgängig machen; dies erreichen wir, indem wir zuerst die Schuhe ausziehen (dies entspricht g^{-1}) und dann die Socken ausziehen (dies entspricht h^{-1}) — also die Operation $h^{-1} \circ g^{-1}$ anwenden. Somit gilt: $(g \circ h)^{-1} = h^{-1} \circ g^{-1}$.

3. *Kürzungsregel*: Für alle $a, b, c \in G$ gilt:
   Wenn $a \circ b = a \circ c$, dann $b = c$. Wenn $b \circ a = c \circ a$, dann $b = c$.

Folie 349

4. Für alle $a, b \in G$ gilt:

   - Die Gleichung $a \circ x = b$ ist eindeutig lösbar, d.h. es gibt genau ein $x \in G$ so dass $a \circ x = b$ ist.

     Beweis: Für $x := a^{-1} \circ b$ gilt:
     $a \circ x = a \circ (a^{-1} \circ b) = (a \circ a^{-1}) \circ b = e \circ b = b$. Die Eindeutigkeit von x folgt dann aus der Kürzungsregel. □

   - Die Gleichung $y \circ a = b$ ist eindeutig lösbar, d.h. es gibt genau ein $y \in G$ so dass $y \circ a = b$ ist.

     Beweis: Für $y := b \circ a^{-1}$ gilt:
     $y \circ a = (b \circ a^{-1}) \circ a = b \circ (a^{-1} \circ a) = b \circ e = b$. Die Eindeutigkeit von y folgt dann aus der Kürzungsregel. □

Folie 350

Untergruppen und Nebenklassen

Definition 6.36. Sei $(G, \circ)$ eine Gruppe und sei $U \subseteq G$.

(a) U ist eine *Untergruppe* von $(G, \circ)$, wenn gilt: U ist abgeschlossen unter der Verknüpfung $\circ$ (d.h. für alle $a, b \in U$ ist $a \circ b \in U$), U enthält das neutrale Element e von $(G, \circ)$ und für jedes $a \in U$ enthält U das Inverse a^{-1} von a in $(G, \circ)$.

(b) Für jedes $a \in G$ setze

$$\begin{aligned} a \circ U &:= \{a \circ u \ : \ u \in U\} \qquad \text{und} \\ U \circ a &:= \{u \circ a \ : \ u \in U\}. \end{aligned}$$

$a \circ U$ wird *Linksnebenklasse* (von U bzgl. a) genannt;
$U \circ a$ heißt *Rechtsnebenklasse* (von U bzgl. a).

Beispiel 6.37. Betrachte die rationalen Zahlen $\mathbb{Q}$ mit der Verknüpfung $+$ (Addition).
Dann ist $(\mathbb{Q}, +)$ eine Gruppe und $\mathbb{Z}$ ist eine Untergruppe.
Für jedes $n \in \mathbb{N}$ mit $n \geqslant 2$ ist die Menge $n\mathbb{Z}$ ebenfalls eine Untergruppe (Beweis: Übungsaufgabe); aber die Menge $\mathbb{Z}_n$ ist keine Untergruppe (denn sie ist nicht abgeschlossen unter der Addition $+$).
Für jedes $a \in \mathbb{Z}$ ist $a + n\mathbb{Z}$ eine Linksnebenklasse von $n\mathbb{Z}$. Da $+$ kommutativ ist, ist $a + n\mathbb{Z} = n\mathbb{Z} + a$ — d.h. Links- und Rechtsnebenklassen sind gleich.

Eigenschaften von Untergruppen und Nebenklassen

Satz 6.38. *Sei $(G, \circ)$ eine Gruppe und sei $U \subseteq G$ eine Untergruppe von $(G, \circ)$.*

(a) Für jedes $a \in G$ ist die Menge $a \circ U$ gleichmächtig zur Menge U.

(b) Für alle $a, b \in G$ gilt: $a \circ U = b \circ U$ oder $a \circ U \cap b \circ U = \emptyset$.

(c) Es gibt eine Menge $A \subseteq G$ so dass gilt: $G = \bigcup_{a \in A} a \circ U$, und die Mengen $a \circ U$ für $a \in A$ sind paarweise disjunkt.

Beweis. (a): Betrachte die Abbildung $f : U \to a \circ U$ mit $f(u) := a \circ u$ für alle $u \in U$. Gemäß der Definition von $a \circ U$ ist die Abbildung f surjektiv. Die Kürzungsregel liefert, dass f injektiv ist. Somit ist f eine bijektive Abbildung von U nach $a \circ U$, und daher sind die Mengen U und $a \circ U$ gleichmächtig.

(b): Wenn $a \circ U \cap b \circ U \neq \emptyset$, dann gibt es ein $c \in a \circ U \cap b \circ U$. D.h. es gibt $u, v \in U$ so dass $c = a \circ u = b \circ v$.
Dann ist $c \circ u^{-1} = (a \circ u) \circ u^{-1} = a \circ (u \circ u^{-1}) = a$.
Und es gilt: $c \circ u^{-1} = (b \circ v) \circ u^{-1} = b \circ (v \circ u^{-1})$. Da U eine Untergruppe von $(G, \circ)$ ist, gilt: $u^{-1} \in U$ und $v \circ u^{-1} \in U$. Somit ist $b \circ (v \circ u^{-1}) \in b \circ U$.
Wegen $a = b \circ (v \circ u^{-1})$ ist also $a \in b \circ U$.
Daraus folgt: $a \circ U \subseteq b \circ U$ (denn: für jedes beliebige $w \in U$ gilt:
$a \circ w = (b \circ (v \circ u^{-1})) \circ w = b \circ ((v \circ u^{-1}) \circ w) \in b \circ U$).
Analog erhält man, dass auch gilt: $b \circ U \subseteq a \circ U$. Somit ist also $a \circ U = b \circ U$.

(c): Die Relation $\sim$ mit $a \sim b \iff a \circ U = b \circ U$ (f.a. $a, b \in G$) ist eine Äquivalenzrelation auf G. Sei M die Menge der Äquivalenzklassen von $\sim$ auf G. Für jedes Element $m \in M$ wähle ein $a_m \in G$ so dass $m = \{g \in G \ : \ g \sim a_m\}$. Sei $A := \{a_m \ : \ m \in M\}$. Man kann sich leicht davon überzeugen, dass $G = \bigcup_{a \in A} a \circ U$ ist und dass die Mengen $a \circ U$ für $a \in A$ paarweise disjunkt sind (Details: Übungsaufgabe). □

Folie 353

Der Satz von Lagrange

Satz 6.39 (Satz von Lagrange)**.** *Sei $(G, \circ)$ eine endliche Gruppe*[3]*.*
Dann gilt für jede Untergruppe U von $(G, \circ)$: $|U| \,|\, |G|$
(d.h. $|G|$ ist ein ganzzahliges Vielfaches von $|U|$),
und die Anzahl der verschiedenen Linksnebenklassen von U in G ist $\frac{|G|}{|U|}$.

Beweis. Gemäß Satz 6.38 gibt es eine Menge $A \subseteq G$ so dass $G = \bigcup_{a \in A} a \circ U$ ist und die Mengen $a \circ U$ für $a \in A$ paarweise disjunkt und gleichmächtig zu U sind. Somit gilt: $|G| = \sum_{a \in A} |a \circ U| = \sum_{a \in A} |U| = |A| \cdot |U|$. □

Als einfache Folgerung aus dem Satz von Lagrange erhalten wir:

Folgerung 6.40. *Sei p eine Primzahl und sei $+_p$ die "Addition modulo p". Die Gruppe $(\mathbb{Z}_p, +_p)$ besitzt als Untergruppen nur sich selbst und die Menge $\{0\}$, die nur aus dem neutralen Element besteht.*

Ringe und Körper

Folie 354

Definition 6.41 (Ringe und Körper)**.**
Ein *Ring* $(M, \oplus, \odot)$ besteht aus einer Menge M und zwei Verknüpfungen $\oplus$ und $\odot$ auf M, so dass gilt:

1.) $(M, \oplus)$ ist eine abelsche Gruppe, und für deren neutrales Element $\mathtt{0}$ gilt:

2.) $(M \setminus \{\mathtt{0}\}, \odot)$ ist ein Monoid (d.h. $\odot$ ist assoziativ und besitzt ein neutrales Element $\mathtt{1} \in M \setminus \{\mathtt{0}\}$), und

[3] d.h. G ist eine endliche Menge und $(G, \circ)$ ist eine Gruppe

3.) es gelten die folgenden *Distributivgesetze*: für alle $a, b, c \in M$ gilt:

$$\begin{aligned} a \odot (b \oplus c) &= (a \odot b) \oplus (a \odot c) \qquad \text{und} \\ (b \oplus c) \odot a &= (b \odot a) \oplus (c \odot a). \end{aligned}$$

Ein Ring $(M, \oplus, \odot)$ heißt *kommutativ*, wenn auch die Verknüpfung $\odot$ kommutativ ist.

Ein *Körper* ist ein Ring $(M, \oplus, \odot)$, für den $(M \setminus \{0\}, \odot)$ eine abelsche Gruppe ist.

Folie 355

Beispiele 6.42.
Seien $+$ und $\cdot$ die herkömmliche Addition und Multiplikation reeller Zahlen. Es gilt:
$(\mathbb{R}, +, \cdot)$ und $(\mathbb{Q}, +, \cdot)$ sind Körper.
$(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring, aber kein Körper (da z.B. die Zahl $2 \in \mathbb{Z} \setminus \{0\}$ kein multiplikatives Inverses in $\mathbb{Z} \setminus \{0\}$ besitzt).
$(\mathbb{N}, +, \cdot)$ ist kein Ring (da z.B. die Zahl $2 \in \mathbb{N}$ kein additives Inverses in $\mathbb{N}$ besitzt).

Folie 356

Der Restklassenring $\mathbb{Z}_n$

Bemerkung 6.43. Sei $n \in \mathbb{N}$ mit $n \geqslant 2$.
Wir betrachten $\mathbb{Z}_n$ mit den Verknüpfungen $+_n$ und $\cdot_n$ (Addition und Multiplikation modulo n).
Dann ist $(\mathbb{Z}_n, +_n, \cdot_n)$ ein kommutativer Ring (Beweis: Übungsaufgabe); er wird *Restklassenring (modulo n)* genannt.

Ist p eine Primzahl, so ist $(\mathbb{Z}_p, +_p, \cdot_p)$ ein Körper.

Beweis: Dass es ein kommutativer Ring ist, wissen wir bereits. Und aus Beispiel 6.34(c) wissen wir, dass $(\mathbb{Z}_p^\times, \cdot_p)$ eine abelsche Gruppe mit neutralem Element 1 ist. Es genügt daher, zu zeigen, dass $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$ ist. Es gilt: $\mathbb{Z}_p^\times = \{a \in \mathbb{Z}_p \ : \ a \neq 0 \text{ und } \mathrm{ggT}(a, p) = 1\}$. Da p eine Primzahl ist, folgt: $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \{0\}$. □

Ist $n \geqslant 2$ keine Primzahl, so ist $(\mathbb{Z}_n, +_n, \cdot_n)$ kein Körper.

Beweis: Sei $a \geqslant 2$ ein Teiler von n. Dann ist $\mathrm{ggT}(a, n) = a \neq 1$. Gemäß Satz 6.17(b) besitzt die Gleichung $ax \equiv 1 \mod n$ keine Lösung in $\mathbb{Z}_n$. Somit besitzt a kein Inverses in $(\mathbb{Z}_n \setminus \{0\}, \cdot_n)$. Also ist $(\mathbb{Z}_n \setminus \{0\}, \cdot_n)$ keine Gruppe. □

Folie 357

Endliche Körper

Bemerkung 6.44. Es ist Folgendes bekannt (hier ohne Beweis):

(a) Für jeden endlichen Körper $(K, \oplus, \odot)$ (d.h.: K ist eine endiche Menge und $(K, \oplus, \odot)$ ist ein Körper) gilt: Es gibt eine Primzahl p und ein $n \in \mathbb{N}_{\geqslant 1}$, so dass $|K| = p^n$ ist.

(b) Für jede Primzahl p und jedes $n \in \mathbb{N}_{\geqslant 1}$ gibt es einen endlichen Körper $(K, \oplus, \odot)$ mit $|K| = p^n$. Dieser Körper ist bis auf Isomorphie eindeutig bestimmt; er wird auch *Galoiskörper* bzw. *Galois-Feld* (engl.: Galois field) der Ordnung p^n genannt und mit $\mathrm{GF}(p^n)$ bzw $\mathbb{F}_{p^n}$ bezeichnet.

Für $n = 1$ ist $\mathrm{GF}(p)$ genau der Restklassenkörper $(\mathbb{Z}_p, +_p, \cdot_p)$.

Für $n \geqslant 2$ ist $\mathrm{GF}(p^n)$ *nicht* der Restklassenring $(\mathbb{Z}_{p^n}, +_{p^n}, \cdot_{p^n})$ (wir wissen ja bereits, dass dies kein Körper ist, da p^n keine Primzahl ist).

Folie 358

Funktionenring

Beispiel 6.45. Sei M eine nicht-leere Menge und sei $(R, \oplus, \odot)$ ein Ring. Betrachte die Menge $F := \mathrm{Abb}(M, R)$ aller Abbildungen $f : M \to R$.
Seien $\boxplus$ und $\boxdot$ die wie folgt definierten Verknüpfungen auf F:
Für alle $f, g \in F$ sei

- $f \boxplus g$ die Abbildung h in F mit $h(m) := f(m) \oplus g(m)$ für alle $m \in M$,
- $f \boxdot g$ die Abbildung h in F mit $h(m) := f(m) \odot g(m)$ für alle $m \in M$.

Dann ist $(F, \boxplus, \boxdot)$ ein Ring (Beweis: Übungsaufgabe); und F ist genau dann kommutativ wenn R kommutativ ist.

Folie 359

Polynomring $K[x]$

Bemerkung 6.46. Sei $(K, \oplus, \odot)$ ein Körper.
Ein *Polynom* in einer Variablen x mit Koeffizienten in K ist ein Ausdruck der Form

$$\sum_{i=0}^{n} a_i x^i$$

mit $n \in \mathbb{N}$ und $a_i \in K$ für alle i mit $0 \leqslant i \leqslant n$. $K[x]$ bezeichnet die Menge all dieser Polynome.

Ein solches Polynom beschreibt die wie folgt definierte *Polynomfunktion* $f : K \to K$: für alle $b \in K$ ist $f(b)$ der Wert, den man erhält, wenn man in dem obigen Ausdruck b für x einsetzt und $a_0 b^0$ als a_0 auffasst, für jedes $i \geqslant 1$ $a_i b^i$ als $a_i \odot \underbrace{b \odot \cdots \odot b}_{i \text{ mal}}$ ausrechnet, und diese Werte für alle $i \in \{0, \ldots, n\}$ gemäß der "Addition" $\oplus$ aufsummiert.

Folie 360

Wir definieren zwei Verknüpfungen $\boxplus$ und $\boxdot$ auf der Menge $K[x]$:

$$\sum_{i=0}^{n} a_i x^i \quad \boxplus \quad \sum_{i=0}^{m} b_i x^i \quad = \quad \sum_{i=0}^{k} c_i x^i$$

mit $k := \max\{n, m\}$ und $c_i = a_i \oplus b_i$ für alle $i \leqslant \min\{n, m\}$ und falls $m < n$ so $c_i = a_i$ für alle i mit $m < i \leqslant n$, bzw. falls $n < m$ so $c_i = b_i$ für alle i mit $n < i \leqslant m$.

$$\sum_{i=0}^{n} a_i x^i \quad \boxdot \quad \sum_{i=0}^{m} b_i x^i \quad = \quad \sum_{i=0}^{k} c_i x^i$$

mit $k := n+m$ und

$$c_i \;:=\; \bigoplus_{\substack{0 \leqslant j \leqslant n, \\ 0 \leqslant j' \leqslant m \,:\, j+j'=i}} (a_j \odot b_{j'})$$

wobei zum Aufaddieren der Summe die Operation $\oplus$ genutzt wird.

Man kann sich leicht davon überzeugen (Übungsaufgabe!), dass $(K[x], \boxplus, \boxdot)$ ein kommutativer Ring ist. Dieser Ring wird *Polynomring über dem Körper K* genannt.

6.3 Literaturhinweise

Als vertiefende Lektüre seien die Kapitel 4 und 5 von [Juk08] sowie die Kapitel 3 und 5 von [Ste07] empfohlen.

Quellennachweis: Teile dieses Kapitels basieren auf Teilen der Kapitel 4 und 5 von [Juk08].