Definition der Ringe

Definition (5.7)

Ein Ring ist ein Tripel $(R, +, \cdot)$ bestehend aus einer Menge R und zwei Verknüpfungen $+$ und $\cdot$ auf R mit folgenden Eigenschaften.

(i) Das Paar $(R, +)$ ist eine abelsche Gruppe.

(ii) Das Paar $(R, \cdot)$ ist ein abelsches Monoid.

(iii) Es gilt das Distributivgesetz $a(b + c) = ab + ac$ für alle $a, b, c \in R$.

Definition

Ein Körper ist ein Ring $(R, +, \cdot)$ mit der Eigenschaft

$$R^\times = R \setminus \{0_R\} \quad ,$$

d.h. die multiplikativ invertierbaren Elemente sind genau die Elemente ungleich null.

Addition und Multiplikation auf $\mathbb{Z}/n\mathbb{Z}$

Erinnerung: Sei $n \in \mathbb{N}$.

- $\mathbb{Z}/n\mathbb{Z} = \{a+n\mathbb{Z} \mid a \in \mathbb{Z}\} = \{0+n\mathbb{Z}, 1+n\mathbb{Z}, ..., (n-1)+n\mathbb{Z}\}$
- Für $a, b \in \mathbb{Z}$ gilt $a + n\mathbb{Z} = b + n\mathbb{Z}$ genau dann, wenn $b - a$ durch n teilbar ist.

Satz (5.9)

Sei $n \in \mathbb{N}$. Dann gibt es eindeutig bestimmte Abbildungen $+ : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ und $\cdot : \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ mit

$$(a + n\mathbb{Z}) + (b + n\mathbb{Z}) \quad = \quad (a + b) + n\mathbb{Z}$$

und

$$(a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) \quad = \quad ab + n\mathbb{Z}$$

für alle $a, b \in \mathbb{Z}$.

Addition und Multiplikation auf $\mathbb{Z}/7\mathbb{Z}$

Beispiele:

- $(5 + 7\mathbb{Z}) + (4 + 7\mathbb{Z}) = 9 + 7\mathbb{Z} = 2 + 7\mathbb{Z}$
- $(6 + 7\mathbb{Z}) \cdot (4 + 7\mathbb{Z}) = 24 + 7\mathbb{Z} = 3 + 7\mathbb{Z}$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{6}$	$\bar{6}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{1}$	$\bar{3}$	$\bar{5}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{2}$	$\bar{5}$	$\bar{1}$	$\bar{4}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{1}$	$\bar{5}$	$\bar{2}$	$\bar{6}$	$\bar{3}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{3}$	$\bar{1}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Definition der Restklassenringe

Satz (5.10)

Sei $n \in \mathbb{N}$. Dann bildet das Tripel $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ einen Ring, mit $\bar{0} = 0 + n\mathbb{Z}$ als Null- und $\bar{1} = 1 + n\mathbb{Z}$ als Einselement. Man bezeichnet ihn als Restklassenring modulo n.

Endliche Körper

Lemma (5.11)

Sind $m, n \in \mathbb{N}$ teilerfremd, dann gibt es $a, b \in \mathbb{Z}$ mit $am + bn = 1$.

Satz (5.12)

Für jedes $n \in \mathbb{N}$ ist der Restklassenring $\mathbb{Z}/n\mathbb{Z}$ genau dann ein Körper, wenn n eine Primzahl ist.

Beweis von Lemma S. 11

geg.: teilerfremde $m, n \in \mathbb{N}$ (d.h. $ggT(m,n) = 1$)

z.zg.: $\exists a, b \in \mathbb{Z}$ mit $am + bn = 1$

Betrachte $S = \{am + bn \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{Z}$

z.zg.: $1 \in S$ Sei $d \in \mathbb{N}$ die kleinste natürliche Zahl in S. Beh.: $d \mid s \ \forall s \in S$

Sei $s \in S$, ang. $d \nmid s$. Division mit Rest

$\Rightarrow \exists q \in \mathbb{Z}, r \in \{0, 1, \ldots, d-1\}$ mit $s = qd + r$

Wegen $d \nmid s$ gilt $r > 0$, also $r \in \mathbb{N}$. Es gilt

$r \in S$, denn: $d \in S \Rightarrow \exists a, b \in \mathbb{Z}$ mit

$d = am + bn$. $s \in S \Rightarrow \exists q_1, q_2 \in \mathbb{Z}$ mit

$s = a_1 m + b_1 n \Rightarrow r = s - qd = (a_1 m + b_1 n)$

$- q(am + bn) = \underbrace{(a_1 - qa)}_{\in \mathbb{Z}} m + \underbrace{(b_1 - qb)}_{\in \mathbb{Z}} n$

$\Rightarrow r \in S$ Wegen $s < d$ steht dies ein Widerspruch zur Minimalität von d. ($\Rightarrow$ Beh.)

Es gilt $m, n \in S$ (da $m = 1 \cdot m + 0 \cdot n$, $n = 0 \cdot m + 1 \cdot n$).

Beh $\Rightarrow d \mid m, d \mid n$ $ggT(m, n) = 1 \Rightarrow d = 1$

$\Rightarrow 1 \in S$ $\square$

Beweis von Satz 5.12 (Abschluss)

„$\Rightarrow$" Sei p eine Primzahl, z.zg.: $\mathbb{Z}/p\mathbb{Z}$ ist ein Körper, d.h. $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/p\mathbb{Z} \setminus \{0+p\mathbb{Z}\}$

„$\subseteq$" z.zg.: $\bar{0} = 0+p\mathbb{Z}$ ist kein invertierbares Element

Bereits bekannt: Ist $\bar{0}$ invertierbar, dann ist $\bar{0} = \bar{1}$, also $0+p\mathbb{Z} = 1+p\mathbb{Z}$. Es folgt $p \mid (1-0)$, d.h. $p \mid 1$ ↯

(1 ist keine Primzahl)

„$\supseteq$" Sei $a+p\mathbb{Z} \in \mathbb{Z}/p\mathbb{Z} \setminus \{0+p\mathbb{Z}\}$, mit $a \in \mathbb{Z}$.

Dann gilt $p \nmid a$ (sonst wäre $a+p\mathbb{Z} = 0+p\mathbb{Z}$).

Daraus folgt, dass p und a teilerfremd sind
(da 1 und p die einzigen Teiler von p in $\mathbb{N}$ sind).

Lemma 5.11 $\Rightarrow \exists\, k, m \in \mathbb{Z}$ mit $am + bp = 1$

$\Rightarrow am + bp + p\mathbb{Z} = 1 + p\mathbb{Z} \Rightarrow am + p\mathbb{Z} = 1 + p\mathbb{Z}$

$\Rightarrow (a + p\mathbb{Z}) \cdot (m + p\mathbb{Z}) = 1 + p\mathbb{Z}$

$\Rightarrow m + p\mathbb{Z} = (a + p\mathbb{Z})^{-1}$, insb. ist $a + p\mathbb{Z}$ ein invertierbares Element, liegt also in $(\mathbb{Z}/p\mathbb{Z})^*$

□

Kehrwerte in den Körpern $\mathbb{F}_7$ und $\mathbb{F}_{13}$

Notation: Ist p eine Primzahl, dann verwendet man für $\mathbb{Z}/p\mathbb{Z}$ auch die Bezeichnung $\mathbb{F}_p$. (Der Buchstabe $\mathbb{F}$ steht für die englische Übersetzung des algebraischen Begriffs „Körper“, „field“.)

Durch probeweises Multiplizieren findet man die folgenden Kehrwerte in $\mathbb{F}_7$.

a	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$
a^{-1}	–	$\bar{1}$	$\bar{4}$	$\bar{5}$	$\bar{2}$	$\bar{3}$	$\bar{6}$

Kehrwerte in $\mathbb{F}_{13}$

a	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{8}$	$\bar{9}$	$\overline{10}$	$\overline{11}$	$\overline{12}$
a^{-1}	–	$\bar{1}$	$\bar{7}$	$\bar{9}$	$\overline{10}$	$\bar{8}$	$\overline{11}$	$\bar{2}$	$\bar{5}$	$\bar{3}$	$\bar{4}$	$\bar{6}$	$\overline{12}$

Definition der Matrizen

Definition (5.13)

Seien $m, n \in \mathbb{N}$, und sei R ein Ring. Eine $m \times n$ - Matrix über R ist eine Abbildung

$$A : \{1, ..., m\} \times \{1, ..., n\} \longrightarrow R.$$

Dabei nennt man $A(i, j)$ den Eintrag von A an der Stelle (i, j). Die Menge aller $m \times n$-Matrizen über R wird mit $\mathscr{M}_{m \times n, R}$ bezeichnet.

Sei $A = (a_{ij}) \in \mathscr{M}_{m \times n, R}$ eine Matrix. Man nennt

- $a_{i\bullet} = (a_{i1}, ..., a_{in}) \in R^n$ die i-te Zeile und
- $a_{\bullet j} = (a_{1j}, ..., a_{mj}) \in R^m$ die j-te Spalte von A.

Allgemeine Form eines 3×4 - Matrix über $\mathbb{R}$:

$$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \\ a_{31} & a_{32} & a_{33} & a_{34} \end{pmatrix} \qquad a_{23} = A(2,3)$$

2.B. $$A = \begin{pmatrix} 2 & -3 & \sqrt{2} & 5 \\ 0 & 1 & 3/4 & 8 \\ -1 & \sqrt{2} & 3 & 7 \end{pmatrix} \qquad a_{2,3} = A(2,3) = 3/4$$

$a_{2\cdot} = (0, 1, 3/4, 8)$

$a_{\cdot 3} = (\sqrt{2}, 3/4, 3)$

Das Kronecker-Delta

Für jeden Ring R und beliebige $m, n \in \mathbb{N}$ definiert man

$$\delta_{mn} \quad = \quad \delta_{mn,R} \quad = \quad \begin{cases} 1_R & \text{falls} \quad m = n \\ 0_R & \text{falls} \quad m \neq n. \end{cases}$$

Wichtige Beispiele für Matrizen

Folgende Matrizen spielen in der Linearen Algebra eine besonders wichtige Rolle:

(i) die Nullmatrix $0^{(m\times n)}$ in $\mathscr{M}_{m\times n,R}$, deren sämtliche Einträge gleich 0_R sind und

(ii) die Einheitsmatrix $E = E^{(n)}$ in $\mathscr{M}_{n,R}$ mit den Einträgen δ_{ij} für $1 \leq i \leq m$ und $1 \leq j \leq n$

(iii) die Basismatrizen $B_{k\ell} = B_{k\ell}^{(m\times n)}$ mit den Einträgen $b_{ij} = \delta_{ik}\delta_{j\ell}$ für $1 \leq i \leq m$ und $1 \leq j \leq n$

Beispiel für eine Nullmatrix über $\mathbb{R}$:

$$0^{(4\times 3)} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Beispiel für eine Einheitsmatrix:

$$E^{(3)} = \begin{pmatrix} \delta_{11} & \delta_{12} & \delta_{13} \\ \delta_{21} & \delta_{22} & \delta_{23} \\ \delta_{31} & \delta_{32} & \delta_{33} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Beispiel für eine Basismatrix:

$$B_{12}^{(3\times 4)} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Das Summenzeichen

Sei R ein Ring, $n \in \mathbb{N}$ und seien $a_1, ..., a_n \in R$. Dann ist

$$\sum_{k=1}^{n} a_k \qquad \text{eine Kurzschreibweise für} \qquad a_1 + ... + a_n.$$

- Der Wert der Summe ist unabhängig vom verwendeten Laufindex. Beispielsweise ist $\sum_{j=1}^{n} a_j = \sum_{k=1}^{n} a_k$.
- Sei $A = (a_{ij})$ eine Matrix in $\mathscr{M}_{m\times n,R}$.
  Dann ist für $1 \leq k \leq m$ und $\leq \ell \leq n$ jeweils

$$\sum_{j=1}^{n} a_{kj} = a_{k1} + ... + a_{kn}$$

  und

$$\sum_{i=1}^{m} a_{i\ell} = a_{1\ell} + ... + a_{m\ell}.$$

- Der erste Gleichung gibt die Summe über $a_{k\bullet}$, die zweite die Summe über $a_{\bullet\ell}$ an.

Rechenoperationen auf Matrizen

(i) **Summe** Seien $A, B \in \mathscr{M}_{m\times n,R}$.
Dann sind die Einträge von $C = A + B$ gegeben durch
$c_{ij} = a_{ij} + b_{ij}$ für $1 \leq i \leq m$, $1 \leq j \leq n$.

(ii) **skalare Vielfache** Sei $A \in \mathscr{M}_{m\times n,R}$ und $\lambda \in R$.
Dann sind die Einträge von λA gegeben durch λa_{ij}.

(iii) **Produkt** Seien $A \in \mathscr{M}_{m\times n,R}$ und $B \in \mathscr{M}_{n\times r,R}$.
Dann sind die Einträge von $C = AB \in \mathscr{M}_{m\times r,R}$ gegeben durch

$$c_{ij} \quad = \quad \sum_{k=1}^{n} a_{ik} b_{kj}.$$

(iv) **Transposition** Sei $A \in \mathscr{M}_{m\times n,R}$.
Dann ist ${}^{\mathrm{t}}A \in \mathscr{M}_{n\times m,R}$, und der Eintrag von ${}^{\mathrm{t}}A$ an der Stelle (i, j) ist a_{ji}.

· NICHT RAUCHEN ·

Beispiel für die Summe von zwei Matrizen:

$$\underbrace{\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}}_{A} + \underbrace{\begin{pmatrix} -1 & 7 & 8 \\ -5 & 3 & 2 \end{pmatrix}}_{B} = \begin{pmatrix} 0 & 9 & 11 \\ -1 & 8 & 8 \end{pmatrix}$$

Beispiel für ein skalares Vielfaches:

$$(-2)\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} -2 & -4 & -6 \\ -8 & -10 & -12 \end{pmatrix}$$

Beispiel für ein Produkt zweier Matrizen:

$$\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}\begin{pmatrix} 0 & -2 \\ 3 & 8 \\ -7 & 5 \end{pmatrix} = \underbrace{\begin{pmatrix} -15 & 29 \\ -27 & 62 \end{pmatrix}}_{C}$$

$c_{11} = 1 \cdot 0 + 2 \cdot 3 + 3 \cdot (-7)$
$= -15$

Beispiel für eine Transposition:

$$t\begin{pmatrix}1 & 2 & 3\\ 4 & 5 & 6\end{pmatrix} = \begin{pmatrix}1 & 4\\ 2 & 5\\ 3 & 6\end{pmatrix} \qquad t\begin{pmatrix}1 & 4\\ 2 & 5\\ 3 & 6\end{pmatrix} = \begin{pmatrix}1 & 2 & 3\\ 4 & 5 & 6\end{pmatrix}$$

Die additive Gruppe der Matrizen

Proposition (5.14)

Sei R ein Ring, und seien $m, n \in \mathbb{N}$. Dann bildet die Menge $\mathscr{M}_{m\times n,R}$ mit der Addition von Matrizen eine abelsche Gruppe. Dabei ist $0^{(m\times n)}$ das Neutralelement, und für jedes $A \in \mathscr{M}_{m\times n,R}$ ist $(-1_R)A$ das Inverse von A. Dieses Inverse wird das Negative von A genannt und mit $-A$ bezeichnet.

Weitere Rechenregeln für Matrizen

Proposition (5.15)

Sei R ein Ring, und seien $m, n, r, s \in \mathbb{N}$. Weiter seien $A, A' \in \mathscr{M}_{m\times n,R}$, $B, B' \in \mathscr{M}_{n\times r,R}$ und $C \in \mathscr{M}_{r\times s,R}$.
Dann gelten die folgenden Rechenregeln.

(i) $A(B + B') = AB + AB'$, $(A + A')B = AB + A'B$

(ii) $A(\lambda B) = (\lambda A)B = \lambda(AB)$

(iii) $E^{(m)}A = AE^{(n)} = A$

(iv) $(AB)C = A(BC)$

(v) ${}^{\mathrm{t}}(AB) = {}^{\mathrm{t}}B\,{}^{\mathrm{t}}A$

Beweis von Prop. 5.15 (teilweise)

zu (i) geg. $A, A' \in M_{m\times n, R}$, $B \in M_{n\times r, R}$

z.zg.: $(A + A') \cdot B = AB + A'B$

Setze $C' = A + A'$, $D = C' \cdot B$, $F = AB$

$G = A'B$ und $H = F + G$. zu zeigen:

Die Matrizen $D, H \in M_{m\times r, R}$ stimmen überein.

Sei $i \in \{1, \dots, m\}$, $j \in \{1, \dots, r\}$ nachzurechnen:

$$d_{ij} = h_{ij}$$

Für $1 \le k \le m$, $1 \le l \le n$ gilt $c'_{kl} = a_{kl} + a'_{kl}$.

Für $1 \le i \le m$ und $1 \le j \le r$ gilt jeweils

$$d_{ij} = \sum_{l=1}^{n} c'_{il} b_{lj} = \sum_{l=1}^{n} (a_{il} + a'_{il}) b_{lj}$$

Für $1 \le i \le m$ und $1 \le j \le r$ gilt

$$f_{ij} = \sum_{l=1}^{n} a_{il} b_{lj} \quad \text{und} \quad g_{ij} = \sum_{l=1}^{n} a'_{il} b_{lj}$$

Somit $h_{ij} = f_{ij} + g_{ij} = \sum_{l=1}^{n} a_{il} b_{lj} + \sum_{l=1}^{n} a'_{il} b_{lj}$

$$= \sum_{l=1}^{n} (a_{il} b_{lj} + a'_{il} b_{lj}) = \sum_{l=1}^{n} (a_{il} + a'_{il}) b_{lj} = d_{ij}$$

zu (iii) z.zg.: $E^{(m)} \cdot A = A$

Für $1 \leq i \leq m$ und $1 \leq j \leq n$ ist der Eintrag von $E^{(m)} A$ an der Stelle (i,j) gegeben durch

$$\sum_{k=1}^{m} \delta_{ik} \cdot a_{kj} = \delta_{ii} a_{ij} = a_{ij}$$

$\delta_{ik} = 0$ für $k \neq i$

zu (iv) gegeben $A \in M_{m \times n, R}$, $B \in M_{n \times r, R}$, $C \in M_{m \times s, R}$

z.zg. $(AB) \cdot C = A(B \cdot C) \in M_{m \times s, R}$

Setze $D = AB$, $F = DC$, $G = BC$, $H = AG$

z.zg.: $F = H$

Sei $i \in \{1, \dots, m\}$, $j \in \{1, \dots, s\}$ zzg: $f_{ij} = h_{ij}$

Für $1 \le i \le m$, $1 \le k \le r$ gilt

$$d_{ik} = \sum_{l=1}^{n} a_{il} b_{lk}$$

Für $1 \le i \le m$ und $1 \le j \le s$ gilt

$$f_{ij} = \sum_{l=1}^{r} d_{il} c_{lj} = \sum_{l=1}^{r} \sum_{u=1}^{n} a_{iu} b_{ul} c_{lj}$$

Für $1 \le k \le n$ und $1 \le j \le s$ gilt

$$g_{kj} = \sum_{u=1}^{r} b_{ku} c_{uj}.$$

Für $1 \leq i \leq m$, $1 \leq j \leq s$ gilt

$$h_{ij} = \sum_{l=1}^{n} a_{il} \cdot g_{lj} = \sum_{l=1}^{n} \sum_{u=1}^{r} a_{il} b_{lu} c_{uj}$$

$$= \sum_{l=1}^{r} \sum_{u=1}^{n} a_{iu} b_{ul} c_{lj} = f_{ij}$$