Definition (5.3)

(i) Eine Halbgruppe ist ein Paar $(G, \cdot)$ bestehend aus einer nichtleeren Menge G und einer assoziativen Verknüpfung $\cdot$ auf der Menge G.

(ii) Ein Element $e \in G$ in einer Halbgruppe wird Neutralelement genannt, wenn $g \cdot e = e \cdot g = g$ für alle $g \in G$ erfüllt ist.

(iii) Eine Halbgruppe $(G, \cdot)$, in der ein Neutralelement existiert, wird Monoid genannt.

Definition (5.4)

(i) Ein Element g in einem Monoid $(G, \cdot)$ mit Neutralelement e heißt invertierbar, wenn ein $h \in G$ existierst, so dass die Gleichungen $g \cdot h = h \cdot g = e$ erfüllt sind.

(ii) Eine Gruppe ist ein Monoid, in dem jedes Element invertierbar ist.

(iii) Eine Halbgruppe, und ebenso ein Monoid und eine Gruppe, wird kommutativ oder abelsch genannt, wenn die zugehörige Verknüpfung kommutativ ist.

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 $a, b, c \in R$.

Wenn die Menge $R^\times$ der invertierbaren Elemente des Monoids $(R, \cdot)$ mit $R \setminus \{0_R\}$ übereinstimmt, dann bezeichnet man den Ring auch als Körper.

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

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

- $\mathbb{Z}/n\mathbb{Z} = \{a+n\mathbb{Z} \mid a+n\mathbb{Z}\} = \{0+n\mathbb{Z}, 1+n\mathbb{Z}, ..., (n-1)+n\mathbb{Z}\}$
- 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 $\mathbb{Z}/4\mathbb{Z}$

Vorgehensweise:

- Um zwei Elemente $a + 4\mathbb{Z}$ und $b + 4\mathbb{Z}$ in $\mathbb{Z}/4\mathbb{Z}$ zu addieren, bilde die Summe $a + b$ und anschließend den Rest von $a + b$ von nach Division durch 4.
- Um zwei Elemente $a + 4\mathbb{Z}$ und $b + 4\mathbb{Z}$ in $\mathbb{Z}/4\mathbb{Z}$ zu multiplizieren, bilde das Produkt ab und anschließend den Rest von ab von nach Division durch 4.

Beispiele:

- $(3 + 4\mathbb{Z}) + (2 + 4\mathbb{Z}) = 5 + 4\mathbb{Z} = 1 + 4\mathbb{Z}$
- $(3 + 4\mathbb{Z}) \cdot (2 + 4\mathbb{Z}) = 6 + 4\mathbb{Z} = 2 + 4\mathbb{Z}$

,

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

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.

Beweis von Satz 5.10:

Sei $n \in \mathbb{N}$. Beh.: $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ ist ein Ring

Es gilt nach Definition

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

$$(a + n\mathbb{Z}) \cdot (b + n\mathbb{Z}) = a \cdot b + n\mathbb{Z} \quad \text{für alle } a, b \in \mathbb{Z}$$

zu überprüfen:

(i) $(\mathbb{Z}/n\mathbb{Z}, +)$ ist eine abelsche Gruppe mit $\overline{0} = 0 + n\mathbb{Z}$ als Neutralelement

(ii) $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ ist ein abelsches Monoid, mit $\overline{1} = 1 + n\mathbb{Z}$ als Neutralelement.

(iii) Es gilt das Distributivgesetz

$$\bar{a} \cdot (\bar{b} + \bar{c}) = \bar{a} \cdot \bar{b} + \bar{a} \cdot \bar{c} \quad \forall \bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}/n\mathbb{Z}.$$

<u>zu (i)</u> Kommutativität von + auf $\mathbb{Z}/n\mathbb{Z}$:

Seien $\bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z}$. z.zg: $\bar{a} + \bar{b} = \bar{b} + \bar{a}$

Nach Def. von $\mathbb{Z}/n\mathbb{Z}$ gibt es Elemente $a, b \in \mathbb{Z}$ mit $\bar{a} = a + n\mathbb{Z}$ und $\bar{b} = b + n\mathbb{Z}$. Es gilt dann

$$\bar{a} + \bar{b} = (a + n\mathbb{Z}) + (b + n\mathbb{Z}) = (a+b) + n\mathbb{Z} \underset{\uparrow}{=} (b+a) + n\mathbb{Z}$$

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

da + auf $\mathbb{Z}$ das Kommutativgesetz erfüllt

Assoziativität von + auf $\mathbb{Z}/n\mathbb{Z}$:

Seien $\bar{a}, \bar{b}, \bar{c} \in \mathbb{Z}/n\mathbb{Z}$. z.zg.:

$$(\bar{a} + \bar{b}) + \bar{c} = \bar{a} + (\bar{b} + \bar{c})$$

$(a + b) + n\mathbb{Z} = a + (b + n\mathbb{Z})$
$a \in \mathbb{Z}$, $b + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$
$\Rightarrow$ keine Verkn. definiert

$\bar a, \bar b, \bar c \in \mathbb{Z}/n\mathbb{Z} \Rightarrow \exists\, a, b, c \in \mathbb{Z}$

mit $\bar a = a + n\mathbb{Z}$, $\bar b = b + n\mathbb{Z}$, $\bar c = c + n\mathbb{Z}$

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

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

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

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

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

$$= \bar a + (\bar b + \bar c)$$

Nachweis, dass $\bar 0$ Neutralelement in $(\mathbb{Z}/n\mathbb{Z}, +)$

zu (ii

$\bar a \cdot ($

$\bar a, \bar b$

$\bar a = a+$

$\Rightarrow \bar a$

ist: Sei $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$. z.zg: $\bar{a} + \bar{0} = \bar{a}$ und $\bar{0} + \bar{a} = \bar{a}$. $\bar{a} \in \mathbb{Z}/n\mathbb{Z} \Rightarrow \exists\, a \in \mathbb{Z}$ mit $\bar{a} = a + n\mathbb{Z}$. $\Rightarrow \bar{a} + \bar{0} = (a + n\mathbb{Z}) + (0 + n\mathbb{Z}) = (a+0) + n\mathbb{Z} \overset{a+0=a \text{ in } \mathbb{Z}}{=} a + n\mathbb{Z}$, ebenso: $\bar{0} + \bar{a} = (0 + n\mathbb{Z}) + (a + n\mathbb{Z}) = (0+a) + n\mathbb{Z} = a + n\mathbb{Z} = \bar{a}$.

[alternativ: $\bar{0} + a \underset{\text{Kommutativgesetz für + auf } \mathbb{Z}/n\mathbb{Z} \text{ bereits gezeigt}}{=} \bar{a} + \bar{0} = \bar{a}$]

Existenz von Inversen: Sei $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$. z.zg: Es gibt ein $\bar{b} \in \mathbb{Z}/n\mathbb{Z}$ mit $\bar{a} + \bar{b} = \bar{0}$ und $\bar{b} + \bar{a} = \bar{0}$.

$\mathbb{Z}$

$+(c+n\mathbb{Z})$

$n\mathbb{Z}$

$(\mathbb{Z}/n\mathbb{Z},+)$

$\bar a \in \mathbb{Z}/n\mathbb{Z} \Rightarrow \exists\, a \in \mathbb{Z}$ mit $\bar a = a + n\mathbb{Z}$.

Sei $\bar b = (-a) + n\mathbb{Z}$. $\bar a + \bar b = (a + n\mathbb{Z}) + ((-a) + n\mathbb{Z})$

$= (a+(-a)) + n\mathbb{Z} = 0 + n\mathbb{Z} = \bar 0$, $\bar b + \bar a =$

$\bar a + \bar b = \bar 0$.

zu (ii) siehe Skript (besser: Übung)

zu (iii) Seien $\bar a, \bar b, \bar c \in \mathbb{Z}/n\mathbb{Z}$. z.zg.:

$\bar a \cdot (\bar b + \bar c) = \bar a \cdot \bar b + \bar a \cdot \bar c$.

$\bar a, \bar b, \bar c \in \mathbb{Z}/n\mathbb{Z} \Rightarrow \exists\, a, b, c \in \mathbb{Z}$ mit

$\bar a = a + n\mathbb{Z}$, $\bar b = b + n\mathbb{Z}$, $\bar c = c + n\mathbb{Z}$.

$\Rightarrow \bar a \cdot (\bar b + \bar c) = (a + n\mathbb{Z}) \cdot ((b + n\mathbb{Z}) + (c + n\mathbb{Z}))$

$\bar{a}$

$\mathbb{Z}$

$+0=a$ in $\mathbb{Z}$

$=$

$)\ +$

$\bar{a}.$

$]$

eits

$\bar{b}\in\mathbb{Z}/n\mathbb{Z}$

$$= (a+n\mathbb{Z})\cdot\big((b+c)+n\mathbb{Z}\big) = a\cdot(b+c)+n\mathbb{Z} =$$

Distributivität in $(\mathbb{Z},+,\cdot)$

$$(ab+ac)+n\mathbb{Z} =$$

$$(ab+n\mathbb{Z})+(ac+n\mathbb{Z}) =$$

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

$$\bar{a}\cdot\bar{b}+\bar{a}\cdot\bar{c}.$$

$\square$

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.

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

Def. Eine natürliche Zahl p ist genau dann eine <u>Primzahl</u>, wenn $p > 1$ ist und keine $r, s \in \mathbb{N}$ mit $p = rs$ und $r, s < p$ existieren.

Beweis von Satz 5.12. Sei $n \in \mathbb{N}$.

<u>Beh.</u>: $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ ist Körper $\iff$ n ist eine Primzahl

„$\Longleftarrow$" zu zeigen: $(\mathbb{Z}/n\mathbb{Z})^\times = \mathbb{Z}/n\mathbb{Z} \setminus \{0 + n\mathbb{Z}\}$

„$\supseteq$" Sei $a + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ vorgeg. (mit $a \in \mathbb{Z}$), wobei $a + n\mathbb{Z} \neq 0 + n\mathbb{Z}$. z.zg: $a + n\mathbb{Z}$ ist invertierbar

„⇐" Sei $a+n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$ vorgeg. (mit $a \in \mathbb{Z}$), wobei $a+n\mathbb{Z} \neq 0+n\mathbb{Z}$. z.zg.: $a+n\mathbb{Z}$ ist invertierbar

Wegen $a+n\mathbb{Z} \neq 0+n\mathbb{Z}$ gilt $n \nmid a$ (n kein Teiler von a), denn: Ang. $n \mid a$ $\Rightarrow \exists k \in \mathbb{Z}$ mit $a = kn \Rightarrow a-0 = kn$ (durch n teilbar) $\Rightarrow a+n\mathbb{Z} = 0+n\mathbb{Z}$ ↯ zur Vor.

Weil n eine Primzahl ist, folgt aus $n \nmid a$, dass n und a teilerfremd sind. Lemma von Bézout $\Rightarrow \exists k, l \in \mathbb{Z}$ mit

$$ka + ln = 1 \Rightarrow (ka+ln)+n\mathbb{Z} = 1+n\mathbb{Z} \Rightarrow$$

$$(ka+n\mathbb{Z}) + (ln+n\mathbb{Z}) = 1+n\mathbb{Z} \Rightarrow$$

$$(k+n\mathbb{Z})(a+n\mathbb{Z}) + (l+n\mathbb{Z})\cdot(n+n\mathbb{Z}) = 1+n\mathbb{Z} \Rightarrow$$

$$(k+n\mathbb{Z})\cdot(a+n\mathbb{Z}) + (l+n\mathbb{Z})\cdot(0+n\mathbb{Z}) = 1+n\mathbb{Z} \Rightarrow$$

$$\Rightarrow (k+n\mathbb{Z})\cdot(a+n\mathbb{Z}) + (0+n\mathbb{Z}) = 1+n\mathbb{Z} \Rightarrow$$

$$(k+n\mathbb{Z})\cdot(a+n\mathbb{Z}) = 1+n\mathbb{Z} \Rightarrow a+n\mathbb{Z} \text{ ist invertierbar}$$

(mit $k + n\mathbb{Z}$ als Kehrwert), liegt also in $(\mathbb{Z}/n\mathbb{Z})^\times$.

noch z.zg.: $0 + n\mathbb{Z}$ ist nicht invertierbar

Ang. $0 + n\mathbb{Z}$ ist invertierbar $\Rightarrow \exists\, c + n\mathbb{Z}$

mit $(0 + n\mathbb{Z}) \cdot (c + n\mathbb{Z}) = 1 + n\mathbb{Z}$ (wobei $c \in \mathbb{Z}$)

$\Rightarrow 0 + n\mathbb{Z} = 1 + n\mathbb{Z} \Rightarrow 1 - 0$ teilbar durch n

$\Rightarrow n \mid 1 \Rightarrow n = 1$ ↯ da n Primzahl

„$\Rightarrow$" Vor.: $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ ist ein Körper

z.zg.: n ist eine Primzahl

Ang.: n ist keine Primzahl $\Rightarrow$ zwei Möglichk.:

(1) $n=1$ (2) $\exists r,s \in \mathbb{N}$ mit $n = rs$, $r,s < n$

zu (1) $n=1 \Rightarrow n \mid (1-0) \Rightarrow 0+n\mathbb{Z} = 1+n\mathbb{Z}$

$\Rightarrow 0+n\mathbb{Z} \in (\mathbb{Z}/n\mathbb{Z})^\times$ Aber das Nullelement in einem Körper ist niemals invertierbar.

zu (2) Seien $r,s \in \mathbb{N}$ wie ang. Betrachte $\bar{a} = r+n\mathbb{Z}$ und $\bar{b} = s+n\mathbb{Z} \Rightarrow \bar{a}\cdot\bar{b} = (r+n\mathbb{Z})\cdot(s+n\mathbb{Z}) =$

$rs+n\mathbb{Z} = n+n\mathbb{Z} = 0+n\mathbb{Z} \xRightarrow{\mathbb{Z}/n\mathbb{Z} \text{ Körper}}$

$\bar{a} = \bar{0}$ oder $\bar{b} = \bar{0}$. aber: $0 < r < n \Rightarrow$

$r-0$ nicht teilbar durch $n \Rightarrow \bar{a} = r+n\mathbb{Z} \neq 0+n\mathbb{Z}$

ebenso: $\bar{b} = s+n\mathbb{Z} \neq 0+n\mathbb{Z}$ ↯ $\square$

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.

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 $1 \leq j \leq n$

Beispiele für Matrizen:

(1)

$$O^{(2\times 3)} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

$a_{11} = 0,\ a_{12} = 0,\ a_{13} = 0$

$a_{21} = 0,\ a_{22} = 0,\ a_{23} = 0$

$$O^{(3\times 2)} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$$

$a_{11} = 0,\ a_{12} = 0$

$a_{21} = 0,\ a_{22} = 0$

$a_{31} = 0,\ a_{32} = 0$

$= a_{\circ 1}$

(2)

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

(3)

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

$k=2,\ l=3$

$$b_{ij} = \delta_{i2}\,\delta_{j3} = \begin{cases} 1 & \text{falls } i=2 \text{ und } j=3 \\ 0 & \text{sonst} \end{cases}$$