Wiederholungen

Primzahlen

- Primkörper: $p \in \mathbb{P}$, $\mathbb{F}_p := \mathbb{Z}_p$, $\mathbb{F}_2 = \{0,1\}$
- $\mathbb{C} = \mathbb{R}[X]/(X^2+1)$, $i := \overline{X}$, $i^2 = -1$

  $\mathbb{C} = \{a+bi \mid a,b \in \mathbb{R}\}$

  komplexe Konjugation

  $a = \mathrm{Re}(a+bi)$, $b = \mathrm{Im}(a+bi)$, $\overline{a+bi} = a-bi$

  $$(a+bi)(c+di) = ac + adi + bci + bdi^2$$
  $$= ac - bd + (ad+bc)i.$$

- $\mathbb{F}_4 = \mathbb{F}_2[X]/(X^2+X+1)$.
- Euler-Funktion: $\varphi : \mathbb{N} \to \mathbb{N}$, $n \mapsto |(\mathbb{Z}_n)^\times|$

  $\varphi(n) = |\{d \mid 1 \le d \le n,\ \mathrm{ggT}(d,n) = 1\}|$

  $\varphi(mn) = \varphi(m)\cdot\varphi(n)$, falls $\mathrm{ggT}(m,n) = 1$.

$\varphi(p) = p-1$ für $p \in \mathbb{P}$

- Satz von Euler: $n \in \mathbb{N}$, $a \in \mathbb{Z}$ mit $ggT(a,n) = 1$

$$\Rightarrow \quad a^{\varphi(n)} \equiv_n 1$$

- Kleiner Fermat: $p \in \mathbb{P}$, $a \in \mathbb{Z}$ mit $p \nmid a$.

$$\Rightarrow \quad a^{p-1} \equiv_p 1 .$$

$n \in \mathbb{N}$ $\quad S_n := \{ \pi : \underline{n} \to \underline{n} \mid \pi \text{ bijektiv} \}$

Permutationen

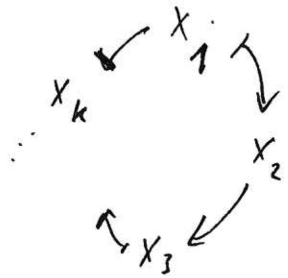
- S_n Gruppe mit „$\circ$"
- $|S_n| = n!$

- $\pi \in S_n$: $T_\pi = \{ i \in \underline{n} \mid \pi(i) \neq i \}$

  $\pi(T_\pi) = T_\pi$, $\pi(\underline{n} \setminus T_\pi) = \underbrace{\underline{n} \setminus T_\pi}_{\text{Fixpunkte von } \pi.}$

- $\varphi, \psi \in S_n$, $T_\varphi \cap T_\psi = \emptyset \implies \varphi \circ \psi = \psi \circ \varphi$.

- k- Zykel $(x_1, x_2, \dots, x_k)$



$(1,2,3) =$
$(2,3,1) =$
$(3,1,2)$

  2 - Zykel $(a,b) = (b,a)$

  Transposition

$(1,2)(2,3) = (1,2,3)$ $\qquad$ $(2,3)(1,2) = (1,3,2)$

$(x_1, x_2, \dots, x_k) = (x_1, x_2)(x_2, x_3) \dots (x_{k-1}, x_k)$

$(x_1, x_2, \dots, x_k)^{-1} = (x_k, x_{k-1}, \dots, x_2, x_1)$

Jedes $\pi \in S_n$ ist Produkt von disjunkten Zykeln.

<u>Beweis</u>: Induktion über $|T_\pi|$. $|T_\pi| = 0 \Rightarrow \pi = id$

$T_\pi \neq \emptyset$: Wähle $x_1 \in T_\pi$ und betrachte Folge

$x_1, x_2 = \pi(x_1), x_3 = \pi(x_2) = \pi(\pi(x_1)) = \pi^2(x_1), \ldots, x_i = \pi^i(x_1), \ldots$

$\Rightarrow$ es ex. i, j mit $1 \leq i < j \leq n$ mit $\pi^i(x_1) = \pi^j(x_1)$

$\Rightarrow$ $x_1 = \pi^k(x_1)$ mit $k = j - i$.

$\Rightarrow$ $\sigma := (x_1, x_2, \ldots, x_k)$ k-Zykel

Sei $B := T_\pi \setminus \{x_1, \ldots, x_k\}$; $\pi(B) = B$

1. $B = \emptyset \Rightarrow \pi = \sigma$ ✓

2. $B \neq \emptyset$: Betrachte $\pi' := \pi_B : B \to B$,

$T_{\pi'} = B$, $|T_{\pi'}| < |T_\pi|$ ✓ $\blacksquare$

Zykel (Forts.)

Beispiel

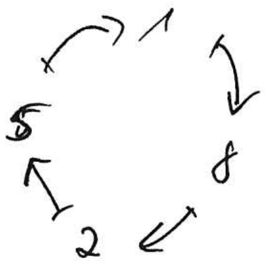
$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 5 & 8 & 3 & 6 & 2 & 7 & 4 & 1 & 9 & 11 & 10 \end{pmatrix} =$$

$(1,5,2,8)(3)(4,6,7)(9)(10,11) = (1,5,2,8)(4,6,7)(10,11)$.

Zykel (Forts.)

Die Zykelschreibweise lässt sich besonders leicht „potenzieren“.

Beispiel



$$
\begin{aligned}
\pi &= (10,11)(7,6,4)(8,2,5,1),\\
\pi^2 &= (1,2)(5,8)(4,6,7),\\
\pi^3 &= (1,5,2,8)(10,11),\\
\pi^4 &= (4,7,6)\\
&\vdots\\
\pi^{11} &= (1,5,2,8)(4,6,7)(10,11) = \pi^{-1}\\
\pi^{12} &= \mathrm{id}.
\end{aligned}
$$

Zykel (Forts.)

Erinnerung

Jeder Zykel ist Produkt von Transpositionen.

Proposition

$(i, i+1)$ $\quad 1 \leq i < n$

Jede Transposition in S_n ist Produkt von Nachbartranspositionen.

(i, j), $i < j$: $\quad \underbrace{(j, j-1)(j-1, j-2)\cdots}_{j-i-1}(i+1, i)\underbrace{(i+2, i+1)\cdots(j, j-1)}_{j-i-1}$

Beispiele

- $(1,4,7,3,5)(2,8,6,9) = \left[(1,4)(4,7)(7,3)(3,5)\right]\left[(2,8)(8,6)(6,9)\right]$
- $(1,4) = (4,3)(3,2)(1,2)(2,3)(3,4)$

Signum

Für $n \in \mathbb{N}$ sei $I_n := \{\{i,j\} \mid 1 \leq i,j \leq n, i \neq j\}$.

Definition

Sei $\pi \in S_n$. Das *Signum* von π ist definiert als

$$\operatorname{sgn} \pi := \prod_{\{i,j\} \in I_n} \frac{\pi(i) - \pi(j)}{i - j}. \qquad \in \mathbb{Q}$$

Bemerkung

- $\operatorname{sgn} \pi \in \{1, -1\}$ für alle $\pi \in S_n$.
- $\operatorname{sgn} \mathrm{id}_{\underline{n}} = 1$.

$I_n = \{\{i,j\} \mid 1 \leq i \neq j \leq n\} = I_n = \{\{\pi(i), \pi(j)\} \mid 1 \leq i \neq j \leq n\}$

$\Rightarrow \quad \operatorname{sgn} \pi \in \{1, -1\}$

$\operatorname{sgn} \pi$ ist wohldefiniert: $\quad \dfrac{\pi(i) - \pi(j)}{i-j} = \dfrac{\pi(j) - \pi(i)}{j-i}$

Signum (Forts.)

Produktsatz

Es seien $n \in \mathbb{N}$, $\pi, \sigma \in S_n$. Dann gilt:

$$\operatorname{sgn}(\pi\sigma) = (\operatorname{sgn}\pi)(\operatorname{sgn}\sigma)$$

<u>Beweis:</u> $\operatorname{sgn}(\pi\sigma) = \prod_{\{i,j\} \in I_n} \dfrac{\pi(\sigma(i)) - \pi(\sigma(j))}{i-j}$ $\qquad I_n = \{\{\sigma(i), \sigma(j)\} \mid 1 \leq i \neq j \leq n\}$

$$= \prod_{\{i,j\} \in I_n} \left(\frac{\pi(\sigma(i)) - \pi(\sigma(j))}{\sigma(i) - \sigma(j)} \cdot \frac{\sigma(i) - \sigma(j)}{i-j} \right)$$

$$= \prod_{\{i,j\} \in I_n} \frac{\pi(\sigma(i)) - \pi(\sigma(j))}{\sigma(i) - \sigma(j)} \cdot \prod_{\{i,j\} \in I_n} \frac{\sigma(i) - \sigma(j)}{i-j} = (\operatorname{sgn}\pi) \cdot (\operatorname{sgn}\sigma)$$

Signum (Forts.)

Proposition

Es sei $\tau = (a, b)$ eine Transposition in S_n.

Dann ist $\operatorname{sgn} \tau = -1$.

Beweis der Proposition: $\quad \pi = (a,b)$ Transposition

$$\operatorname{sgn} \pi = \prod_{\{i,j\}} \frac{\pi(i) - \pi(j)}{i-j} = \mathrm{I} \cdot \mathrm{II} \cdot \mathrm{III} \cdot \mathrm{IV}$$

$\mathrm{I}: \{i,j\} = \{a,b\} \qquad \dfrac{\pi(a) - \pi(b)}{a-b} = \dfrac{b-a}{a-b} = -1.$

$\mathrm{II}: \{i,j\} \cap \{a,b\} = \{a\} \qquad n-2$ solcher Mengen $\{i,j\}$

$i = a, \; j \neq a,b$

$$\frac{\pi(i) - \pi(j)}{i-j} = \frac{b-j}{a-j}$$

$\mathrm{III}: \{i,j\} \cap \{a,b\} = \{b\} \qquad n-2$ solcher Mengen $\{i,j\}$

$$\frac{\pi(i) - \pi(j)}{i-j} = \frac{a-j}{b-j}$$

$i = b, \; j \neq a,b$

$$\Rightarrow \prod_{\{i,j\} \in \mathrm{II}} \frac{\pi(i) - \pi(j)}{i-j} \cdot \prod_{\{i,j\} \in \mathrm{III}} \frac{\pi(i) - \pi(j)}{i-j} = 1.$$

$\mathrm{IV}: \{i,j\} \cap \{a,b\} = \emptyset \quad \rightsquigarrow \quad 1.$ $\blacksquare$

Signum (Forts.)

Korollar

Es sei $n \in \mathbb{N}$. Dann gilt:

(a) ▶ $\operatorname{sgn} \pi^{-1} = \operatorname{sgn} \pi$ für alle $\pi \in S_n$.

(b) ▶ Ist $\pi = \tau_1 \tau_2 \cdots \tau_r$ mit Transpositionen $\tau_i \in S_n$, dann ist $\operatorname{sgn} \pi = (-1)^r$.

(c) ▶ Ist $\pi \in S_n$ ein k-Zykel, dann ist $\operatorname{sgn} \pi = (-1)^{k-1}$.

<u>Beweis von (a)</u>: $1 = \operatorname{sgn} \mathrm{id} = \operatorname{sgn}(\pi \pi^{-1}) = \operatorname{sgn} \pi \cdot \operatorname{sgn}(\pi^{-1})$

11. Dezember 2018

Matrixarithmetik

Matrizen

Setup

- R kommutativer Ring mit $1 \neq 0$, d.h. $R \neq \{0\}$.
- $m, n \in \mathbb{N}$

R ist z.B. ein Körper $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_4$, ...

oder $R = \mathbb{Z}$, oder $R = K[X]$, K Körper

Matrizen (Forts.)

Definition

Eine $(m \times n)$-*Matrix A über R* ist ein rechteckiges „Schema“ von $m \cdot n$ Elementen $a_{ij} \in R$ der Form

$$A = \begin{array}{cl} \begin{array}{cc} \text{1. Spalte} & \text{2. Spalte} \end{array} & \\ \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & & & \vdots \\ a_{m1} & a_{m2} & \cdots & a_{mn} \end{pmatrix} & \begin{array}{l} \leftarrow \text{1. Zeile} \\ \leftarrow \text{2. Zeile} \\ \cdot \\ \leftarrow \text{m. Zeile} \end{array} \end{array}$$

Alternative Schreibweise: $A = (a_{ij})_{\substack{1 \leq i \leq m, \\ 1 \leq j \leq n}}$ oder $A = (a_{ij}) \in R^{m \times n}$

Die a_{ij} heißen die *Koeffizienten* oder *Einträge* von A.

$R^{m \times n}$: Menge der $(m \times n)$-Matrizen über R

Matrizen (Forts.)

Beispiele

- $\begin{pmatrix} 1 & -1 & 2 \\ 0 & -2 & 3 \end{pmatrix} \in \mathbb{Z}^{2\times 3}$
- $\begin{pmatrix} \frac{1}{2} & \frac{12}{5} & 3 & 8 \\ -7 & 0 & \frac{3}{4} & 0 \\ -2 & 4 & 5 & 0 \end{pmatrix} \in \mathbb{Q}^{3\times 4}$
- $\begin{pmatrix} X^2 - 1 & X^3 + X + 1 & \frac{4}{5}X \\ \frac{16}{7}X^6 - 1 & 2X^2 + 2X + 3 & 0 \\ 3 & \frac{1}{9}X^5 + \frac{1}{3}X & -1 \end{pmatrix} \in \mathbb{Q}[X]^{3\times 3}$
- $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} \in \mathbb{Z}^{1\times 6}$
- $\begin{pmatrix} 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} \in \mathbb{Z}^{4\times 1}$

Matrizen (Forts.)

Definitionen

Es sei $A = (a_{ij}) \in R^{m \times n}$.

- Die $(1 \times n)$-Matrix $z_i := \begin{pmatrix} a_{i1} & a_{i2} & \dots & a_{in} \end{pmatrix}$ heißt i-te *Zeile* von A.
- Die $(m \times 1)$-Matrix $s_j := \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix}$ heißt j-te *Spalte* von A.

  Zeilen-Vektor
- Eine $(1 \times n)$-Matrix wird auch (Zeilen-)n-Tupel genannt.

  Spalten-Vektor
- Eine $(m \times 1)$-Matrix wird (Spalten-)m-Tupel genannt.
- Wir setzen $R^n := R^{n \times 1}$.

Matrizen (Forts.)

Beispiele

- $A = \begin{pmatrix} 1 & -1 & 2 \\ 0 & -2 & 3 \end{pmatrix} \in \mathbb{Z}^{2\times 3}$

  Zeilen von A:

  1. Zeile: $(1 \;\; -1 \;\; 2) \in \mathbb{Z}^{1\times 3}$

  2. Zeile: $(0 \;\; -2 \;\; 3) \in \mathbb{Z}^{1\times 3}$

  Spalten von A:

  1. Spalte: $\begin{pmatrix} 1 \\ 0 \end{pmatrix} \in \mathbb{Z}^{2\times 1}$, 2. Spalte: $\begin{pmatrix} -1 \\ -2 \end{pmatrix} \in \mathbb{Z}^{2\times 1}$, 3. Spalte: $\begin{pmatrix} 2 \\ 3 \end{pmatrix} \in \mathbb{Z}^{2\times 1}$.

- $\underbrace{\begin{pmatrix} 2 \\ 4 \\ 5 \end{pmatrix}}_{\in \mathbb{Z}^{3\times 1}} \neq \underbrace{(2 \;\; 4 \;\; 5)}_{\in \mathbb{Z}^{1\times 3}}$.

Matrizen (Forts.)

Bemerkung

Eine $(m \times n)$-Matrix $A = (a_{ij})$ über R kann als Abbildung

$$a : \underline{m} \times \underline{n} \to R, (i,j) \mapsto a(i,j) := a_{ij}$$

aufgefasst werden (vgl. Definition von Tupeln).

Bemerkung

Zwei Matrizen $A = (a_{ij}) \in R^{m \times n}$ und $A' = (a'_{ij}) \in R^{m' \times n'}$ sind genau dann gleich, geschrieben $A = A'$, wenn gilt:

- $m = m'$ und $n = n'$;
- $a_{ij} = a'_{ij}$ für alle $1 \leq i \leq m$ und alle $1 \leq j \leq n$.

Matrixaddition

Proposition $A = (a_{ij}) \in R^{m\times n}$, $B = (b_{ij}) \in R^{m\times n}$

$R^{m\times n}$ wird abelsche Gruppe mit:

- Addition: $A+B := (a_{ij}+b_{ij})_{\substack{1\le i\le m,\\ 1\le j\le n}}$, $A+B \in R^{m\times n}$
- Null: $0 \in R^{m\times n}$: $0 = (a_{ij}) \in \underline{\underline{R^{m\times n}}}$ mit $a_{ij} = 0$ $\forall 1\le i\le m, 1\le j\le n$.
- Negative: $-A = (-a_{ij})_{\substack{1\le i\le m,\\ 1\le j\le n}} \in R^{m\times n}$

Matrixaddition (Forts.)

Beispiele

In $\mathbb{Z}^{2\times 3}$:

- $\begin{pmatrix} 1 & 0 & -2 \\ 2 & -1 & 3 \end{pmatrix} + \begin{pmatrix} -2 & 2 & 4 \\ 1 & 1 & -1 \end{pmatrix} = \begin{pmatrix} -1 & 2 & 2 \\ 3 & 0 & 2 \end{pmatrix}$
- $0 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$
- $-\begin{pmatrix} 1 & 0 & -2 \\ 2 & -1 & 3 \end{pmatrix} = \begin{pmatrix} -1 & 0 & 2 \\ -2 & 1 & -3 \end{pmatrix}$

Multiplikation von Matrizen mit Skalaren

Definition Skalar := Element von R

$c \in R$, $A \in R^{m\times n}$ $\qquad A = (a_{ij}) \in R^{m\times n}$

c-faches von A:

$$cA = c \cdot A = (c \cdot a_{ij})_{\substack{1\le i\le m,\\ 1\le j\le n}} \in R^{m\times n}$$

Beispiel

In $\mathbb{Z}^{2\times 3}$:

$$(-3)\begin{pmatrix}1 & 0 & -2\\ 2 & -1 & 3\end{pmatrix} = \begin{pmatrix}-3 & 0 & 6\\ -6 & 3 & -9\end{pmatrix}$$

Skalarmultiplikation von Matrizen (Forts.)

Proposition

Es seien $c, d \in R$, $A, B \in R^{m \times n}$

- $c(dA) = (cd)A$
- $1A = A$
- $(c+d)A = cA + dA$
  $c(A+B) = cA + cB$

Matrixmultiplikation

Definition

- $A \in R^{m \times n}$, $B \in R^{n \times l}$ $\quad A = (a_{ij}) \in R^{m \times n}, \quad B = (b_{ij}) \in R^{n \times l}$

  Matrixprodukt von A und B: $\quad A \cdot B \in R^{m \times l}$

  $$AB = A \cdot B = (c_{ij}) \in R^{m \times l} \text{ mit } c_{ij} = \sum_{k=1}^{n} a_{ik} \cdot b_{kj}$$

- *n-reihige Einheitsmatrix* über R:

  $$\mathrm{E}_n = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \vdots \\ \vdots & 0 & \ddots & 0 \\ 0 & \cdots & 0 & 1 \end{pmatrix} \in R^{n \times n}$$

Matrixmultiplikation (Forts.)

Beispiel (4×3) (3×2) (4×2)

- $\begin{pmatrix} 0 & -1 & 1 \\ 1 & 0 & 0 \\ 2 & 0 & 1 \\ -1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 0 & -1 \\ -2 & 3 \end{pmatrix} = \begin{pmatrix} -2 & 4 \\ 1 & 2 \\ 0 & 7 \\ -1 & -3 \end{pmatrix}$
- $\mathrm{E}_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$

Zur Matrix-Multiplikation: $A = (a_{ij}) \in R^{m \times n}$, $B = b_{ij} \in R^{n \times l}$

$z_1, \dots, z_m$ Zeilen von A, $s_1, \dots, s_l$ Spalten von B

Der Eintrag an der Position (i,j) in $A \cdot B$ ist der Eintrag

von $z_i \cdot s_j \in R^{1 \times 1}$

Matrixmultiplikation (Forts.)

Proposition

$A, A' \in R^{m\times n}$, $B, B' \in R^{n\times l}$, $C \in R^{l\times k}$

- $A(BC) = (AB)C$
- $\mathrm{E}_m A = A\mathrm{E}_n = A$
- $(A + A')B = AB + A'B$
  $A(B + B') = AB + AB'$
- $(cA)B = A(cB) = c(AB)$

Matrixmultiplikation (Forts.)

Korollar

$R^{n \times n}$ wird ein Ring mit:

- Multiplikation: $A \cdot B$ Matrixprodukt für $A, B \in R^{n \times n}$
- Eins: E_n

Bemerkung

$R^{n \times n}$ ist nicht kommutativ für $n \geq 2$.

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}; \quad \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$