Endliche Primkörper

Definition

$p \in \mathbb{P}$

Primkörper zu p: $\mathbb{F}_p := \mathbb{Z}/(p)$

Beispiel

- $\mathbb{F}_2 = \mathbb{Z}/(2) = \{\overline{0}, \overline{1}\}$

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

Endliche Primkörper (Forts.)

Unterdrücke den Querstrich in der Notation

- $\mathbb{F}_3 = \mathbb{Z}/(3) = \{0, 1, 2\}$

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

- $\mathbb{F}_5 = \mathbb{Z}/(5) = \{0, 1, 2, 3, 4\}$

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Restklassenkörper von Polynomringen

Beispiel

$\mathbb{R}[X]/(X^2+1)$ ist Körper

Definition

Körper der komplexen Zahlen: $\mathbb{C} := \mathbb{R}[X]/(X^2+1)$

Terminologien und Notationen:

- *komplexe Zahl*: Element von $\mathbb{C}$
- *imaginäre Einheit*: $\mathrm{i} := \overline{X} \in \mathbb{C}$

Restklassenkörper von Polynomringen (Forts.)

Bemerkung

- $\mathbb{C} = \{a + b\mathrm{i} \mid a, b \in \mathbb{R}\}$
- $a, b, a', b' \in \mathbb{R}$

  $a + b\mathrm{i} = a' + b'\mathrm{i} \Leftrightarrow a = a'$ und $b = b'$
- $a, b, c, d \in \mathbb{R}$

$$(a + b\mathrm{i}) + (c + d\mathrm{i}) = (a + c) \quad + (b + d) \quad \mathrm{i}$$
$$(a + b\mathrm{i}) \cdot (c + d\mathrm{i}) = (ac - bd) + (ad + bc)\mathrm{i}$$

Restklassenkörper von Polynomringen (Forts.)

Definition

$z \in \mathbb{C}$, $a, b \in \mathbb{R}$ mit $z = a + b\mathrm{i}$

- *Realteil* von z: $\quad \mathrm{Re}\, z := a$
- *Imaginärteil* von z: $\quad \mathrm{Im}\, z := b$

Beispiel

- $\mathrm{Re}(2 - \mathrm{i}) =$
- $\mathrm{Im}(2 - \mathrm{i}) =$

Restklassenkörper von Polynomringen (Forts.)

Definition

$z \in \mathbb{C}$

zu z *konjugierte komplexe Zahl*: $\quad \overline{z} := \mathrm{Re}\, z - (\mathrm{Im}\, z)\mathrm{i}$

Beispiel

$\overline{3 - 2\mathrm{i}} =$

Restklassenkörper von Polynomringen (Forts.)

Beispiel

- $\mathbb{F}_2[X]/(X^2+X+1)$ ist Körper
- $\mathbb{F}_2[X]/(X^3+X+1)$ ist Körper
- $\mathbb{F}_3[X]/(X^2+1)$ ist Körper

Notation

- $\mathbb{F}_4 := \mathbb{F}_2[X]/(X^2+X+1)$; $\alpha := \overline{X}$ in $\mathbb{F}_4$
- $\mathbb{F}_8 := \mathbb{F}_2[X]/(X^3+X+1)$; $\beta := \overline{X}$ in $\mathbb{F}_8$
- $\mathbb{F}_9 := \mathbb{F}_3[X]/(X^2+1)$; $\iota := \overline{X}$ in $\mathbb{F}_9$

Restklassenkörper von Polynomringen (Forts.)

Bemerkung

- $\mathbb{F}_4 = \{a + b\alpha \mid a, b \in \mathbb{F}_2\}$
- $a, b, a', b' \in \mathbb{F}_2$

  $a + b\alpha = a' + b'\alpha \Leftrightarrow a = a'$ und $b = b'$
- $a, b, c, d \in \mathbb{F}_2$

$$(a + b\alpha) + (c + d\alpha) = (a + c) \quad + (b + d) \qquad \alpha$$
$$(a + b\alpha) \cdot (c + d\alpha) = (ac + bd) + (ad + bc + bd)\alpha$$

Restklassenkörper von Polynomringen (Forts.)

$\mathbb{F}_4$

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

$\cdot$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

Euler-Funktion

Definition

Euler-Funktion:

$$\varphi : \mathbb{N} \to \mathbb{N},\ n \mapsto |(\mathbb{Z}_n)^\times|$$

Beispiel

$\varphi(8) =$

Euler-Funktion (Forts.)

Bemerkung

$\varphi(n) = |\{x \in \{0, 1, \ldots, n-1\} \mid \mathrm{ggT}(n, x) = 1\}|.$

Proposition

- $p, q \in \mathbb{P}$ mit $p \neq q$

$$\varphi(pq) = (p-1)(q-1)$$

- $p \in \mathbb{P}$

$$\varphi(p) = p - 1$$

Euler-Funktion (Forts.)

Lemma

G endliche abelsche Gruppe, $x \in G$

$$x^{|G|} = 1$$

Euler-Funktion (Forts.)

Satz von Euler

$n \in \mathbb{N}$, $a \in \mathbb{Z}$ mit $\mathrm{ggT}(n, a) = 1$

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

Kleiner Satz von Fermat

$p \in \mathbb{P}$, $a \in \mathbb{Z}$

$$a^{p-1} \equiv_p 1$$

6. Dezember 2018

Die symmetrische Gruppe

Symmetrische Gruppe

Erinnerung

Es sei A eine Menge.

$\mathrm{Abb}(A, A)$ ist Monoid mit Verknüpfung

$$(g, f) \mapsto g \circ f = gf$$

(Komposition von Abbildungen).

Symmetrische Gruppe (Forts.)

Definition

- Es sei A eine Menge.
  - *Symmetrische Gruppe* auf A:

    $$S_A := \mathrm{Abb}(A, A)^\times$$

  - *Permutation* von A: Element von S_A

- Es sei $n \in \mathbb{N}_0$.

  Symmetrische Gruppe vom Grad n:

  $$S_n := S_{\underline{n}}$$

Symmetrische Gruppe (Forts.)

Notation

Für $\pi \in S_A$:

$$\pi = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ \pi(a_1) & \pi(a_2) & \cdots & \pi(a_n) \end{pmatrix}.$$

Für $\pi \in S_n$:

$$\pi = \begin{pmatrix} 1 & 2 & \cdots & n \\ \pi(1) & \pi(2) & \cdots & \pi(n) \end{pmatrix}.$$

Meistens lassen wir das Zeichen „$\circ$“ für die Verknüpfung weg.

Symmetrische Gruppe (Forts.)

Beispiele

- $S_0 =$
- $S_1 =$
- $S_2 =$
- $S_3 =$

Beispiele

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} =$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} =$$

Symmetrische Gruppe (Forts.)

Definition

Für $n \in \mathbb{N}_0$ ist $n! \in \mathbb{N}$, gesprochen „*n Fakultät*“, definiert durch

$$0! := 1,$$

$$n! := \prod_{i=1}^{n} i = 1 \cdot 2 \cdot 3 \cdots n$$

für $n > 0$.

Proposition

Für $n \in \mathbb{N}_0$ ist $|S_n| = n!$.

Träger einer Permutation

Definition

Für $\pi \in S_A$ heißt

$$T_\pi := \{a \in A \mid \pi(a) \neq a\} \subseteq A$$

der *Träger* von π.

Beispiel

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

$$T_\pi = \{1, 2, 4, 5, 6, 7, 8, 10, 11\}.$$

Träger einer Permutation (Forts.)

Bemerkung

Es seien $\pi, \psi \in S_A$.

- $\pi(T_\pi) = T_\pi$.
- Gilt $T_\pi \subseteq B$, so kann π auch als Element von S_B aufgefasst werden.
- Haben π und ψ disjunkte Träger, so gilt $\pi \circ \psi = \psi \circ \pi$.

Zykel

Definition

Es seien $x_1, x_2, \ldots, x_k \in A$ paarweise verschieden.
$\sigma \in S_A$ mit

$$\sigma(x) = \begin{cases} x_{i+1} & \text{falls } x = x_i \text{ und } i < k, \\ x_1 & \text{falls } x = x_k, \\ x & \text{falls } x \neq x_1, x_2, \ldots, x_k, \end{cases}$$

heißt *Zykel der Länge k* oder kurz *k-Zykel* von S_A.
Schreibweise:

$$\sigma = (x_1, x_2, \ldots, x_k).$$

Die 2-Zykel heißen auch *Transpositionen* von S_A.

Zykel (Forts.)

Beispiele

- Der 4-Zykel $\sigma := (1, 5, 2, 4) \in S_5$ ist die Permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 1 & 2 \end{pmatrix}.$$

- $(1, 2, 3, 4, 5)(2, 1)(5, 4) =$
- $(1, 2)(2, 3) =$
- $(1, 2, 3)(3, 2, 1) =$

Zykel (Forts.)

Bemerkung

- Es gilt stets $(x_1, x_2, \ldots, x_k)^k = \mathrm{id}$.
- Es gilt stets $(x_1, x_2, \ldots, x_k)^{-1} = (x_k, x_{k-1}, \ldots, x_1)$.
- Für Transpositionen τ gilt $\tau^{-1} = \tau$.
- Jeder 1-Zykel ist die Identität.
- Jeder k-Zykel läßt sich als Produkt von $k-1$ Transpositionen schreiben:

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

Eine solche Zerlegung ist im Allgemeinen nicht eindeutig.

Zykel (Forts.)

Satz

Jede Permutation $\pi \in S_A$ läßt sich als Produkt von Zykeln schreiben, deren Träger paarweise disjunkt sind.

Eindeutigkeit: Bis auf Reihenfolge der Faktoren.

Sprechweise: Zerlegung von π in *paarweise disjunkte Zykeln*.

Konvention: Lasse 1-Zykel weg.

Zykel (Forts.)

Beispiel

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