Primkörper

Für jede Primzahl p ist die Menge

$$\mathbb{Z}_p = \{0, 1, \ldots, p-1\}$$

ein Körper unter der Addition und Multiplikation modulo p.
Allgemeiner existieren endliche Körper mit p^k Elementen für jedes $k \in \mathbb{N}$, die sogenannten Galois-Körper. Dies sind die einzigen Körper mit endlich vielen Elementen.

Beweis

Rechenregeln für Addition und Multiplikation in Körpern gelten in den ganzen Zahlen

$\rightsquigarrow$ Gültigkeit der Rechenregeln für $\mathbb{Z}_p$

$\rightsquigarrow$ noch zu zeigen: Existenz eines inversen Elementes a^{-1} für $a \in \{2, \ldots, p-1\}$

betrachte dazu die Folge

$$a^k \bmod p, \quad k = 0, \ldots, p-1$$

$a^k \neq 0 \bmod p \, \forall k \in \mathbb{N}$, denn

$$a^k = np \implies p \text{ teilt } a^k \underset{p \text{ Primzahl}}{\implies} p \text{ teilt } a \implies \text{Widerspruch zu } a < p$$

$\implies$ mindestens ein Rest tritt zweimal auf:

$$a^{k_1} = a^{k_2} \bmod p, \quad k_1 < k_2$$

$a^{k_1} a^{k_2 - k_1} = a^{k_1} \implies$

$$1 = a^{k_2 - k_1} \bmod p = a^{k_2 - k_1 - 1} a \bmod p \implies a^{-1} = a^{k_2 - k_1 - 1} \bmod p$$

Beispiel

Inverse Elemente im Primkörper $\mathbb{Z}_5$

$$2^{-1} \bmod 5 = 3, \quad 3^{-1} \bmod 5 = 2, \quad 4^{-1} \bmod 5 = 4$$

Überprüfung durch Multiplikation, z.B.

$$2 \cdot 2^{-1} \bmod 5 = 2 \cdot 3 \bmod 5 = 6 \bmod 5 = 1 \quad \checkmark$$

Illustration anhand des Distributivgesetzes

$$\begin{aligned} (2+4) \cdot 3^{-1} \bmod 5 &= 6 \cdot 2 \bmod 5 \\ &= 12 \bmod 5 = 2 \\ 2 \cdot 3^{-1} + 4 \cdot 3^{-1} \bmod 5 &= 2 \cdot 2 + 4 \cdot 2 \bmod 5 \\ &= 4 + 8 \bmod 5 = 12 \bmod 5 = 2 \end{aligned}$$

Beispiel

Paarungstabellen für Sportturniere

In Stuttgart, München und Berlin soll an 4 Terminen ein Turnier unter 9 Mannschaften ausgetragen werden. Dabei soll „jeder gegen jeden“ spielen. Es sind also an jedem Termin 3 Gruppen aus je 3 Mannschaften zu bilden, die jeweils in einer der Städte ihre Spiele untereinander austragen.

Mathematische Formulierung:

$$S_{0,k} \cup S_{1,k} \cup S_{2,k} = \{1, \ldots, 9\}, \qquad k = 0, \ldots, 3\,,$$
$$\mid S_{j,k} \cap S_{j',k'} \mid \leq 1,$$

mit drei-elementigen Mengen $S_{j,k}$, die jeweils der Dreiergruppe in der Stadt j am Termin k entsprechen. Die Bedingung an den Durchschnitt besagt, dass kein Mannschaftspaar doppelt vorkommt.

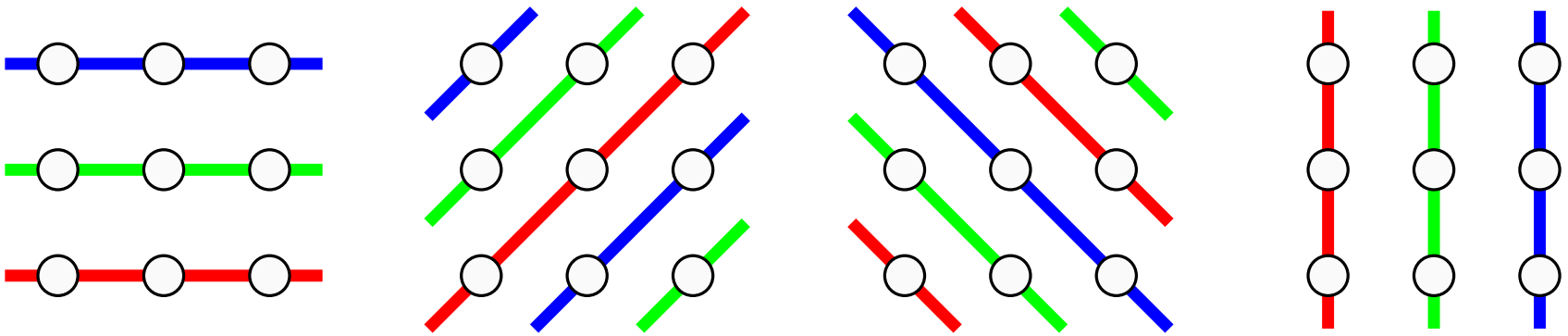
Konstruktion mit Hilfe des Primkörpers $\mathbb{Z}_3 = \{0, 1, 2\}$:
Identifikation der Mannschaften mit Punkten der Ebene $\mathbb{Z}_3^2$, d.h.

$$\{1, 2, ..., 9\} \quad \leftrightarrow \quad \{(x, y) : \ x, y \in \mathbb{Z}_3\}$$

und der Mengen $S_{j,k}$ mit den Geraden in $\mathbb{Z}_3$

$$\begin{aligned} S_{j,k} &= \{(x, k \cdot x + j \bmod 3) : \ x = 0, 1, 2\}, \quad \text{(Steigung } k = 0, 1, 2) \\ S_{j,3} &= \{(j, y) : \ y = 0, 1, 2\} \quad \text{(senkrechte Geraden)} \end{aligned}$$

Durchschnittsbedingung trivialerweise erfüllt: Geraden schneiden sich in höchstens einem Punkt



Paarungstabelle für 16 Mannschaften, 4 Städte und 5 Termine basierend auf 4-elementigen Galois-Körper GF[2^2]

	Spielort 1	Spielort 2	Spielort 3	Spielort 4
1. Spieltag	1,2,3,4	5,6,7,8	9,10,11,12	13,14,15,16
2. Spieltag	1,6,11,16	5,2,15,12	9,14,3,8	13,10,7,4
3. Spieltag	1,10,15,8	5,14,11,4	9,2,7,16	13,6,3,12
4. Spieltag	1,14,7,12	5,10,3,16	9,6,15,4	13,2,11,8
5. Spieltag	1,5,9,13	2,6,10,14	3,7,11,15	4,8,12,16

Galois-Körper GF[q] mit q einer Primzahlpotenz

$\rightsquigarrow$ Paarungstabelle für q^2 Mannschaften und q Städte