5.1 Gruppen und Körper

Gruppe

Menge G mit binärer Operation $\diamond : G \times G \longmapsto G$

- Assoziativität: $(a \diamond b) \diamond c = a \diamond (b \diamond c)$
- Neutrales Element: $\exists!\, e \in G$: $e \diamond a = a \diamond e = a$
- Inverses Element: $a \diamond a^{-1} = a^{-1} \diamond a = e$

kommutativ oder abelsch $\quad\Leftrightarrow\quad a \diamond b = b \diamond a$

Untergruppe

Teilmenge U einer Gruppe G

abgeschlossen unter der Gruppenoperation von G, d.h.

$$a, b \in U \quad\Longrightarrow\quad a \diamond b \in U, \qquad a \in U \quad\Longrightarrow\quad a^{-1} \in U$$

Permutationen und symmetrische Gruppe

Gruppe S_n der Bijektionen auf $\{1, 2, \ldots, n\}$

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \pi(1) & \pi(2) & \pi(3) & \ldots & \pi(n) \end{pmatrix}$$

$n!$ Elemente

Zyklenschreibweise von Permutationen

Zyklus: Bilder eines Elementes bei mehrfacher Ausführung der Permutation

$\rightsquigarrow$ Zerlegung von $\pi \in S_n$, z.B.

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 6 & 5 & 1 \end{pmatrix} \equiv (1\,4\,6)\ (2\,3)\ (5) \quad \text{bzw.} \quad \pi = (1\,4\,6)\ (2\,3)$$

Transposition und Signum einer Permutation

$\tau = (j\,k)$: Vertauschung von j und k

$\rightsquigarrow$ Produktdarstellung von Permutationen

$$\pi = \tau_1 \circ \cdots \circ \tau_m$$

Vorzeichen (Signum) einer Permutation: $\sigma(\pi) = (-1)^m$

Körper

Menge K, auf der eine Addition $+$ und eine Multiplikation $\cdot$ definiert sind

- $(K, +)$: abelsche Gruppe mit neutralem Element 0

$$\begin{aligned} a + b &= b + a \\ (a + b) + c &= a + (b + c) \\ a + 0 &= a \\ a + (-a) &= 0 \end{aligned}$$

- $(K \backslash \{0\}, \cdot)$: abelsche Gruppe mit neutralem Element 1

$$\begin{aligned} a \cdot b &= b \cdot a \\ (a \cdot b) \cdot c &= a \cdot (b \cdot c) \\ a \cdot 1 &= a \\ a \cdot a^{-1} &= 1 \end{aligned}$$

- Distributivgesetz: $a \cdot (b + c) = a \cdot b + a \cdot c$

Primkörper

$$\mathbb{Z}_p = \{0, 1, \ldots, p-1\}, \quad p: \text{ Primzahl}$$

Körper unter Addition und Multiplikation modulo p

Chinesischer Restsatz

Kongruenzen

$$\begin{aligned} x &= a_1 \bmod p_1 \\ &\cdots \\ x &= a_n \bmod p_n \end{aligned}$$

eindeutige Lösung $x \in \{0, \ldots, P-1\}$, $P = p_1 \cdots p_n$, für teilerfremde Zahlen $p_1, \ldots, p_n$

$$x = \sum_{k=1}^{n} a_k Q_k(P/p_k) \bmod P, \quad Q_k(P/p_k) = 1 \bmod p_k$$