Gruppen, Ringe und Körper

M sei eine Menge und $\circ$ eine zweistellige Operation (Abbildung von $M \times M$ in M).

Bezeichnung $(M, \circ)$, analog $(M, \circ, *)$ bei zwei Operationen.

Definition 1: $(M, \circ)$ ist eine Gruppe, wenn gilt:

(1) Die Operation $\circ$ ist assoziativ.

(2) Es gibt genau ein neutrales Element $e \in M$ mit $a \circ e = e \circ a = a$ (für alle $a \in M$).

(3) Es gibt zu jedem $a \in M$ genau ein inverses Element a^{-1} mit $a \circ a^{-1} = a^{-1} \circ a = e$.

Eine Gruppe heißt abelsch, wenn die Operation $\circ$ kommutativ ist.

Beispiel: Die Menge der regulären Matrizen vom Typ (n,n) bildet mit der Operation Matrizen-Multiplikation eine (nicht-abelsche) Gruppe.

Definition 2: $(M, \oplus, *)$ heißt Ring, wenn gilt:

(1) $(M, \oplus)$ ist eine abelsche Gruppe.

(2) Die Operation $*$ ist assoziativ.

(3) Es gelten die Distributivgesetze (für beliebige a, b, c $\in$ M):

$$a * (b \oplus c) = (a * b) \oplus (a * c) \quad \text{und} \quad (a \oplus b) * c = (a * c) \oplus (b * c).$$

Ein Ring heißt kommutativer Ring, wenn die Operation $*$ kommutativ ist.

Beispiel: Die Menge der quadratischen Matrizen vom Typ (n, n) bildet mit den Operationen Matrizen-Addition und -Multiplikation einen nicht-kommutativen Ring.

Definition 3: $(M, \oplus, *)$ heißt Körper, wenn gilt:

(1) $(M, \oplus, *)$ ist ein Ring (mit dem neutralen Element 0 für die Operation $\oplus$).

(2) $(M \setminus \{0\}, *)$ ist eine abelsche Gruppe (mit dem neutralen Element 1 für die Operation $\bullet$).

Beispiele:

1) Die rationalen Zahlen (Q), die reellen Zahlen (R) und die komplexen Zahlen (C) jeweils mit den üblichen arithmetischen Operationen Addition und Multiplikation.

2) Die Restklassenmenge Z_p (p ... Primzahl) mit den modularen Operationen Addition $\oplus$ und Multiplikation $\otimes$ **(s. Seite 2).**

Der Restklassenkörper Z_p

- **Es seien a und b ganze Zahlen und m > 0 eine natürliche Zahl. Es bedeute**

$a \equiv b \pmod m$ (lies: a kongruent b modulo m), dass a und b bei Division durch m den gleichen Rest besitzen.

Durch $(a, b) \in T :\Leftrightarrow a \equiv b \pmod m$ ist auf Z eine Äquivalenzrelation T erklärt. Äquivalenzklassen sind die Restklassen modulo m (Eine Restklasse enthält alle ganzen Zahlen, die bei Division durch den Modul m den gleichen Rest lassen.)

- **Es seien $a \in Z$ und $m \in N^*$. Dann gibt es eine eindeutige Darstellung von a der Gestalt $a = q \cdot m + r$ mit $0 \le r < m$ und $q \in Z$.**

Bezeichnungen: r ist der (kleinste nichtnegative) Rest, q ist der Quotient (größte ganze Zahl k, für die $k \cdot m$ kleiner oder gleich a ist) bei Division durch den Modul m.

- **Es seien $a \equiv b \pmod m$ und $c \equiv d \pmod m$, dann gelten auch**

$a + c \equiv b + d \pmod m$ und $a \cdot c \equiv b \cdot d \pmod m$, d. h.

in Summen und Produkten darf jede Zahl durch einen beliebigen Vertreter der gleichen Restklasse ersetzt werden.

- **Beispiel: Restklassen modulo 7**

Restklasse 0: {…, -21, -14, -7, 0, 7, 14, 21, 28, 35, …} = {7k + 0 | k ∈ Z},

Restklasse 1: {…, -20, -13, -6, 1, 8, 15, 22, 29, 36, …} = {7k + 1 | k ∈ Z},

Restklasse 2: {…, -19, -12, -5, 2, 9, 16, 23, 30, 37, …} = {7k + 2 | k ∈ Z},

…

Restklasse 6: {…, -15, -8, -1, 6, 13, 20, 27, 34, 41, …} = {7k + 6 | k ∈ Z}.

In der modularen Arithmetik werden die Restklassen mit den jeweils kleinsten nichtnegativen Vertretern identifiziert (im Beispiel 0, 1, 2, … , 6). Diese bilden die Restklassenmenge Z_m, hier $Z_7 = \{0, 1, 2, 3, 4, 5, 6\}$. Für Addition ⊕ und Multiplikation ⊗ ergeben sich in Z_7 folgende Rechentabellen:

⊕	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

⊗	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Wegen $3 \cdot 5 \equiv 1 \pmod 7$, d. h. $3 \otimes 5 = 1$ ist 5 in Z_7 die Inverse von 3: $3^{-1} = 5$.

- **Ist p eine Primzahl, so ist $(Z_p, \oplus, \otimes)$ ein Körper.**