## 6. Der Restklassenring $\mathbb{Z}_m$

**Definition:** Es sei $G \neq \emptyset$ eine Menge und $\cdot$ eine Verknüpfung auf $G$ (d.h. eine Abbildung $\cdot : G \times G \to G$). Dann heißt $(G, \cdot)$ abelsche Gruppe (oder auch kommutative Gruppe), wenn die folgenden Bedingungen erfüllt sind:

1) $\forall a,b,c \in G: (a \cdot b) \cdot c = a \cdot (b \cdot c)$ (Assoziativität)
2) $\exists e \in G \ \forall a \in G: e \cdot a = a \cdot e = a$ (neutrales Element)
3) $\forall a \in G \ \exists a^{-1} \in G: a \cdot a^{-1} = a^{-1} \cdot a = e$ (inverses Element)
4) $\forall a,b \in G: a \cdot b = b \cdot a$ (Kommutativität)

**Bemerkungen:** 1) Die Abgeschlossenheit (d.h. $a \cdot b \in G \ \forall a,b \in G$) ist in unserer Definition in der Forderung enthalten, dass $\cdot$ eine Verknüpfung ist.
2) Bei vielen abelschen Gruppen wird die Verknüpfung als Addition (d.h. $+$) geschrieben. Man schreibt dann in der Regel $0$ für das neutrale Element und $-a$ für das inverse Element von $a$. Die Axiome einer abelschen Gruppe lauten dann

1) $\forall a,b,c \in G: (a+b)+c = a+(b+c)$
2) $\exists 0 \in G \ \forall a \in G: 0+a = a+0 = a$
3) $\forall a \in G \ \exists -a \in G: a+(-a) = (-a)+a = 0$
4) $\forall a,b \in G: a+b = b+a$

**Beispiele:** 1) $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$ und $(\mathbb{C},+)$ sind abelsche Gruppen.
2) $(\{1,-1\},\cdot)$ (mit der Verknüpfung $1 \cdot 1 = (-1)\cdot(-1) = 1$, $1 \cdot (-1) = (-1) \cdot 1 = -1$), $(\mathbb{Q} \setminus \{0\},\cdot)$, $(\mathbb{R} \setminus \{0\},\cdot)$ und $(\mathbb{C} \setminus \{0\},\cdot)$ sind abelsche Gruppen. (Dabei ist $1$ neutrales Element und $a^{-1} = \frac{1}{a}$.)

**Definition:** Es sei $R \neq \emptyset$ eine Menge und $+$ und $\cdot$ zwei Verknüpfungen auf $R$. Dann heißt $(R,+,\cdot)$ kommutativer Ring mit $1$, wenn die folgenden Bedingungen erfüllt sind:

1) $(R,+)$ ist eine abelsche Gruppe
2.1) $\forall a,b,c \in R: (a \cdot b) \cdot c = a \cdot (b \cdot c)$ (Assoziativität der Multiplikation)
2.2) $\exists 1 \in R \ \forall a \in R: 1 \cdot a = a \cdot 1 = a$ (Einselement)
2.3) $\forall a,b \in R: a \cdot b = b \cdot a$ (Kommutativität der Multiplikation)
3.1) $\forall a,b,c \in R: (a+b) \cdot c = a \cdot c + b \cdot c$
3.2) $\forall a,b,c \in R: a \cdot (b+c) = a \cdot b + a \cdot c$
} (Distributivgesetze)

**Beispiele:** $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ und $(\mathbb{C},+,\cdot)$ sind kommutative Ringe mit Einselement.

**Definition:** Es sei $m \in \mathbb{N}$, $m \geq 2$. Wir bezeichnen die Menge aller Restklassen modulo $m$ mit $\mathbb{Z}_m$. Schreibt man kurz $[a]$ für die Restklasse $a + m\mathbb{Z}$, so ist also $\mathbb{Z}_m = \{[0], [1], \ldots, [m-1]\}$. Wir definieren Summe und Produkt zweier Restklassen $[a], [b] \in \mathbb{Z}_m$ durch $[a] + [b] := [a+b]$ und $[a] \cdot [b] := [a \cdot b]$.

**Bemerkung:** Diese Definitionen hängen nicht von der Wahl der Repräsentanten $a, b \in \mathbb{Z}$ ab. Ist $[a] = [c]$ und $[b] = [d]$, so ist $a \equiv c \,(m)$ und $b \equiv d \,(m)$ und daher $a + b \equiv c + d \,(m)$ und $a \cdot b \equiv c \cdot d \,(m)$ (nach Satz 39 (i) und (ii)). Daher ist $[a] + [b] = [a+b] = [c+d] = [c] + [d]$ und $[a] \cdot [b] = [a \cdot b] = [c \cdot d] = [c] \cdot [d]$.

**Satz 67** Es sei $m \in \mathbb{N}$, $m \geq 2$. Dann ist $(\mathbb{Z}_m, +, \cdot)$ ein kommutativer Ring mit 1.

**Beweis:** $([a] + [b]) + [c] = [(a+b)+c] = [a + (b+c)] = [a] + ([b] + [c])$ $\forall a, b, c \in \mathbb{Z}$

Alle übrigen Rechenregeln überprüft man völlig analog.

Nullelement (als neutrales Element der Addition) ist $[0] \in \mathbb{Z}_m$

Additives Inverses von $[a] \in \mathbb{Z}_m$ ist $-[a] = [-a] = [m-a] \in \mathbb{Z}_m$

Einselement ist $[1] \in \mathbb{Z}_m$.

**Beispiele:** 1) $m = 2$ Die Verknüpfungstafeln für Addition und Multiplikation sind

| + | [0] | [1] |
|---|---|---|
| [0] | [0] | [1] |
| [1] | [1] | [0] |

| · | [0] | [1] |
|---|---|---|
| [0] | [0] | [0] |
| [1] | [0] | [1] |

oder

| + | g | u |
|---|---|---|
| g | g | u |
| u | u | g |

| · | g | u |
|---|---|---|
| g | g | g |
| u | g | u |

wobei bei der 2. Version g und u für „gerade" und „ungerade" stehen

2) $m = 3$ Die Verknüpfungstafeln für Addition und Multiplikation sind

| + | [0] | [1] | [2] |
|---|---|---|---|
| [0] | [0] | [1] | [2] |
| [1] | [1] | [2] | [0] |
| [2] | [2] | [0] | [1] |

| · | [0] | [1] | [2] |
|---|---|---|---|
| [0] | [0] | [0] | [0] |
| [1] | [0] | [1] | [2] |
| [2] | [0] | [2] | [1] |

3) $m = 4$ Die Verknüpfungstafeln für Addition und Multiplikation sind

| + | [0] | [1] | [2] | [3] |
|---|---|---|---|---|
| [0] | [0] | [1] | [2] | [3] |
| [1] | [1] | [2] | [3] | [0] |
| [2] | [2] | [3] | [0] | [1] |
| [3] | [3] | [0] | [1] | [2] |

| · | [0] | [1] | [2] | [3] |
|---|---|---|---|---|
| [0] | [0] | [0] | [0] | [0] |
| [1] | [0] | [1] | [2] | [3] |
| [2] | [0] | [2] | [0] | [2] |
| [3] | [0] | [3] | [2] | [1] |

**Definition**: Es sei $(R,+,\cdot)$ ein kommutativer Ring mit 1. Ein $a \in R$ heißt invertierbar (oder Einheit) wenn es ein $a^{-1} \in R$ mit der Eigenschaft $a \cdot a^{-1} = a^{-1} \cdot a = 1$ gibt. Weiters verwenden wir die Bezeichnung $R^* = \{a \in R \mid a \text{ ist invertierbar}\}$ für die Menge aller Einheiten von $R$.

**Satz 68**: Es sei $(R,+,\cdot)$ ein kommutativer Ring mit 1. Dann ist $(R^*,\cdot)$ eine abelsche Gruppe.

**Beweis**: Es ist $R^* \neq \emptyset$, da $1 \in R^*$ (denn $1 \cdot 1 = 1$). Aus $a,b \in R^*$ folgt $a \cdot b \in R^*$ (da es gilt Abgeschlossenheit, da $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1} \in R$. Assoziativität und Kommutativität gelten allgemein. Neutrales Element ist $1 \in R^*$. Ist $a \in R^*$, so ist auch $a^{-1} \in R^*$, da $(a^{-1})^{-1} = a \in R^*$.

**Definition** Es sei $(R,+,\cdot)$ ein kommutativer Ring mit 1. Die Gruppe $(R^*,\cdot)$ wird als Einheitengruppe von $R$ bezeichnet

**Beispiele**: $\mathbb{Z}^* = \{-1,1\}$, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$

**Satz 69** Es sei $m \in \mathbb{N}$, $m \geq 2$.

(i) Ein $[a] \in \mathbb{Z}_m$ gilt $[a] \in \mathbb{Z}_m^* \iff [a]$ ist prime Restklasse,

(ii) $\mathbb{Z}_m^* = \{[a] \in \mathbb{Z}_m \mid [a] \text{ ist prime Restklasse}\}$,

(iii) $\varphi(m) = |\mathbb{Z}_m^*|$.

**Beweis**: (i) Folgt aus Satz 46 und Lemma 47

(ii) Folgt aus (i).

(iii) Folgt aus (ii) und der Definition der Eulerschen $\varphi$-Funktion (siehe die Bemerkung auf Seite 32).

**Definition**: Es sei $m \in \mathbb{N}$, $m \geq 2$. Dann wird $(\mathbb{Z}_m^*,\cdot)$ als prime Restklassengruppe modulo $m$ bezeichnet.

**Beispiele**: 1) $m = 2$, $\mathbb{Z}_2^* = \{[1]\}$ mit Verknüpfungstafel

| $\cdot$ | $[1]$ |
|---|---|
| $[1]$ | $[1]$ |

2) $m = 3$, $\mathbb{Z}_3^* = \{[1],[2]\}$ mit Verknüpfungstafel

| $\cdot$ | $[1]$ | $[2]$ |
|---|---|---|
| $[1]$ | $[1]$ | $[2]$ |
| $[2]$ | $[2]$ | $[1]$ |

3) $m = 4$, $\mathbb{Z}_4^* = \{[1],[3]\}$ mit Verknüpfungstafel

| $\cdot$ | $[1]$ | $[3]$ |
|---|---|---|
| $[1]$ | $[1]$ | $[3]$ |
| $[3]$ | $[3]$ | $[1]$ |

**Definition** Ein kommutativer Ring mit 1 $(K,+,\cdot)$ heißt Körper, wenn jedes $a \in K \setminus \{0\}$ invertierbar ist, d.h. wenn $K^* = K \setminus \{0\}$ gilt.

**Beispiele:** $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ und $(\mathbb{C},+,\cdot)$ sind Körper

**Definition:** Es sei $(R,+,\cdot)$ ein kommutativer Ring mit 1. Ein $a \in R$ heißt Nullteiler, wenn es ein $b \in R \setminus \{0\}$ mit der Eigenschaft $ab = ba = 0$ gibt.

**Beispiele** In $(\mathbb{Z},+,\cdot)$, $(\mathbb{Q},+,\cdot)$, $(\mathbb{R},+,\cdot)$ und $(\mathbb{C},+,\cdot)$ ist 0 der einzige Nullteiler.

**Satz 70** Es sei $m \in \mathbb{N}$, $m \geq 2$. Ist $[a] \in \mathbb{Z}_m$ keine prime Restklasse (d.h. $ggT(a,m) > 1$), so ist $[a]$ ein Nullteiler des Restklassenringes $(\mathbb{Z}_m,+,\cdot)$

**Beweis:** Es sei $d = ggT(a,m) > 1$. Dann ist $1 \leq \frac{m}{d} < m$ und daher $\left[\frac{m}{d}\right] \neq [0]$ und

$$[a] \cdot \left[\frac{m}{d}\right] = \left[\frac{a \cdot m}{d}\right] = \left[\frac{a}{d}\right] \cdot [m] = \left[\frac{a}{d}\right] \cdot [0] = [0].$$

**Lemma 71** Es sei $(R,+,\cdot)$ ein kommutativer Ring mit 1. Dann ist $0 \cdot a = a \cdot 0 = 0$ $\forall a \in R$

**Beweis:** $0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a$. Durch Addition von $-(0 \cdot a)$ erhält man $0 = 0 \cdot a$.

**Lemma 72** Es sei $(R,+,\cdot)$ ein kommutativer Ring mit 1. (und $1 \neq 0$). Ein Element $a \in R$ kann nicht zugleich Einheit und Nullteiler von $R$ sein. (D.h. $R^*$ und die Menge der Nullteiler von $R$ sind disjunkt.)

**Beweis:** Ist $a \in R^*$ und $b \in R$ hat die Eigenschaft $ab = ba = 0$, so folgt

$$b = b \cdot 1 = b \cdot (a \cdot a^{-1}) = (ba) \cdot a^{-1} = 0 \cdot a^{-1} \overset{\text{Lemma 71}}{=} 0.$$

**Satz 73** Es sei $m \in \mathbb{N}$, $m \geq 2$. Dann sind äquivalent:

(i) $m$ ist eine Primzahl,

(ii) $(\mathbb{Z}_m,+,\cdot)$ ist ein Körper.

**Beweis:** (i) $\Rightarrow$ (ii) Ist $m$ Primzahl, so ist $\mathbb{Z}_m^* = \{[1],[2],\dots,[m-1]\} = \mathbb{Z}_m \setminus \{[0]\}$ und $(\mathbb{Z}_m,+,\cdot)$ daher ein Körper

(ii) $\Rightarrow$ (i) Ist $m$ keine Primzahl, so gibt es ein $d \in \{2,\dots,m-1\}$ mit der Eigenschaft $d \mid m$. Dann ist $ggT(d,m) > 1$ und $[d]$ ist Nullteiler nach Satz 70. Wegen Lemma 72 ist $[d] \notin \mathbb{Z}_m^*$ und $(\mathbb{Z}_m,+,\cdot)$ daher kein Körper

30.6.2025