6. Endliche Gruppen

6.1. Eigenschaften einer Gruppe

Die Addition von Restklassen in $\mathbb{Z}_n$ wird durch die Angabe der Verknüpfungstafel vollständig beschrieben. Diese hat bestimmte Eigenschaften, die systematisch zusammengestellt werden sollen.

Bsp: $n = 4$

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Allgemein heißt ein geordnetes Tripel $(G, \circ, e)$ bestehend aus

(i) einer endlichen nichtleeren Menge G,

(ii) einer Verknüpfung $\circ : G \times G \to G$ und

(iii) einem Element $e \in G$

endliche kommutative Gruppe, wenn die folgenden Eigenschaften erfüllt sind:

(1) $\forall a \in G \; \forall b \in G \; \forall c \in G \; ((a \circ b) \circ c = a \circ (b \circ c))$

(2) $\forall a \in G \; \forall b \in G \; (a \circ b = b \circ a)$

(3) $\forall a \in G \; (a \circ e = e \circ a = a)$ "neutrales Element"

(4) $\forall a \in G \; \exists b \in G \; (a \circ b = b \circ a = e)$ "inverses Element"

Bsp: ◦) Für alle $n \in \mathbb{N} \setminus \{0\}$ ist $(\mathbb{Z}_n, +, 0)$ eine endliche kommutative Gruppe.

•) Für $n=3$ ist $(\mathbb{Z}_3\setminus\{0\}, \cdot, 1)$ eine endliche kommutative Gruppe mit Verknüpfungstafel:

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

•) Für $n=4$ ist $(\mathbb{Z}_4\setminus\{0\}, \cdot, 1)$ keine Gruppe:

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

Grund: Für $a=2$ gibt es kein $b\in\mathbb{Z}_4\setminus\{0\}$ mit $a\cdot b = 1$.

6.2. Die Eulersche φ-Funktion

Lemma: Für $a\in\mathbb{Z}_n\setminus\{0\}$ gibt es genau dann ein $b\in\mathbb{Z}_n\setminus\{0\}$ mit $a\cdot b = 1$, wenn $\operatorname{ggt}(a,n)=1$ ist.

Beweis: Wenn $\operatorname{ggt}(a,n)=1$ ist, dann gibt es $p,q\in\mathbb{Z}$ mit

$$1 = p\cdot a + q\cdot n.$$

Für $b=\overline{p}$ gilt dann $a\cdot b = 1$.

Wenn $\operatorname{ggt}(a,n)=d>1$ ist, dann gibt es $s,t\in\{1,2,\dots,n-1\}$ mit $s\cdot d = a$ und $t\cdot d = n$. Angenommen es gäbe $b\in\mathbb{Z}_n\setminus\{0\}$ mit $1 = a\cdot b$. Dann wäre

$$t = t\cdot a\cdot b = t\cdot s\cdot d\cdot b = s\cdot b\cdot n \equiv_n 0,$$ im

Widerspruch zu $t\in\{1,2,\dots,n-1\}$. ▨

Wir setzen $\mathbb{Z}_n^* = \{a\in\mathbb{Z}_n\setminus\{0\} : \operatorname{ggt}(a,n)=1\}$

Bsp: $\mathbb{Z}_{14}^* = \{1,3,5,9,11,13\}$

Folgerung: Für alle $n \in \mathbb{N} \setminus \{0,1\}$ ist $(\mathbb{Z}_n^*, \circ, 1)$ eine endliche kommutative Gruppe.

Bsp: $(\mathbb{Z}_4^*, \circ, 1)$ hat die Verknüpfungstafel:

$\circ$	1	3
1	1	3
3	3	1

Wir setzen $\varphi(n) = |\mathbb{Z}_n^*|$ ... Eulersche φ-Funktion

Es gilt:

(i) Für alle Primzahlen p ist $\varphi(p) = p-1$.

(ii) Für alle $n \in \mathbb{N} \setminus \{0,1\}$ ist $\varphi(n) = n \cdot \left(1-\frac{1}{p_1}\right) \cdot \left(1-\frac{1}{p_2}\right) \cdot \ldots \cdot \left(1-\frac{1}{p_k}\right)$,

wobei $p_1, p_2, \ldots, p_k$ diejenigen Primzahlen sind, die n teilen.

(iii) Für alle $n \in \mathbb{N} \setminus \{0,1\}$ und alle $a \in \mathbb{Z}_n^*$ gilt $a^{\varphi(n)} = 1$.

Bsp: •) $\varphi(15) = \varphi(3 \cdot 5) = 15\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 15 \cdot \frac{2}{3} \cdot \frac{4}{5} = 8$

•) $3^{17} \equiv_{14} 3^6 \cdot 3^6 \cdot 3^5 \equiv_{14} 1 \circ 1 \circ 3^5 \equiv_{14} 3^5$

6.3. Homomorphismen

Wir wollen beschreiben, dass z.B. die Verknüpfungstafeln von $(\mathbb{Z}_4, +, 0)$ und $(\mathbb{Z}_5^*, \circ, 1)$ im Wesentlichen gleich aufgebaut 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

$\circ$	1	2	4	3
1	1	2	4	3
2	2	4	3	1
4	4	3	1	2
3	3	1	2	4

Allgemein heißen zwei Gruppen $(G_1, \circ, e_1)$ und $(G_2, \circ, e_2)$ homomorph, wenn es eine surjektive Abbildung $f: G_1 \to G_2$ gibt, sodass $f(a \circ b) = f(a) \circ f(b)$ für alle $a, b \in G_1$ gilt. Ist f sogar bijektiv, so heißen die Gruppen isomorph. f heißt Homomorphismus bzw. Isomorphismus.

Bsp: •) $f: \mathbb{Z}_4 \to \mathbb{Z}_2$ mit $f(0) = f(2) = 0$ und $f(1) = f(3) = 1$ ist ein Homomorphismus von $(\mathbb{Z}_4, +, 0)$ nach $(\mathbb{Z}_2, +, 0)$.

•) $(\mathbb{Z}_4, +, 0)$ und $(\mathbb{Z}_5^*, \cdot, 1)$ sind isomorph.

•) $(\mathbb{Z}_4, +, 0)$ und $(\mathbb{Z}_8^*, \cdot, 1)$ sind nicht isomorph.

$\cdot$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Der Kern eines Homomorphismus $f: G_1 \to G_2$ ist die Menge

$$\ker(f) = \{a \in G_1 : f(a) = e_2\}.$$

Merke: •) f ist ein Isomorphismus genau dann, wenn $\ker(f) = \{e_1\}$

•) $\ker(f)$ ist eine Untergruppe von G_1, d.h. $(\ker(f), \circ, e_1)$ ist eine Gruppe.

6.4. Permutationsgruppen

Die Menge Perm_n der Permutationen der Menge $\{1, 2, \ldots, n\}$ bildet bzgl. der Hintereinanderausführung der Permutationen als Verknüpfung eine nicht kommutative Gruppe.

Bsp: $n = 5$

$p_1 \in Perm_5$:

1	2	3	4	5
↓	↓	↓	↓	↓
2	4	1	5	3

$p_2 \in Perm_5$:

1	2	3	4	5
↓	↓	↓	↓	↓
3	1	2	4	5

$p_1 \circ p_2$:

1	2	3	4	5
↓	↓	↓	↓	↓
1	4	3	5	2

$p_2 \circ p_1$:

1	2	3	4	5
↓	↓	↓	↓	↓
1	2	4	5	3

Im Allgemeinen ist $p_1 \circ p_2 \neq p_2 \circ p_1$.
(nicht kommutativ)

Das neutrale Element für $Perm_n$ ist:

e :

1	2	3	...	n
↓	↓	↓	...	↓
1	2	3		n

Merke: $\{p \in Perm_n : sgn(p) = 1\}$ bildet immer eine Untergruppe.