Mathematik I

Gruppen

Prof. Dr. Doris Bohnet

Sommersemester 2020

Lernziele

- **Begriffe bzw. Aussagen kennen:**
  - ✓ (abelsche) Gruppe, Untergruppe, Ordnung
  - ✓ Inverses Element
  - ✓ Satz von Euler bzw. „Kleiner Fermat“
- Beispiele von Gruppen kennen
- Nachweisen können, dass es sich bei einem Beispiel um eine Gruppe handelt
- Untergruppen einer Gruppe, Ordnung einer Gruppe bzw. eines Elements bestimmen können
- Inverse Elemente ausrechnen können

Wiederholungsfragen…

1. $(x,y) \in R \Rightarrow x^2 - y^2 = x - y$

$1^2 - 0^2 = 1 - 0 \Rightarrow 0^2 - 1^2 = 0 - 1$ $\not\Rightarrow$ R symm.

für x,y beliebig mit $x^2 - y^2 = x - y$

$\Rightarrow$ $y^2 - x^2 = y - x \Rightarrow (y,x) \in R$

$\cdot(-1)$

2. $\mathbb{Z}_8^* = \{a \in \mathbb{Z}_8 \setminus \{0\} \mid ggT(a,8) = 1\}$, $\mathbb{Z}_8 = \{0,1,2,3,4,\dots,7\}$

$= \{1,3,5,7\}$

alle Elemente, die teilerfremd zu 8 sind

3. $3x = 1 \bmod 7$, $x = 5$, denn $15 = 1 \bmod 7$

4. $\varphi(n) = |\mathbb{Z}_n^*|$

$\varphi(p) = p - 1$

$ggT(n,m) = 1 : \boxed{\varphi(n \cdot m) = \varphi(n)\varphi(m)}$

$\varphi(57) = \varphi(3 \cdot 19)$

$= \varphi(3) \cdot \varphi(19) = 2 \cdot 18$

Beispiel – Cäsar-Verschlüsselung

A	B	C	D	...	U	V	W	X	Y	Z
0	1	2	3	...	23	24	25			

D	E	F	G	...	X	Y	Z	A	B	C
3	4	5	6	...	23	24	25	0	1	2

$\mathbb{Z}_{26} = \{0, 1, 2, \ldots, 25\}$

Verschlüsselung

$$f : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$$
$$a \mapsto a + 3 \bmod 26$$

3: Schlüssel

Wie sieht f^{-1} aus? (so dass $f^{-1}(f(a)) = a$)

Entschlüsselung

$$f^{-1} : \mathbb{Z}_{26} \to \mathbb{Z}_{26}$$
$$a \mapsto a + 23 \bmod 26$$

$-3 \bmod 26 = 23 \bmod 26$ ← additive Inverse von 3

$$f^{-1}(f(a)) = f^{-1}(a + 3 \bmod 26) = a + 3 \bmod 26 + 23 \bmod 26$$
$$= a \bmod 26 \quad \checkmark$$

Beispiel – inverse Elemente

$(\mathbb{Z}_{26}, +)$ $\quad \mathbb{Z}_{26} = \{0, 1, 2, \dots, 25\}$

Verknüpfung

- für $a, b \in \mathbb{Z}_{26}$: $a + b \bmod 26 \in \mathbb{Z}_{26}$
- $\exists 0 \in \mathbb{Z}_{26} : \forall a \in \mathbb{Z}_{26} : a + 0 \bmod 26 = a$ — neutrales Element
- $\forall a \in \mathbb{Z}_{26} \ \exists a' \in \mathbb{Z}_{26} : a + a' \bmod 26 = 0 \bmod 26$ — a': inverse Element von a

z.B. $3 \in \mathbb{Z}_{26}$: $3 + 23 \bmod 26 = 0 \bmod 26$

Definition Sei G eine Menge und $\circ : G \times G \to G$, $(g, h) \mapsto g \circ h$ eine Verknüpfung, mit folgenden Eigenschaften:

(G1) assoziativ: $(g \circ h) \circ i = g \circ (h \circ i) \quad \forall g, h, i \in G$

(G2) neutrales Element: $\exists e \in G : \forall g \in G : g \circ e = g$

(G3) inverse Elemente: $\forall g \in G \ \exists g^{-1} \in G : g \circ g^{-1} = e$

dann heißt $(G, \circ)$ eine Gruppe.

Gruppe - Definition

Sei G eine Gruppe.
Falls (G4) kommutativ: $\forall g,h \in G: g \circ h = h \circ g$,
dann heißt G abelsch

$|G|$ = Anzahl der Elemente heißt Ordnung

Beispiele: 1) $(\mathbb{Z}, +)$: $n+m \in \mathbb{Z}$ $\forall n,m \in \mathbb{Z}$

(G1) gilt ✓

(G2) $n + 0 = n$ $\forall n \in \mathbb{Z}$

(G3) $\forall n \in \mathbb{Z}\ \exists m \in \mathbb{Z}: n + m = 0$

nämlich $m = -n$

Gruppe

2) $(\mathbb{N}_0, +)$: $n + m \in \mathbb{N}_0$ $\forall n,m \in \mathbb{N}_0$

(G1) ✓, (G2) $n+0=n$ $\forall n \in \mathbb{N}_0$

(G3) $\forall n \in \mathbb{N}_0\ \exists m \in \mathbb{N}_0: n+m=0$?

NEIN, denn $m = -n \notin \mathbb{N}_0$ für $n \neq 0$

keine Gruppe

Gruppe

Eine Menge G zusammen mit einer Verknüpfung $\circ$: $G \times G \to G$ heißt **Gruppe,** falls gilt**:**

(G1) assoziativ:$(a \circ b) \circ c = a \circ (b \circ c)$
(G2) Existenz eines neutralen Element: Es gibt $e \in G$: $a \circ e = a$, für alle $a \in G$
(G3) Existenz inverser Elemente: Zu jedem $a \in G$ existiert ein $a^{-1} \in G$ so dass: $a^{-1} \circ a = e$

Gilt zusätzlich:
(G4) kommutativ: $a \circ b = b \circ a$
heißt die Gruppe **abelsch**.

Die Mächtigkeit der Menge $|G|$ wird als **Ordnung** der Gruppe bezeichnet.

Gruppen - Beispiele

3) $(\mathbb{Z}_n, +)$ ist eine Gruppe für $n \in \mathbb{N}$

z.B. $n = 4$

$\mathbb{Z}_4$

$|\mathbb{Z}_n| = n$

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

4.) $S_3 = \{ g : \{1,2,3\} \to \{1,2,3\} \mid g \text{ ist bijektiv} \}$ $|S_3| = 3! = 6$

$(S_3, \circ)$ ist eine Gruppe

$\circ$ ↖ Verknüpfung von Abbildungen

$id = (1\ 2\ 3)$, $s_1 = (1\ 3\ 2)$, $s_2 = (2\ 1\ 3)$, $s_3 = (2\ 3\ 1)$, $s_4 = (3\ 1\ 2)$, $s_5 = (3\ 2\ 1)$

(G2) $\exists\, id\ \forall\, g \in G : g \circ id = g$ ↖ Identität

Gruppen - Beispiele

(G3) Inverse?

$s_1 = (1\ 3\ 2)$

$s_1 \circ s_1 = (1\ 3\ 2) \circ (1\ 3\ 2) = (1\ 2\ 3) = id$

von s_1 ist s_1 das Inverse

$s_2 = (2\ 1\ 3)$

$s_2 \circ s_2 = (2\ 1\ 3) \circ (2\ 1\ 3) = (1\ 2\ 3)$ ✓

S_n Permutationsgruppe oder symmetrische Gruppe

↑ Permutationen von n Elementen.

Gruppen - Beispiele

5) $(\mathbb{Z}, \cdot)$ ist Gruppe?

keine Gruppe.

(G1) erfüllt ✓

(G2) 1 ist neutrales Element

(G3) $\forall n \in \mathbb{Z} \; \exists m \in \mathbb{Z}$

$n \cdot m = 1$

z.B. $5 \cdot m = 1$

$m = \frac{1}{n} \notin \mathbb{Z}$ für $n \neq 1$

keine inverse Elemente

6) $(\mathbb{Z}_4, \cdot)$ Gruppe?

neutral

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

für 0 und 2 finden wir keine Inversen

1, 3 sind teilerfremd zu 4, dann existiert ein Inverses

Wiederholung: $\mathbb{Z}_n^*$

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \setminus \{0\} \mid ggT(a,n) = 1\}$$

$$\mathbb{Z}_4^* = \{1,3\} \qquad |\mathbb{Z}_4^*| = 2$$

letzte Vorlesung: $ggT(n,a) = 1 \iff \exists x,y : nx + ay = 1$

$\iff \exists y : ay = 1 \bmod n$

$\rightsquigarrow (\mathbb{Z}_4^*, \cdot)$ ist dann eine Gruppe

y^ das Inverse von a

allgemein: $(\mathbb{Z}_n^*, \cdot)$ ist eine Gruppe

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

Untergruppe

Eine Teilmenge $H \subset G$ heißt **Untergruppe** von einer Gruppe $(G,\circ)$, falls

1. $g,h \in H \Rightarrow g \circ h \in H$,
2. $g \in H \Rightarrow g^{-1} \in H$.

Man schreibt: $H < G$

} $e \in H$

„$\circ$" Verknüpfung
z.B. „$+$" „$\cdot$" „$\cup$"

Satz: $|H|$ teilt $|G|$, falls G eine endliche Gruppe ist.

Beispiel:

- $\mathbb{Z}_6^* = \{1,5\}$ $\varphi(6) = \varphi(2\cdot 3) = \varphi(2)\cdot\varphi(3) = 1\cdot 2$
  $|\mathbb{Z}_6^*| = 2$, also keine Untergruppen außer $\{1\}$
- $\mathbb{Z}_8^* = \{1,3,5,7\}$ $|\mathbb{Z}_8^*| = 4$ Teiler von 4: 2
  Gibt es eine Untergruppe aus 2 Elementen?
  $H = \{1,7\}$ $7^2 = 1$

Ordnung von Untergruppen & Elementen

Sei G eine Gruppe und $a \in G$. Die kleinste Zahl $n \in \mathbb{N}$, so dass

$$a^n = e$$

heißt **Ordnung des Elementes** $a \in G$.
Man schreibt: $ord(a) = n$.
Gibt es kein solches n, dann setzt man: $ord(a) = \infty$.

$a^n = \underbrace{a \circ a \circ \dots \circ a}_{n\text{-mal}}$

$\mathbb{Z}_8^* = \{1, 3, 5, 7\}$

$|\mathbb{Z}_8^*| = 4$

$ord(a) \mid |G|$

1 oder 2 oder 4 $\mid$ 4

$7^2 \bmod 8 = 1 \bmod 8$
also $ord(7) = 2$

$3^2 \bmod 8 = 1 \bmod 8$
also: $ord(3) = 2$

$5^2 \bmod 8 = 1 \bmod 8$
$\Rightarrow ord(5) = 2$

Ordnung von Untergruppen & Elementen

Satz: Sei G eine endliche Gruppe. Dann gilt für alle Untergruppen $H < G$ und alle Elemente $a \in G$:

$$|H| \mid |G|$$

$$|ord(a)| \mid |G|$$

Wiederholung: Eulersche Phi-Funktion

Es gilt für $\text{ggT}(n, m) = 1$:

$$\phi(n \cdot m) = \phi(n) \cdot \phi(m)$$

und

$$\phi(n) = \prod_{i=1}^{k} (p_i - 1) p_i^{a_i - 1}, n = p_1^{a_1} \cdot \ldots \cdot p_k^{a_k}$$

Insbesondere gilt für Primzahlen:
$\phi(p) = p - 1$

Beispiel:
Wir berechnen $\phi(26)$:
Primfaktorzerlegung von 26: $26 = 2 \cdot 13$
Damit ist $\phi(26) = \phi(2)\phi(13) = 12$.
Wir berechnen $\phi(48)$:
Primfaktorzerlegung von 48: $48 = 2^4 \cdot 3$
Damit ist $\phi(48) = (2 - 1) \cdot 2^3 \cdot (3 - 1) \cdot 3^0 = 8$.

Satz von Euler

Sei $n \in \mathbb{N}, n \geq 2$. Dann gilt für alle $a \in \mathbb{Z}_n^*$: $|\mathbb{Z}_n^*| = \varphi(n)$

$|\mathbb{Z}_8^*| = 4$ $\quad 7^4 = 1 \bmod 8$

$$a^{\phi(n)} = 1 \, mod \, n$$

Beispiel:

Speziell: wenn p Primzahl, $\varphi(p) = p - 1$

$ggT(a,p) = 1$: $\quad a^{p-1} = 1 \bmod p$ „Kleiner Fermat"

„Kleiner Fermat“

Sei $n \in \mathbb{N}, n \geq 2$. Dann gilt für alle $a \in \mathbb{Z}_n \setminus \{0\}$:

$$n \ Primzahl \Leftrightarrow a^{n-1} \equiv 1 \ mod \ n.$$