Mathematik I

Homomorphismen, Ringe & Körper

Prof. Dr. Doris Bohnet

Sommersemester 2020

Zeitplan Vorlesung

		Datum	Bemerkung	Inhalt
Grund-lagen			Selbststudium	Grundlagen: Mengen
			Selbststudium	Grundlagen: Relationen
			Selbststudium	Grundlagen: Abbildungen
Zahlen-theorie	1	22.04.	Einmalig Mi.	Wiederholung & Zusammenfassung Selbststudium
	2	27.04.		Zahlentheorie I
	3	28.04.		Zahlentheorie II
Algebra	4	04.05.		Gruppen
	5	**11.05.**		**Homomorphismen, Ringe & Körper**
	6	12.05.		Kryptographie
	7	18.05.		Vektorräume
Lineare Algebra	8	25.05.		Lineare Gleichungssysteme
	9	26.05.		Lineare Gleichungssysteme
	10	01.06.	Pfingstmontag	--
	11	08.06.		Matrizen
	12	09.06.		Lineare Abbildungen

Lernziele

- **Begriffe bzw. Aussagen kennen:**
  - ✓ Zyklische Gruppe, Erzeuger
  - ✓ Gruppenhomomorphismus bzw. -isomorphismus
  - ✓ Chinesischer Restsatz
  - ✓ Ring, Körper

- Überprüfen können, ob eine Abbildung ein Homomorphismus ist;
- den Erzeuger einer Gruppe bestimmen bzw. überprüfen, ob eine Gruppe zyklisch ist;
- Überprüfen, ob zwei Gruppen isomorph sind;
- ein System aus Kongruenzgleichungen mit Hilfe des chinesischen Restsatzes zu lösen;
- Beispiele für zyklische Gruppen und endliche Körper kennen

Wiederholung

$$\mathbb{Z}_{12}^* = \{ a \in \mathbb{Z}_{12} \setminus \{0\} \mid ggT(a,12) = 1 \}$$

$$= \{1, 5, 7, 11\}$$

$$\mathbb{Z}_{12} = \{0, 1, 2, 3, \ldots, 11\}$$

$$|\mathbb{Z}_{12}^*| = 4 = \varphi(12)$$

$$\varphi(12) = \varphi(2^2 \cdot 3) = \varphi(2^2)\varphi(3) = 2 \cdot 2 = 4$$

für $a \in \mathbb{Z}_{12}^*$: $a^{\varphi(12)} = 1 \mod 12$

$ord(a) = n$: kleinste Zahl, so dass $a^n = 1$

$ord(a) \mid$ Gruppenordnung : $ord(1) = 1$ ← neutrales Element

denn $5^2 \mod 12 = 1$

$ord(5) = 2$
$ord(7) = 2$
$ord(11) = 2$

Beispiel – zyklische Gruppe

$\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$ hat nur Elemente der Ordnung 1 oder 2.

$\mathbb{Z}_5^* = \{1, 2, 3, 4\}$ $|\mathbb{Z}_5^*| = 4$

$ord(1) = 1$

$ord(2) = 4$ $= |\mathbb{Z}_5^*|$

$ord(3) = 4$

$ord(4) = 2$

NR: $2^2 = 4$

$2^3 = 8$

$2^4 = 16 = 4^2$

$16 \bmod 5 = 1 \bmod 5$

$2^0 = 1, \quad 2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 3, \quad 2^4 = 1$

NR: $3^3 = 27$

$3^2 = 9$

$3^4 = 81$

$\mathbb{Z}_5^* = \{2^4, 2, 2^3, 2^2\} = \{3^4, 3^3, 3^1, 3^2\}$ ← 3 ist auch ein Erzeuger

↑ 2 heißt ERZEUGER von $\mathbb{Z}_5^*$

$\mathbb{Z}_5^*$ heißt dann ZYKLISCHE GRUPPE

$\mathbb{Z}_5^* = \langle 2 \rangle$

Definition - Zyklische Gruppe

Eine Gruppe $(G, \circ)$ heißt **zyklisch**, falls es ein Element $g \in G$ gibt, so dass

$\circ$: + oder ·

$$G = \{g^i | i \in \mathbb{Z}\}$$

$g^n = g \circ g \circ \dots \circ g$ (n-mal)

Ein solches Element $g \in G$ heißt **Erzeuger** (oder erzeugendes Element) der Gruppe.

Beispiel $(\mathbb{Z}_5, +)$ $\quad \mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$, $|\mathbb{Z}_5| = 5$

~~Beispiel.~~

Die Gruppen $(\mathbb{Z}, +)$ und $(\mathbb{Z}_n, +)$ sind zyklisch. Das erzeugende Element ist jeweils die Eins.

Ordnung von 1: $\underbrace{1+1}_{\hat{=} 1^2} \quad \underbrace{1+1+1+1+1}_{\hat{=} 1^5} = 5 \bmod 5 = 0 \bmod 5$

$\text{ord}(1) = 5$

also ist 1 ein Erzeuger von $\mathbb{Z}_5$: $\mathbb{Z}_5 = \langle 1 \rangle$

Allgemein ist jede Gruppe $(\mathbb{Z}_n, +)$ zyklisch mit Erzeuger 1.

Beispiel – Produkt von Gruppen

Beispiel zyklische Gruppe: $(\mathbb{Z}, +)$ $|\mathbb{Z}| = \infty$

$\mathbb{Z} = \langle 1 \rangle$

Beispiel: $\mathbb{Z}_2 \times \mathbb{Z}_3 = \{(a,b) \mid a \in \mathbb{Z}_2, b \in \mathbb{Z}_3\}$

$\{0,1\}$ $\{0,1,2\}$

$= \{(0,0), (0,1), (0,2), (1,0), (1,1), (1,2)\}$

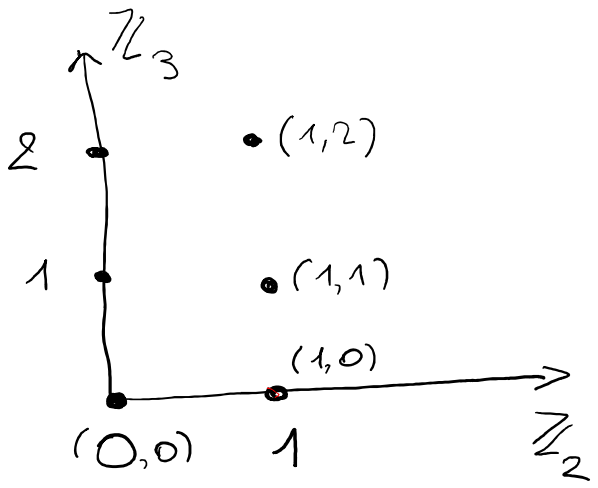
$|\mathbb{Z}_2 \times \mathbb{Z}_3| = 6$

Verknüpfung:

$(a,b) + (c,d) = (a+c, b+d)$

$(1,0) + (0,1) = (1+0, 0+1)$

neutrales Element: $(0,0)$



Definition - Homomorphismus

Eine Abbildung $f: G \to H$ zwischen zwei Gruppen $(G,\circ)$ und $(H,*)$, für die für alle $g, h \in G$

$$f(g \circ h) = f(g) * f(h)$$

gilt, heißt **(Gruppen)Homomorphismus**.

Ist der Homomorphismus bijektiv, nennt man ihn einen **Isomorphismus**. G und H heißen dann isomorph: $G \cong H$

Beispiel: $(\mathbb{Z}_2 \times \mathbb{Z}_3, +)$ Gruppe, $|\mathbb{Z}_2 \times \mathbb{Z}_3| = 6$

$(\mathbb{Z}_6, +)$ Gruppe, $|\mathbb{Z}_6| = 6$

$f: \mathbb{Z}_6 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_3$

$\{0,1,2,3,4,5\}$ $\{(0,0),(0,1),(0,2),(1,0),(1,1),(1,2)\}$

$f((2+3) \bmod 6) = f(2) + f(3)$

Beispiele für Homomorphismen

Beispiele: 1) $f: \mathbb{Z}_6 \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_3$

$a \longmapsto (a \bmod 2, a \bmod 3)$

$f(1) = (1,1)$, $f(2) = (2 \bmod 2, 2 \bmod 3) = (0,2)$

$f(0) = (0,0)$, $f(3) = (1,0)$, $f(4) = (0,1)$, $f(5) = (1,2)$

f ist bijektiv?

surjektiv: ✓

injektiv: ✓

f Homomorphismus? $\quad f(a +_{\mathbb{Z}_6} b) = f(a) +_{\mathbb{Z}_2 \times \mathbb{Z}_3} f(b)$

$f(2 \oplus 3) = f(5) = (1,2)$ =

$f(2) \oplus f(3) = (0,2) + (1,0) = (1,2)$ ✓

allgemein:

$f(a+b) = (a+b \bmod 2, a+b \bmod 3)$

$= (a \bmod 2, a \bmod 3) + (b \bmod 2, b \bmod 3)$

$\rightsquigarrow f$ Isomorphismus

Zyklische Gruppen

Jede unendliche zyklische Gruppe G ist isomorph zu $(\mathbb{Z}, +)$. Jede endliche zyklische Gruppe G der Ordnung n ist isomorph zu $(\mathbb{Z}_n, +)$.
Der jeweilige Isomorphismus bildet das erzeugende Element g von G auf die Eins ab:

$$f: G \to \mathbb{Z}, g \mapsto 1$$

$f(g^n) = \underbrace{1 + 1 + 1 \dots + 1}_{n\text{-mal}} = n$

„große" Gruppe

$\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$

2 kleine Gruppen

Idee

statt Zahlen in „großen" Gruppen zu berechnen, können sie in kleineren Gruppen berechnet werden.

Schnelle Addition & Multiplikation

Idee: Große Zahlen in kleineren Restklassen berechnen

Beispiel: $1878 + 1384 \in \mathbb{Z}_{4000}$

$f: \mathbb{Z}_{4000} \to \mathbb{Z}_{32} \times \mathbb{Z}_{125}$

$f(a) = (a \bmod 32, a \bmod 125)$

$f(1878) = (22, 3)$

$f(1384) = (8, 9)$

gesucht ist x, so dass

$x \bmod 32 = 30 \bmod 32$

$x \bmod 125 = 12 \bmod 125$

$\mathbb{Z}_{4000}$

1878

$+ 1384$

3262

$\mathbb{Z}_6 \cong \mathbb{Z}_2 \times \mathbb{Z}_3$

$\mathbb{Z}_{4000} \cong \mathbb{Z}_{32} \times \mathbb{Z}_{125}$

$4000 = 2^5 \cdot 5^3$

$\mathbb{Z}_{32} \times \mathbb{Z}_{125}$

$(22, 3)$

$+ (8, 9)$

$(30, 12)$

Schnelle Addition & Multiplikation

Chinesischen Restsatz

Seien n_i, $i = 1, \dots, k$ teilerfremd und $x_i \in \mathbb{Z}$

Dann existiert genau eine Lösung $x \in \mathbb{Z}_n$ mit

$n = n_1 \cdot \dots \cdot n_k$, so daß

$x \bmod n_i = x_i \bmod n_i$ für $i = 1, \dots, k$

Bei uns: $n_1 = 32$, $n_2 = 125$, $ggT(32, 125) = 1$

$x \bmod 32 = 30 \bmod 32$, $x \bmod 125 = 12 \bmod 125$

mit dem Satz: $\exists! \, x \in \mathbb{Z}_{4000}$

Lösung mit erw. eukl. Alg.: $\exists r, s \in \mathbb{Z}$: $1 = r \cdot 125 + s \cdot 32$

$r \cdot 125 \bmod 125 = 0$

$s \, 32 \bmod 125 = 1 \Rightarrow 12 \cdot s \cdot 32 \bmod 125$

$= 12 \bmod 125$

Chinesischer Restsatz

Seien $n_1, n_2, \dots, n_k \in \mathbb{N}$ zueinander teilerfremde Zahlen und $x_1, \dots, x_k \in \mathbb{Z}$. Sei $n = n_1 \cdot \dots \cdot n_k$.
Dann existiert genau eine Lösung $x \in \mathbb{Z}_n$ so dass

$$x \bmod n_i = x_i \bmod n_i, i = 1, \dots, k.$$

$x \bmod 32 = 30 \bmod 32$, $x \bmod 125 = 12 \bmod 125$

x_i

Wir berechnen die Lösung, indem wir jeweils für jedes $i = 1, \dots, k$ mit Hilfe des erweiterten euklidischen Algorithmus zu $n_i, n/n_i$ die Zahlen
r_i, s_i berechnen, so dass

$$1 = r_i \cdot n_i + s_i \cdot \frac{n}{n_i}$$

$n_1 = 32$, $n_2 = 125$

$1 = r \cdot 125 + s \cdot 32$

$a_1 = s \cdot 32$

Und dann setzen $a_i = s_i \cdot \frac{n}{n_i}$, denn dann ist $a_i \bmod n_i = 1, a_i \bmod n_j = 0, j \neq i$.

Die Lösung bildet sich aus $x = \sum a_i x_i$.

$x = 12 \cdot s \cdot 32 + 30 \cdot r \cdot 125$

Anwendung

Seien $n_1, n_2, \dots, n_k \in \mathbb{N}$ zueinander teilerfremde Zahlen. Dann gilt:

$$\mathbb{Z}_{n_1 \cdot \dots \cdot n_k} \cong \mathbb{Z}_{n_1} \times \cdots \mathbb{Z}_{n_k}$$

$$\mathbb{Z}_{2 \cdot 3} \cong \mathbb{Z}_2 \times \mathbb{Z}_3$$

Beispiel weiter: erweiterter eukl. Algo. $ggT(125, 32) = 1$

a	b	r	s	k
125	32	1	0	–
32	29	0	1	3
29	3	1	−3	1
3	2	−1	4	9
2	1	10	−39	1
1	0	−11	43	2

$r \cdot 125 + s \cdot 32 = 1$

$-11 \cdot 125 + 43 \cdot 32 = 1$

Rest mod 125

$x = 30 \cdot (-11 \cdot 125) + 12 \cdot 43 \cdot 32$

Rest mod 32

$= -24738$

$\mod 4000$

$= 3262$

$x \in \mathbb{Z}_{4000}$