Mathematik I

Gruppen

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.		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:**
  - ✓ Gruppe, Untergruppe, Ordnung
- 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. $ggT(186{,}66) = ?$

2. In welcher Zeile ist der erste Fehler passiert?

i	a	b	x	y	k
0	186	66	1	0	–
1	66	54	0	1	2
2	54	12	1	−2	1
3	12	6	−1	−1	4
4	6	0	5	−6	2

3. In welcher Restklasse liegen 17, 22 und -13?

4. Wieviele Äquivalenzklassen hat die folgende Äquivalenzrelation?

$$a \equiv_7 b :\Leftrightarrow \exists k \in \mathbb{Z}\colon\ a - b = 7k$$

Wiederholung

$$x_{i+1} = x_{i-1} - k_i \cdot x_i$$
$$y_{i+1} = y_{i-1} - k_i \cdot y_i$$

Frage 2

ggT(186, 66)

$\in \mathbb{Z}$

	a	b	x	y	k
0	186	66	1	0	—
1	66	54	0	1	2
2	54	12	1	−2	1
3	12	6	−1	3	4
4	6	0	5	−14	2

$ggT(186, 66) = 6$

$6 = 5 \cdot 186 + (-14) \cdot 66$

$186 = 2 \cdot 66 + 54$

$x = 1 - 0 \cdot 2$

$y = 0 - 1 \cdot 2$

$66 = 1 \cdot 54 + 12$

$x = 0 - 1 \cdot 1$

$y = 1 - (-2) \cdot 1$

$54 = 4 \cdot 12 + 6$

$x = 1 - 4 \cdot (-1)$

$y = -2 - 3 \cdot 4 = -14$

$12 = 2 \cdot 6 + 0$

Wiederholung

Restklassen

Äquivalenzrelation $a \equiv_7 b :\Leftrightarrow \exists k \in \mathbb{Z}: a - b = 7k$

$(\Leftrightarrow \quad a = b \bmod 7)$ „modulo"

reflexiv? Für $a \in \mathbb{Z}$: $a - a = 0 = 7 \cdot 0$, also $a \equiv_7 a$

symmetrisch? Für $a, b \in \mathbb{Z}$ mit $a \equiv_7 b$ gilt: $\exists k \in \mathbb{Z}: a - b = 7k$.

Also ist $b - a = 7 \cdot (-k)$. Da $(-k) \in \mathbb{Z}$, ist $b \equiv_7 a$.

transitiv? Für $a, b, c \in \mathbb{Z}$ mit $a \equiv_7 b$ und $b \equiv_7 c$ gilt:

$\exists k, k': a - b = 7k$ und $b - c = 7k'$

Gleichungen addieren: $a - b + b - c = a - c = 7(k + k')$

also $a \equiv_7 c$

Restklassen - Einführung

Äquivalenzklassen

$[0] = \{\dots, -14, -7, 0, 7, 14, \dots\}$

$a \in \mathbb{Z}: \quad a - 0 = 7k$

$a = 7k$

$[1] = \{\dots, -13, -6, 1, 8, 15, \dots\}$

$a \in \mathbb{Z}: \quad a - 1 = 7k \iff a = 1 + 7k$

$[2], [3], [4], [5], [6], [7] = [0]$

also 7 Äquivalenzklassen

$a \sim b :\iff a^2 - b^2 = a - b$

$0 \sim a \iff a^2 - 0 = a - 0$

$1 \sim a \iff a^2 - 1 = a - 1$

Restklassen - Definition

Zu jedem $n \in \mathbb{N}$ können wir die folgende Äquivalenzrelation auf der Menge der ganzen Zahlen $\mathbb{Z}$ definieren:

$$a \equiv_n b :\Leftrightarrow \exists k \in \mathbb{Z}: a - b = k \; (\Leftrightarrow a - b = 0 \; mod \; n \Leftrightarrow a = b \; mod \; n)$$

Diese Äquivalenzrelation besitzt n Äquivalenzklassen:

$$[0] = \{a \in \mathbb{Z} |\; a \equiv 0 \; mod \; n\}, [1] = \{a \in \mathbb{Z} |\; a \equiv 1 \; mod \; n\}, \dots, [n-1] = \{a \in \mathbb{Z} |\; a \equiv (n-1) \; mod \; n\}$$

Wir nennen diese Äquivalenzklassen **Restklassen** und schreiben kurz für die Menge der Äquivalenzklassen:

$$\mathbb{Z}_n = \{[0], [1], \dots, [n-1]\}, |\mathbb{Z}_n| = \mathrm{n}$$

Beispiel:
Es gibt nur eine Restklasse von 1, deswegen ist $\mathbb{Z}_1 = \{[0]\} = \mathbb{Z}$.
Es gibt zwei Restklassen von 2, deswegen ist $\mathbb{Z}_2 = \{[0], [1]\}$. Die Restklassen enthalten die geraden bzw. ungeraden Zahlen.

Modulorechnung - Beispiele

$$(38 + 22) \bmod 9$$
$$= 38 \bmod 9 + 22 \bmod 9 = 2 \bmod 9 + 4 \bmod 9$$
$$= 6 \bmod 9$$

$$(101 \cdot 234) \bmod 5 = (101 \bmod 5)(234 \bmod 5)$$
$$= (1 \bmod 5)(4 \bmod 5)$$
$$= 1 \cdot 4 \bmod 5 = 4 \bmod 5$$

$$(38 + 22 \cdot 17) \bmod 4 = 38 \bmod 4 + 22 \bmod 4 \cdot 17 \bmod 4$$
$$= 2 \bmod 4 + 2 \bmod 4 \cdot 1 \bmod 4$$
$$[38 + 22 \cdot 17] = [38] + [22] \cdot [17] = 0 \bmod 4$$

Modulorechnung (Rechnen mit Restklassen)

Seien $n_1 \equiv a \; mod \; m, n_2 \equiv b \; mod \; m.$

Addition:

$$(n_1 + n_2) mod \; m = (a + b) \; mod \; m$$

Multiplikation:

$$(n_1 \cdot n_2) mod \; m = (a \cdot b) \; mod \; m$$

Bsp Mit welcher Ziffer endet 9^{99}? $9^{99} = 10 \cdot a + b$ $a, b \in \mathbb{N}_0, b \leq 9$

$9^{99} \bmod 10 = (-1)^{99} \bmod 10 = -1 \bmod 10$

$= 9 \bmod 10$

$9 \bmod 10 = -1 \bmod 10$ ↳ letzte Ziffer.

$[9] = \{9 + 10k \mid k \in \mathbb{Z}\} = \{\ldots, -11, -1, 9, 19, 29, \ldots$

Teilbarkeitsregeln

Ist 1782 durch 3 teilbar?

Quersumme: $1+7+8+2 = 18$

$$1782 \bmod 3 = (1 \cdot 10^3 + 7 \cdot 10^2 + 8 \cdot 10 + 2) \bmod 3$$

$$= (1 \cdot 10^3 \bmod 3 + 7 \cdot 10^2 \bmod 3 + 8 \cdot 10 \bmod 3 + 2 \bmod 3)$$

$$= 1 \bmod 3 + 7 \bmod 3 + 8 \bmod 3 + 2 \bmod 3$$

$$= (1+7+8+2) \bmod 3$$

NR: $10 \bmod 3 = 1 \bmod 3$

$10^2 \bmod 3 = 1 \bmod 3$

$10^k \bmod 3 = 1 \bmod 3$

Wir fassen alle $[a] \in \mathbb{Z}_n$ zusammen, die teilerfremd zu $n \in \mathbb{Z}$ sind:

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

↑ Menge der Restklassen von modulo n: $[0], [1], \dots, [n-1]$

Bsp:

$$\mathbb{Z}_7^* = \{\dot{1}, \dot{2}, \dot{3}, \dot{4}, \dot{5}, \dot{6}\} \leftarrow \text{alle Restklassen!} = \mathbb{Z}_7$$

$$\mathbb{Z}_8^* = \{1, 3, 5, 7\} \rightsquigarrow \varphi(8) = |\mathbb{Z}_8^*| = 4$$

$ggT(6,8) = 2$

↑ Eulersche φ-Funktion

$$\varphi(7) = |\mathbb{Z}_7^*| = 6$$

Anwendung: Prüfziffern

Eine ISBN-Nummer besteht aus 13 Ziffern, die letzte Ziffer ist eine Prüfziffer. Die Prüfziffer berechnet sich aus der Modulorechnung wie folgt:

ISBN: $a_1 a_2 \dots a_9$
Prüfziffer: Man wählt die Prüfziffer a_{13}, so dass

$$(1 \cdot a_1 + 3 \cdot a_2 + 1 \cdot a_3 + \cdots + 3 \cdot a_{12} + 1 \cdot a_{13}) mod\ 10 = 0$$

Anwendung: Prüfziffern

Hier ist ein Tippfehler passiert. Berechnen Sie die Prüfziffer für die falsche ISBN

979−3−540−89106−2

Berechnen Sie die Prüfziffer der folgenden ISBN, bei der zwei Ziffern vertauscht wurden:

973−8−540−89106−2

Eulersche Phi-Funktion

Wir bezeichnen mit

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

die Menge aller zu n teilerfremden Zahlen und mit

$$\phi(n) = |\mathbb{Z}_n^*|$$

die Anzahl der zu n teilerfremden Zahlen.

Eulersche phi-Funktion

p Primzahl: $\varphi(p) = p - 1$ $\varphi(7) = 6$

$n, m \in \mathbb{Z}$: $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$

$\Rightarrow$ || $ggT(n,m) = 1$

$\varphi(10) = \varphi(2 \cdot 5) = \varphi(2) \cdot \varphi(5) = 1 \cdot 4 = 4$

$\varphi(26) = \varphi(2 \cdot 13) = \varphi(2) \cdot \varphi(13) = 1 \cdot 12 = 12$

Euler Phi-Funktion - Aufgabe

Berechnen Sie

1. $\phi(256)$
2. $\phi(19)$
3. $\phi(57)$