Übung 14: Algebra

Diskrete Strukturen im Wintersemester 2013/2014

Markus Kaiser

25. Februar 2014

Modulo

Definition (Modulo-Kongruenz)

Zwei Zahlen $a, b \in \mathbb{Z}$ heißen kongruent Modulo $n \in \mathbb{N}$, falls

$$\exists k \in Z.\ a = k \cdot n + b$$

Wir schreiben dann $a \equiv b \pmod{n}$ oder $a \equiv_n b$.
Durch $\equiv_n$ wird eine Äquivalenzrelation definiert.

Definition (Modulo-Operator)

Der Modulo-Operator ordnet jeder Zahl $a \in \mathbb{Z}$ seine Äquivalenzklasse (Restklasse) Modulo $n \in \mathbb{N}$ zu. Es gilt

$$a \mod n = r \quad \text{gdw.} \quad \exists q \in \mathbb{Z}.\ a = q \cdot n + r \quad \text{mit} \quad 0 \leq r < n$$

Modulo gibt den Rest bei einer Ganzzahldivision zurück.

Beispiel

$$5 \mod 3 = 2 \qquad 6 \mod 3 = 0 \qquad -5 \mod 3 = 1$$

Definition (Algebra)

Eine Algebra $\langle M, (\circ_i)_{i \in I} \rangle$ besteht aus einer Menge von Operanden und einer oder mehrerer innerer Verknüpfungen.
Eine innere Verknüpfung auf M ist eine Abbildung

$$\circ : M \times M \to M$$

Eine Verknüpfung heißt

assoziativ wenn $(a \circ b) \circ c = a \circ (b \circ c)$

kommutativ wenn $a \circ b = b \circ a$

für alle $a, b, c \in M$.

Beispiel

Einige Beispiele für Algebren sind (mit üblichen Verknüpfungen)

- $\langle \mathbb{Z}, +, \cdot \rangle$ die ganzen Zahlen
- $\langle \mathbb{Z}_{11}, +_{11} \rangle$ die Restklassen Modulo 11
- $\langle \mathbb{R}^3, +, \cdot \rangle$ der 3-Dimensionale $\mathbb{R}$-Vektorraum

Definition (Gruppe)

Eine Algebra $\langle G, \circ, e \rangle$ heißt Gruppe, wenn für alle $a, b, c \in G$ gilt

- **Assoziativität** $(a \circ b) \circ c = a \circ (b \circ c)$
- **Neutrales Element** Für e gilt $a \circ e = e \circ a = a$
- **Inverse Elemente** Es gibt a^{-1} mit $a \circ a^{-1} = a^{-1} \circ a = e$

Wir schreiben auch kurz G.
Wir nennen G abelsch (oder kommutativ), wenn $\circ$ kommutativ ist.

Beispiel

Die Menge $[4]$ zusammen mit der Multiplikation modulo 5 beschreibt die Gruppe $\langle [4], \cdot_5, 1 \rangle = \mathbb{Z}_5^*$.

$\cdot_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

- Erfüllt „Sudokuprinzip“
- Multiplikation ist assoziativ
- 1 ist neutrales Element
- Inverse existieren
- Kommutativ da symmetrisch

Definition (Untergruppe)

Sei G eine Gruppe und $H \subseteq G$ eine Teilmenge.
H heißt Untergruppe von G, wenn für $a, b \in H$ gilt

$$\text{Abgeschlossenheit} \quad a \circ b \in H$$
$$\text{Inverse} \quad a^{-1} \in H$$

Wir schreiben $H < G$.

- Um zu zeigen dass $H < G$ gilt, reicht es zu zeigen dass

$$a, b \in H \to ab^{-1} \in H$$

- Jede Gruppe enthält $\{e\}$ und sich selbst als Untergruppe

Beispiel

Betrachte $G = \langle \mathbb{Z}_{10}, +_{10}, 0 \rangle$ die Restklassen Modulo 10.
Dann ist $H = \langle \{0, 2, 4, 6, 8\}, +_{10}, 0 \rangle$ eine Untergruppe von G, da die Summe zweier gerader Zahlen gerade ist und für $a \in H$ gilt, dass $a^{-1} = 10 - a \in H$.

Ordnung und Erzeugnis

Sei $\langle G, \circ, e \rangle$ eine Gruppe.

Definition (Ordnung)

Die Ordnung eines Elements $a \in G$ ist die kleinste Potenz k, sodass $a^k = e$.

$$\operatorname{ord}(a) := \min \left\{ k \in \mathbb{N} \setminus \{0\} \mid a^k = e \right\}$$

Existiert kein solches k, so ist $\operatorname{ord}(a) := \infty$.

Definition (Erzeugnis)

Das Erzeugnis $\langle a \rangle$ von a in G ist die Menge aller Elemente, die durch Potenzierung von a und a^{-1} erhalten werden können.

$$\langle a \rangle := \left\{ a^k \mid k \in \mathbb{Z} \right\}$$

Es gilt $\langle a \rangle < G$.

Zyklische Gruppen

Definition (Zyklische Gruppe)

Man nennt eine Gruppe G zyklisch, wenn ein Element $a \in G$ existiert, sodass a die gesamte Gruppe erzeugt.

$$\langle a \rangle = G$$

Man nennt a einen Generator (oder Erzeuger).

- Alle Untergruppen einer zyklischen Gruppe sind zyklisch
- Zyklische Gruppen sind isomorph zu einer $\mathbb{Z}_i$ oder $\mathbb{Z}$

Beispiel

Die ganzen Zahlen $\mathbb{Z}$ und alle Gruppen der Form $\langle \mathbb{Z}_i, +_i, 0 \rangle$ sind zyklisch mit dem Generator 1.
Betrachte $\langle \mathbb{Z}_7, +_7, 0 \rangle$. Es ist

- $\mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\}$
- $\langle 2 \rangle = \{2, 4, 6, 1, 3, 5, 0\} = \langle 1 \rangle = \mathbb{Z}_7$

Homomorphismen

Seien $\langle G, \circ, e \rangle$ und $\langle G', \bullet, e' \rangle$ Gruppen.

Definition (Homomorphismus)

Eine Abbildung $\varphi : G \to G'$ heißt Homomorphismus, wenn gilt

$$\varphi(a \circ b) = \varphi(a) \bullet \varphi(b)$$

Ist φ bijektiv, so nennt man sie einen Isomorphismus.

- Homomorphismen sind strukturerhaltend
- Sie betten eine Gruppe in eine andere ein

Satz

Ist $\varphi : G \to G'$ ein Homomorphismus, so gilt

- $\varphi(e) = e'$
- *Für alle $a \in G$ gilt $\varphi(a)^{-1} = \varphi(a^{-1})$*
- *Ist $H < G$, dann auch $\varphi(H) < G'$*

Nebenklassen

Sei $\langle G, \circ, e \rangle$ eine Gruppe und $H < G$.

Definition (Nebenklasse)

Zu einem Element $a \in G$ nennen wir

$$aH := \{ax \mid x \in H\}$$
$$Ha := \{xa \mid x \in H\}$$

die linke/rechte Nebenklasse von a bezüglich H.
Die Anzahl der Nebenklassen zu H nennt man ihren Index $\mathrm{ind}(G : H)$.

- Die Nebenklassen zu H sind eine Partition von G

Satz (Satz von Lagrange)

Ist G eine endliche Gruppe, so gilt

$$\mathrm{ord}(G) = \mathrm{ord}(H) \cdot \mathrm{ind}(G : H)$$

Daraus folgt direkt $\mathrm{ord}(a) \mid \mathrm{ord}(G)$ für alle $a \in G$.

Eulersche φ-Funktion

Definition (Eulersche φ-Funktion)

Die Funktion $\varphi : \mathbb{N} \setminus \{0\} \to \mathbb{N}$ heißt Eulersche φ-Funktion. Sie ist definiert durch die Anzahl der zu n teilerfremden Zahlen.

$$\varphi(n) := |\{x \mid x \in [n], \text{ggT}(x, n) = 1\}|$$

Es gilt für

$$\begin{aligned} \text{ggT}(m, n) = 1 &\quad \varphi(m \cdot n) = \varphi(m) \cdot \varphi(n) \\ p \text{ prim} &\quad \varphi(p) = p - 1 \\ p \text{ prim}, k > 0 &\quad \varphi(p^k) = p^{k-1}(p - 1) \end{aligned}$$

Satz (Euler-Fermat)

Für $m \in \mathbb{N}$ mit $m \geq 2$ und $k \in \mathbb{Z}$ mit $\text{ggT}(k, m) = 1$ gilt

$$k^{\varphi(m)} \equiv 1 \pmod{m}$$

ist p prim, so gilt im speziellen

$$k^{p-1} \equiv 1 \pmod{p}$$

Erweiterter Euklidscher Algorithmus

Der erweiterte Euklische Algorithmus berechnet für zwei Zahlen $a, b \in \mathbb{N}$ ganze Zahlen $x, y \in \mathbb{Z}$, sodass gilt

$$a \cdot x + b \cdot y = \text{ggT}(x, y)$$

Beispiel

Seien $a = 99$, $b = 78$ mit $\text{ggT}(99, 78) = 3$.

$$\begin{aligned}
99 &= 1 \cdot 78 + 21 && \longrightarrow && 21 &= 99 - 1 \cdot 78 \\
78 &= 3 \cdot 21 + 15 && \longrightarrow && 15 &= 78 - 3 \cdot 21 \\
21 &= 1 \cdot 15 + 6 && \longrightarrow && 6 &= 21 - 1 \cdot 15 \\
15 &= 2 \cdot 6 + 3 && \longrightarrow && 3 &= 15 - 2 \cdot 6 \\
6 &= 2 \cdot 3 + 0
\end{aligned}$$

$$\begin{aligned}
21 &= 1 \cdot 99 - 1 \cdot 78 \\
15 &= 1 \cdot 78 - 3 \cdot 21 = -3 \cdot 99 + 4 \cdot 78 \\
6 &= 1 \cdot 21 - 1 \cdot 15 = 4 \cdot 99 - 5 \cdot 78 \\
3 &= 1 \cdot 15 - 2 \cdot 6 = -11 \cdot 99 + 14 \cdot 78
\end{aligned}$$

Erweiterter Euklidscher Algorithmus

Satz

Die vorhergehende Rechnung kann kompakter in einer Tabelle dargestellt werden. Setze dazu

$$q_k = r_{k-1} \div r_k \qquad s_k = s_{k-2} - s_{k-1} \cdot q_{k-1}$$
$$r_k = r_{k-2} \mod r_{k-1} \qquad t_k = t_{k-2} - t_{k-1} \cdot q_{k-1}$$

Und initialisiere die Tabelle folgendermaßen:

k	q_k	r_k	s_k	t_k
0	-	99	1	0
1		78	0	1
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\vdots$
n	-	0	-	-

Dann gilt für jedes k: $a \cdot s_k + b \cdot t_k = r_k$ *und*

$$a \cdot s_{n-1} + b \cdot t_{n-1} = \mathrm{ggT}(a, b)$$

Erweiterter Euklidscher Algorithmus

Beispiel

Seien $a = 99$, $b = 78$ mit $\text{ggT}(99, 78) = 3$.

k	q_k	r_k	s_k	t_k
0	-	99	1	0
1	1	78	0	1
2	3	21	1	-1
3	1	15	-3	4
4	2	6	4	-5
5	2	3	-11	14
6	-	0	-	-

Es ist $3 = -11 \cdot 99 + 14 \cdot 78$.