Script **generated by TTT**

Title: Esparza: Diskrete Strukturen (30.01.2014)

Date: Thu Jan 30 10:15:38 CET 2014

Duration: 88:56 min

Pages: 30

Kapitel V – Algebra; Gruppen

- Eigenschaften von Gruppen

  Satz: Sei $\langle S,\circ\rangle$ eine Gruppe. Dann gilt:

  (1) S enthält genau ein neutrales Element e.

  (2) Jedes $a \in S$ hat genau ein inverses Element a^{-1}.

  (3) (Involutionsgesetz). Für alle $a \in S$: $a = (a^{-1})^{-1}$

  (4) (Kürzungsregel). Für alle $a, b, c \in S$:

  - wenn $a \circ c = b \circ c$ dann $a = b$
  - wenn $c \circ a = c \circ b$ dann $a = b$

3

Kapitel V – Algebra; Gruppen

- Eigenschaften von Gruppen

  (5) (Eindeutige Lösung linearer Glgn.). Für alle $a, x, b \in S$:

  - wenn $a \circ x = b$ dann $x = a^{-1} \circ b$
  - wenn $x \circ a = b$ dann $x = b \circ a^{-1}$

  (6) (Injektivität von $\circ$). Für alle $a, b, c \in S$:

  - $a \neq b$ gdw. $a \circ c \neq b \circ c$
  - $a \neq b$ gdw. $c \circ a \neq c \circ b$

  (7) (Surjektivität von $\circ$). Für alle $a, b \in S$:

  - es gibt $x \in S$: $a \circ x = b$
  - es gibt $y \in S$: $y \circ a = b$

4

Kapitel V – Algebra; Gruppen

- Ordnung eines Gruppenelements

  Definition: Sei $\langle S,\circ\rangle$ eine Gruppe und sei $a \in S$. Wir definieren

  - $a^0 := e$
  - $\forall n \geq 1$: $a^n := a \circ a^{n-1} = a^{n-1} \circ a$
  - $\forall n \geq 1$: $a^{-n} := (a^{-1})^n$

  Man bezeichnet a^n auch als die n-te Potenz des Elements a.

7

Kapitel V – Algebra; Gruppen

- Ordnung eines Gruppenelements

  Beispiele:

  $\langle \mathbb{Z}, + \rangle$: $\mathrm{ord}(1) = \infty$.

  $\langle \mathbb{Z}_{12}, +_{12} \rangle$:

a	0	1	2	3	4	5	6	7	8	9	10	11
$\mathrm{ord}(a)$	1	12	6	4	3	12	2	12	3	4	6	12

  $\langle \mathbb{Z}_7 \setminus \{0\}, *_7 \rangle$:

a	1	2	3	4	5	6
$\mathrm{ord}(a)$	1	3	6	3	6	2

Kapitel V – Algebra; Gruppen

- Ordnung eines Gruppenelements

  Satz: Sei $\langle S, \circ \rangle$ eine endliche Gruppe. Dann hat auch jedes Element in S endliche Ordnung.

  Beweis: Sei $a \in S$ beliebig. Mindestens zwei von $a^0, \dots, a^{|S|}$ sind gleich (Schubfachprinzip). Wähle $0 \le j < k \le |S|$ mit $a^j = a^k$ und k minimal.

  Durch Multiplikation mit a^{-j} erhält man $a^0 = a^{k-j}$.

  Aus der Minimalität von k folgt $j = 0$ (nehme sonst $k' = k - 1,\ j' = j - 1$), d.h. $e = a^k$.

  Aus der Minimalität von k folgt $\mathrm{ord}(a) = k$.

Kapitel V – Algebra; Gruppen

- Ordnung eines Gruppenelements

  Satz: Sei $\langle S, \circ \rangle$ eine endliche Gruppe. Dann hat auch jedes Element in S endliche Ordnung.

  $a^0\ a^1\ a^2\ a^3\ a^4\ a^5\ a^6\ a^7\ a^8$

  Beweis: Sei $a \in S$ beliebig. Mindestens zwei von $a^0, \dots, a^{|S|}$ sind gleich (Schubfachprinzip). Wähle $0 \le j < k \le |S|$ mit $a^j = a^k$ und k minimal.

  Durch Multiplikation mit a^{-j} erhält man $a^0 = a^{k-j}$.

  Aus der Minimalität von k folgt $j = 0$ (nehme sonst $k' = k - 1,\ j' = j - 1$), d.h. $e = a^k$.

  Aus der Minimalität von k folgt $\mathrm{ord}(a) = k$.

10

Vorlesung Diskrete Strukturen WS 13/14
Prof. Dr. J. Esparza – Institut für Informatik, TU München

- Untergruppen

Definition: Ist $\langle S,\circ\rangle$ eine Gruppe und $S' \subseteq S$, so heißt $\langle S',\circ\rangle$ Untergruppe von $\langle S,\circ\rangle$, wenn sie selbst eine Gruppe ist.

Beispiele:

- $\langle \mathbb{Z},+\rangle$ ist Untergruppe von $\langle \mathbb{Q},+\rangle$.
- $\langle \{0,2,4\},+_6\rangle$ ist Untergruppe von $\langle \mathbb{Z}_6,+_6\rangle$
- $\langle \mathbb{Z}_n,+_n\rangle$ ist nicht Untergruppe zu $\langle \mathbb{Z},+\rangle$, da sich die Operationen unterscheiden.

Kapitel V – Algebra; Gruppen

- Untergruppen

Lemma: Sei G eine Gruppe und sei H eine Untergruppe von G. Die neutralen Elemente von G und H sind identisch.

Beweis: Seien e_H und e_G die neutralen Elemente von H und G. Dann gilt

$$e_H \circ e_H = e_H = e_G \circ e_H$$

und daraus folgt (Kürzungsregel) $e_H = e_G$. □

Kapitel V – Algebra; Gruppen

- Untergruppen

Satz: Seien $\langle S_1,\circ\rangle$ und $\langle S_2,\circ\rangle$ Untergruppen von $\langle S,\circ\rangle$. Dann ist auch $\langle S_1 \cap S_2,\circ\rangle$ eine Untergruppe von $\langle S,\circ\rangle$.

Beweis: Aus dem vorigen Lemma folgt $e \in S_1$ und $e \in S_2$ und so $e \in S_1 \cap S_2$.

Sei $a \in S_1 \cap S_2$. Aus der Eindeutigkeit von a^{-1} in $\langle S,\circ\rangle$ folgt, dass a^{-1}auch das inverse Element von a in $\langle S_1,\circ\rangle$ und $\langle S_2,\circ\rangle$ ist. Es gilt also $a^{-1} \in S_1$ und $a^{-1} \in S_2$ und damit $a^{-1} \in S_1 \cap S_2$. □

Kapitel V – Algebra; Gruppen

- Untergruppen

Satz: Sei $\langle S,\circ\rangle$ eine endliche Gruppe und a $\in S$. Dann ist $\langle \{a^0, a^1, \dots, a^{\mathrm{ord}(a)-1}\},\circ\rangle$ eine Untergruppe von $\langle S,\circ\rangle$.

Beweis: Folgt sofort aus $a^0 = a^{\mathrm{ord}(a)} = e$. □

Kapitel V – Algebra; Gruppen

- Untergru

Satz: Sei ⟨ … a ∈ S.

Dann ist ⟨

Untergrup

Beweis: F … e. □

New

Size

Current page size

Style

5mm

7mm

Orientation

Pages

1

OK

Cancel

$a^5 = e$

$a^2 \circ a^3 = a^5 = e$

$a^4 \circ a^1 = a^5 = e$

$a^{-2} = a^3$

$= a^7 = a^2 \circ a^5 = a^2$

$a \circ a = e$ $\quad$ $a \circ a = e$

$a^3 = a^{-2}$

Kapitel V – Algebra; Gruppen

- Nebenklassen

Definition: Sei $H = \langle T, \circ \rangle$ eine Untergruppe von $G = \langle S, \circ \rangle$ und sei $b \in G$. Dann heißt

$$T \circ b := \{ c \circ b \mid c \in T \} =: H \circ b$$

eine rechte Nebenklasse von H in G und

$$b \circ T := \{ b \circ c \mid c \in T \} =: b \circ H$$

eine linke Nebenklasse von H in G (engl. coset).

Der Index $ind_G(H)$ von H in G ist die Anzahl verschiedener linke Nebenklassen von H in G.

Kapitel V – Algebra; Gruppen

- Nebenklassen

Beispiel:

$H = \langle \{0,3,6,9\}, +_{12} \rangle$ bildet eine Untergruppe $\langle \mathbb{Z}_{12}, +_{12} \rangle$ mit 3 verschiedenen Nebenklassen:

$$0 \circ H = 3 \circ H = 6 \circ H = 9 \circ H = \{0,3,6,9\}$$

$$1 \circ H = 4 \circ H = 7 \circ H = 10 \circ H = \{1,4,7,10\}$$

$$2 \circ H = 5 \circ H = 8 \circ H = 11 \circ H = \{2,5,8,11\}$$

- Nebenklassen

$T \subseteq S$

Definition: Sei $H = \langle T, \circ \rangle$ eine Untergruppe von $G = \langle S, \circ \rangle$ und sei $b \in G$. Dann heißt

$$T \circ b := \{ c \circ b \mid c \in T \} =: H \circ b$$

eine rechte Nebenklasse von H in G und

$$b \circ T := \{ b \circ c \mid c \in T \} =: b \circ H$$

eine linke Nebenklasse von H in G (engl. coset).

Der Index $ind_G(H)$ von H in G ist die Anzahl verschiedener linke Nebenklassen von H in G.

- Nebenklassen

$\langle \mathbb{Z}_{12}, +_{12} \rangle$

Beispiel:

$H = \langle \{0,3,6,9\}, +_{12} \rangle$ bildet eine Untergruppe $\langle \mathbb{Z}_{12}, +_{12} \rangle$ mit 3 verschiedenen Nebenklassen:

$$0 \circ H = 3 \circ H = 6 \circ H = 9 \circ H = \{0,3,6,9\}$$

$$1 \circ H = 4 \circ H = 7 \circ H = 10 \circ H = \{1,4,7,10\}$$

$$2 \circ H = 5 \circ H = 8 \circ H = 11 \circ H = \{2,5,8,11\}$$

- Nebenklassen

$\langle \mathbb{Z}_{12}, +_{12} \rangle$

3 linke Nebenklassen

Beispiel:

$H = \langle \{0,3,6,9\}, +_{12} \rangle$ bildet eine Untergruppe $\langle \mathbb{Z}_{12}, +_{12} \rangle$ mit 3 verschiedenen Nebenklassen:

$$0 \circ H = 3 \circ H = 6 \circ H = 9 \circ H = \{0,3,6,9\}$$

$H \circ b$

$$1 \circ H = 4 \circ H = 7 \circ H = 10 \circ H = \{1,4,7,10\}$$

$$2 \circ H = 5 \circ H = 8 \circ H = 11 \circ H = \{2,5,8,11\}$$

Kapitel V – Algebra; Gruppen

- Nebenkla

3 linke Nebenklassen

Beispiel:

$H = \langle \{0,3$ ... uppe

$\langle \mathbb{Z}_{12}, +_{12}$ ... assen:

$0 \circ H = 3$ ... $6,9\}$

$H \circ b$

$1 \circ H = 4$ ... $,7,10\}$

$2 \circ H = 5$ ... $5,8,11\}$

New
Size
Current page size
Style
5mm
7mm
Orientation
Pages
1
OK
Cancel

16

Vorlesung Diskrete Strukturen WS 13/14
Prof. Dr. J. Esparza – Institut für Informatik, TU München

Kapitel V – Algebra; Gruppen

- Nebenklassen

  Satz: Sei H Untergruppe von G. Dann bildet die Menge der rechten (linken) Nebenklassen von H eine Partition (Zerlegung in disjunkte Teilmengen) von G.

  Beweis: Zuerst zeigen wir $H \circ h = H$ für alle $h \in H$.

  – $H \circ h \subseteq H$ weil H abgeschlossen bzgl. $\circ$ ist.

  – Sei nun $h' \in H$ beliebig. Es gilt $h' \circ h^{-1} \in H$ und so $h' = h' \circ (h^{-1} \circ h) = (h' \circ h^{-1}) \circ h \in H \circ h$.

Kapitel V – Algebra; Gruppen

- Nebenklassen

  Beweis (Fort.): Wir zeigen nun:

  - $G \subseteq \bigcup_{a \in G} H \circ a$.

    Folgt aus $e \in H$.

  - Wenn $H \circ a \cap H \circ b \neq 0$ dann $H \circ a = H \circ b$.

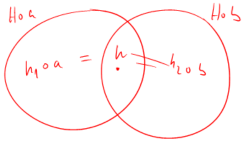
    Aus $H \circ a \cap H \circ b \neq 0$ folgt, dass es $h_1, h_2 \in H$ gibt mit $h_1 \circ a = h_2 \circ b$. Dann:

    $$H \circ b = H \circ h_2^{-1} \circ h_1 \circ a = H \circ a \qquad \square$$

Kapitel V – Algebra; Gruppen

- Nebenklassen

  Beweis (Fort.): Wir zeigen nun:



  - $G \subseteq \bigcup_{a \in G} H \circ a$.

    Folgt aus $e \in H$.

  - Wenn $H \circ a \cap H \circ b \neq 0$ dann $H \circ a = H \circ b$.

    Aus $H \circ a \cap H \circ b \neq 0$ folgt, dass es $h_1, h_2 \in H$ gibt mit $h_1 \circ a = h_2 \circ b$. Dann:

    $$H \circ b = H \circ h_2^{-1} \circ h_1 \circ a = H \circ a \qquad \square$$

Kapitel V – Algebra; Gruppen

- Nebenklassen

  Satz (Lagrange): Sei G eine endliche Gruppe und H eine Untergruppe in G. Es gilt:

  (1) Alle Nebenklassen von H in G haben gleich viele Elemente.

  (2) $|G| = \mathrm{ind}_G(H) \cdot |H|$

  (3) $|H|$ teilt $|G|$.

  Korollar: Sei G eine endliche Gruppe und sei a ein Element von G. Es gilt: $\mathrm{ord}(a)$ teilt $|G|$.

Kapitel V – Algebra; Gruppen

- Nebenklassen

  $x \circ h = h'$

  Satz: Sei H Untergruppe von G. Dann bildet die Menge der rechten (linken) Nebenklassen von H eine Partition (Zerlegung in disjunkte Teilmengen) von G.

  Beweis: Zuerst zeigen wir $H \circ h = H$ für alle $h \in H$.

  – $H \circ h \subseteq H$ weil H abgeschlossen bzgl. $\circ$ ist.

  – Sei nun $h' \in H$ beliebig. Es gilt $h' \circ h^{-1} \in H$ und so $h' = h' \circ (h^{-1} \circ h) = (h' \circ h^{-1}) \circ h \in H \circ h$.

Kapitel V – Algebra; Gruppen

- Eigenschaften von Gruppen

  Beweis (Fort.):

  (3) Beweis von $a = (a^{-1})^{-1}$

  $(a^{-1})^{-1} =: b = b \circ e = b \circ (a^{-1} \circ a)$

  $= (b \circ a^{-1}) \circ a = e \circ a = a$ □

  (4) Beweis von $a \circ c = b \circ c \rightarrow a = b$

  $b = b \circ (c \circ c^{-1}) = (b \circ c) \circ c^{-1}$

  $= (a \circ c) \circ c^{-1} = a \circ (c \circ c^{-1}) = a$ □

Kapitel V – Algebra; Gruppen

- Nebenklassen

  Beweis:

  (1) Aus der Injektivität von $\circ$ folgt $|H \circ a| = |H|$ für alle $a \in G$.

  (2) Folgt aus dem letzten Satz.

  (3) Folgt aus (2) . □

Kapitel V – Algebra; Gruppen

- Multiplikative Gruppen modulo n
  - $\langle \mathbb{Z}_4 \setminus \{0\}, *_4 \rangle$ und $\langle \mathbb{Z}_9 \setminus \{0\}, *_9 \rangle$ sind keine Gruppen (2 bzw. 3 haben kein inverses Element.
  - Sei $\mathbb{Z}_n^*$ die Menge der Zahlen $i \in \{1, \ldots, n-1\}$, die teilerfremd zu n sind: $\mathbb{Z}_4^* = \{1,3\}$, $\mathbb{Z}_5^* = \{1,2,3,4\}$, $\mathbb{Z}_9^* = \{1,2,4,5,7,8\}$.
  - Wir zeigen, dass $\langle \mathbb{Z}_n^*, *_n \rangle$ immer eine Gruppe ist. Man nennt sie die multiplikative Gruppe modulo n.
  - Wir brauchen einen Exkurs über größte gemeinsame Teiler.

$\langle \{1,3\}, *_4 \rangle$

Kapitel V – Algebra; Gruppen

- Multiplikative Gruppen modulo n $\langle \quad , *_n \rangle$
  - $\langle \mathbb{Z}_4 \setminus \{0\},\ *_4 \rangle$ und $\langle \mathbb{Z}_9 \setminus \{0\},\ *_9 \rangle$ sind keine Gruppen (2 bzw. 3 haben kein inverses Element. $\{1, \ldots, n-1\}$
  - Sei $\mathbb{Z}_n^*$ die Menge der Zahlen $i \in \{1, \ldots, n-1\}$, die teilerfremd zu n sind: $\mathbb{Z}_4^* = \{1,3\}$, $\mathbb{Z}_5^* = \{1,2,3,4\}$, $\mathbb{Z}_9^* = \{1,2,4,5,7,8\}$.
  - Wir zeigen, dass $\langle \mathbb{Z}_n^*, *_n \rangle$ immer eine Gruppe ist. Man nennt sie die multiplikative Gruppe modulo n.
  - Wir brauchen einen Exkurs über größte gemeinsame Teiler.

Kapitel V – Algebra; Gruppen

- Größter gemeinsamer Teiler

  Definition: Seien $x, y \in \mathbb{N}$. Der größte gemeinsame Teiler $\mathrm{ggT}(x, y)$ von y und y ist die größte natürliche Zahl, die sowohl x als auch y teilt.

  Mit $y|x$ („y teilt x“) bezeichnen wir, dass $(x \bmod \mathrm{y}) = 0$ ist.

  Fakt: x und y sind teilerfremd gdw. $\mathrm{ggT}(x, y) = 1$.