WS 2014/15

Diskrete Strukturen

Kapitel 5: Algebraische Strukturen (Gruppen)

Hans-Joachim Bungartz

Lehrstuhl für wissenschaftliches Rechnen
Fakultät für Informatik
Technische Universität München

http://www5.in.tum.de/wiki/index.php/Diskrete_Strukturen_-_Winter_14

Kapitel 5: Algebraische Strukturen (Gruppen)

- Algebraische Strukturen
  - Grundlagen
  - Gruppen
  - Endliche Körper

- 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, bezeichnet als 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 $a = b$.

- Eigenschaften von Gruppen:

(5) (Eindeutige Lösung linearer Gleichungen):
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 $y \in S$: $y \circ a = b$.

- Eigenschaften von Gruppen:

  Beweis:

  (1) Beweis der Eindeutigkeit von e:

  Seien e_1, e_2 neutrale Elemente. Dann gilt

  $$e_1 = e_1 \circ e_2 = e_2 \,.\, \square$$

  (2) Beweis der Eindeutigkeit von a^{-1}:

  Seien i_1, i_2 inverse Elemente von a.

  $$i_1 = i_1 \circ e = i_1 \circ (a \circ i_2)$$
  $$= (i_1 \circ a) \circ i_2 = e \circ i_2 = i_2. \ \square$$

- Eigenschaften von Gruppen

  Beweis (Fort.):

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

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

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

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

- 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.

- Ordnung eines Gruppenelements:

  Definition: Sei $\langle S, \circ \rangle$ eine Gruppe mit neutralem Element e und sei $a \in S$.

  Die Ordnung $\mathrm{ord}(a)$ von a ist die kleinste Zahl $r \in \mathbb{N}$, sodass $a^r = e$. Falls kein solches r existiert, dann ist $\mathrm{ord}(a) := \infty$.

- Ordnung eines Gruppenelements:
  Beispiele:

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

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

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

- 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 $a^0, \ldots, a^{|S|}$ sind gleich (Schubfachprinzip). Wähle $0 \leq j < k \leq |S|$ 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 $j = 0$ (sonst nehme man $k' = k - 1$, $j' = j - 1$), d.h. $e = a^k$.

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

- 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.

- 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) $e_H = e_G$. □

- 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 damit gilt $e \in S_1 \cap S_2$.

  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 $a^{-1} \in S_1 \cap S_2$. □

- Untergruppen:

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

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

- Nebenklassen:

  Definition: Sei $H = \langle T, \circ \rangle$ eine Untergruppe von $G = \langle S, \circ \rangle$ und sei $b \in S$. 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 $\mathrm{ind}_G(H)$ von H in G ist die Anzahl von verschiedenen linken Nebenklassen von H in G.

- Nebenklassen:

  Beispiel:

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

  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 daher $h' = h' \circ (h^{-1} \circ h) = (h' \circ h^{-1}) \circ h \in H \circ h$.

- Nebenklassen:

  Beweis (Fort.): Wir zeigen nun:

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

    Folgt aus $e \in H$.
  - Wenn $H \circ a \cap H \circ b \neq \emptyset$, dann $H \circ a = H \circ b$:

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

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

- Nebenklassen:

  Satz (Lagrange): Sei G eine endliche Gruppe und H eine Untergruppe von 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 $|G|$.

- Nebenklassen:

  Beweis:

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

  (2) Folgt aus (1) sowie dem letzten Satz.

  (3) Folgt aus (2). □

- 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.

- Größter gemeinsamer Teiler:

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

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

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

- Größter gemeinsamer Teiler:

  Satz: Seien $x, y \in \mathbb{N}$ mit $x \leq y$.

  (1) Wenn $(y \bmod x) = 0$, dann
  $$\mathrm{ggT}(x, y) = x.$$

  (2) Wenn $(y \bmod x) > 0$, dann
  $$\mathrm{ggT}(x, y) = \mathrm{ggT}(y \bmod x, x).$$

- Größter gemeinsamer Teiler:

  Beweis: (1) Klar.

  (2) Es gilt $y = (y \bmod x) + \lfloor y/x \rfloor \cdot x$.

  Daraus folgt für alle $z \in \mathbb{N}$:

  $$(z|x \text{ und } z|y) \text{ gdw. } (z|x \text{ und } z|(y \bmod x)).$$

  (Zur Erinnerung: $z|x$ bedeutet „z teilt x“.)

  Damit haben (x, y) und $(x, y \bmod x)$ dieselben gemeinsamen Teiler, und so insbesondere

  $$\mathrm{ggT}(x, y) = \mathrm{ggT}(y \bmod x, x). \square$$

- Größter gemeinsamer Teiler:

  Der Satz führt zum Euklidischen Algorithmus zur Berechnung vom ggT zweier Zahlen:

Procedure ggT $(x, y \in \mathbb{N}$ mit $x \leq y)$
  if $(y \bmod x) = 0$ **then return** x;
  else return $\mathrm{ggT}(y \bmod x, x)$;

(Euklid von Alexandria, ca. 325–265 v. Chr.)

- Größter gemeinsamer Teiler:

Satz: Seien $x, y \in \mathbb{N}$. Es gibt $a, b \in \mathbb{Z}$ mit

$$\mathrm{ggT}(x, y) = ax + by.$$

Beweis: Durch Induktion über $\max\{x, y\}$.

Basis: $\max\{x, y\} = 1$.

Dann $x = 1 = y$ und $\mathrm{ggT}(x, y) = 1 = 1 \cdot x + 0 \cdot y$.

Schritt: $\max\{x, y\} > 1$.

O.B.d.A. sei $x \leq y$. Wir betrachten zwei Fälle.

Fall 1: $(y \bmod x) = 0$. Dann
$\mathrm{ggT}(x, y) = x = 1 \cdot x + 0 \cdot y$.

- Größter gemeinsamer Teiler:

  Fall 2: $(y \bmod x) > 0$. In diesem Fall gelten $x < y$ und $\mathrm{ggT}(x, y) = \mathrm{ggT}(y \bmod x, x)$. Wir haben

  $$\max\{x, y \bmod x\} = x < y \leq \max\{x, y\}.$$

  Nach Induktionsannahme gibt es $a', b' \in \mathbb{Z}$ mit

  $$\mathrm{ggT}(x, y) = \mathrm{ggT}(y \bmod x, x) = a'(y \bmod x) + b'x.$$

  Mit $y \bmod x = y - \lfloor y/x \rfloor \cdot x$ erhalten wir

  $$\begin{aligned} \mathrm{ggT}(x, y) &= a'(y - \lfloor y/x \rfloor \cdot x) + b'x \\ &= (b' - \lfloor y/x \rfloor a')\, x + a'y. \end{aligned}$$ □

- Größter gemeinsamer Teiler:

  Der Beweis des Satzes führt zu einem Algorithmus für die Berechnung der Zahlen a und b, dem erweiterten Euklidischen Algorithmus:

Procedure erwggT($x, y \in \mathbb{N}$ mit $x \leq y$)

if $(y \bmod x) = 0$ **then return** $(1, 0)$;

else $(a', b') :=$ erwggT$(y \bmod x, x)$;

$(a, b) := (b' - \lfloor y/x \rfloor a',\ a')$;

return (a, b);

- Größter gemeinsamer Teiler:

  Beispiel mit $x = 45, y = 63$:

$$\begin{aligned}
\text{ggT}(45,63) \quad & 9 = \big(1 - \lfloor 63/45 \rfloor \cdot (-2)\big) \cdot 45 + (-2) \cdot 63 \\
= \quad & = 3 \cdot 45 + (-2) \cdot 63 \\
\text{ggT}(18,45) \quad & 9 = (0 - \lfloor 45/18 \rfloor \cdot 1) \cdot 18 + 1 \cdot 45 \\
= \quad & = -2 \cdot 18 + 1 \cdot 45 \\
\text{ggT}(9,18) \quad & 9 = 1 \cdot 9 + 0 \cdot 18 \\
= & \\
9 &
\end{aligned}$$

- Multiplikative Gruppen modulo n:

  Satz: $\langle \mathbb{Z}_n^*, *_n \rangle$ ist eine Gruppe für alle $n \geq 1$.

  Beweis: Wir zeigen, dass jedes $x \in \mathbb{Z}_n^*$ ein inverses Element hat.

  Sei $x \in \mathbb{Z}_n^*$ beliebig. Es gilt $\mathrm{ggT}(x, n) = 1$.

  Der erwggT berechnet $a, b \in \mathbb{Z}$ mit $ax + bn = 1$.

  Es gilt also $a *_n x +_n b *_n n = 1$.

  Aus $(b *_n n) = 0$ folgt $(a *_n x) = 1$.

  Wähle $x^{-1} := a \bmod n$. □

- Multiplikative Gruppen modulo n:
  - Korollar: Sei $\varphi(n) = |\mathbb{Z}_n^*|$. Ist n Primzahl, dann gilt $\varphi(n) = n - 1$.

- Zyklische Gruppen:

  Definition: Eine Gruppe $\langle S, \circ \rangle$ heißt zyklisch, wenn es ein $a \in S$ gibt, sodass $S = \{a^i \mid i \in \mathbb{Z}\}$.

  Ein Element a mit $S = \{a^i \mid i \in \mathbb{Z}\}$ nennt man erzeugendes Element der Gruppe.

  Beispiele: $\langle \mathbb{Z}, + \rangle$ und $\langle \mathbb{Z}_n, +_n \rangle$ sind zyklisch.

  Aufgabe: Erzeugendes Element?

- Zyklische Gruppen:

  Definition: Ein Isomorphismus zwischen zwei Gruppen $\langle S_1, \circ_1 \rangle$ und $\langle S_2, \circ_2 \rangle$ ist eine Bijektion $f: S_1 \to S_2$ mit $f(a \circ_1 b) = f(a) \circ_2 f(b)$ für alle $a, b \in S_1$.

  Zwei Gruppen sind isomorph, wenn es einen Isomorphismus zwischen ihnen gibt.

  Beispiel: Die Bijektion $\{0, \ldots, 3\} \to \{1, \ldots, 4\}$ mit $0 \mapsto 1$, $1 \mapsto 2$, $2 \mapsto 4$, $3 \mapsto 3$ ist ein Isomorphismus zwischen $\langle \mathbb{Z}_4, +_4 \rangle$ und $\langle \mathbb{Z}_5 \setminus \{0\}, *_5 \rangle$.

- Zyklische Gruppen:

  Satz: Sei $G = \langle S, \circ \rangle$ eine zyklische Gruppe.

  (1) Ist S unendlich, dann ist G isomorph zu $\langle \mathbb{Z}, + \rangle$.

  (2) Ist S endlich, dann ist G isomorph zu $\langle \mathbb{Z}_{|S|}, +_{|S|} \rangle$.

  Beweis: (1) Sei G zyklisch und unendlich.

  Es existiert $a \in S$ mit $S = \{a^i \mid i \in \mathbb{Z}\}$.

  Wir zeigen: Die Abbildung $f: \mathbb{Z} \to S$ definiert durch $f(i) = a^i$ ist ein Isomorphismus zwischen G und $\langle \mathbb{Z}, + \rangle$:

- Zyklische Gruppen:

  Beweis (Fort.):

  - f ist surjektiv: Folgt aus der Definition einer zyklischen Gruppe.
  - f ist injektiv: Wäre f nicht injektiv, dann gäbe es i, j mit $i > j$ und $a^i = a^j$. Dann wäre $a^{i-j} = e$ und somit $S \subseteq \{a^0, \ldots, a^{i-j-1}\}$, im Widerspruch zur Annahme, dass S unendlich ist.
  - $\forall i, j \in \mathbb{Z} : f(i+j) = f(i) \circ f(j)$:

    Es gilt: $f(i+j) = a^{i+j} = a^i \circ a^j = f(i) \circ f(j)$.

- Zyklische Gruppen:

  Beweis (Fort.):

  (2) Sei G zyklisch und endlich mit $|G| = m$.

  Analog zu (1):

  Es existiert $a \in S$ mit $S = \{a^0, a^1, \ldots, a^{m-1}\}$.

  Beweisskizze: Die Abbildung $f: \{0,1, \ldots, m-1\} \to S$ definiert durch $f(i) = a^i$ ist ein Isomorphismus zwischen G und $\langle \mathbb{Z}_m, +_m \rangle$. Details analog zu (1).

- Symmetrische Gruppen:

  Definition: Eine Permutation ist eine bijektive Abbildung einer endlichen Menge auf sich selbst.

  Sei U_n die Menge aller Permutationen $\{1, \ldots, n\} \to \{1, \ldots, n\}$.

  Die symmetrische Gruppe für n Elemente ist die Gruppe $S_n = \langle U_n, \circ \rangle$, wobei „$\circ$“ die Komposition von Abbildungen bezeichnet.

- Für $n = 3$ enthält S_3 sechs verschieden Permutationen:

∘	(1)(2)(3)	(1)(23)	(12)(3)	(13)(2)	(123)	(132)
(1)(2)(3)	(1)(2)(3)	(1)(23)	(12)(3)	(13)(2)	(123)	(123)
(1)(23)	(1)(23)	(1)(2)(3)	(132)	(123)	(13)(2)	(12)(3)
(12)(3)						
(13)(2)			…			
(123)						
(132)						

Praktische Anwendungen in der Informatik:

- Lineare Modelle
- Lineare Gleichungssysteme
- Zahlreiche Varianten des Euklidischen Algorithmus
- Rechnen mit Booleschen Werten und Operationen
- Basis von Verschlüsselungsverfahren