Mathematik für Informatiker 1 – Tutorium

Malte Isberner

16.1.2014

Thema heute

Thema heute: Algebra (Teil 2)

- Faktorstrukturen
- Homomorphismen

Faktorstrukturen

- Basieren auf speziellen Unterstrukturen
  - Gruppe $\rightarrow$ Normalteiler
  - Ring $\rightarrow$ Ideale

Untergruppen (Wdh.)

Untergruppe

Sei $\langle G, \oplus \rangle$ eine Gruppe mit neutralem Element $e \in G$. Eine Teilmenge $H \subseteq G$ heißt Untergruppe von G („$H \leq G$“) genau dann, wenn $\langle H, \oplus \rangle$ eine Gruppe mit neutralem Element e ist.

Nachweis Untergruppe

Sei $H \subseteq G$. Zu zeigen ist:

- $\forall x, y \in H.\ (x \oplus y) \in H$ (Abgeschlossenheit)
- $e \in H$ (Existenz des neutralen Elementes)
- $\forall x \in H.\ x^{-1} \in H$ (Existenz der inversen Elemente)

Wichtiges Resultat: Satz von Lagrange (für endliche Gruppen G)

$$H \leq G \Rightarrow |H| \,\Big|\, |G|$$

Nebenklassen

Nebenklassen: Übergang von Rechnen mit Elementen der Gruppe zu Rechnen mit Teilmengen (Untergruppen) der Gruppe

Nebenklassen

Sei $\langle G, \oplus \rangle$ eine Gruppe und $H \leq G$. Dann bezeichnen

- $a \oplus H =_{df} \{a \oplus x \mid x \in H\}$
- $H \oplus a =_{df} \{x \oplus a \mid x \in H\}$

die Menge der Links- bzw. Rechtsnebenklassen von H.

Nebenklassen – Beispiele

- $2 + 5\mathbb{Z} = 2 + \{\ldots, -10, -5, 0, 5, 10, \ldots\} = \{\ldots, -8, -3, 2, 7, 12, \ldots\}$
- $(1\ 3) \circ \{\mathrm{id}, (1\ 2)\} = \{(1\ 3), (1\ 2\ 3)\}$
- $\{\mathrm{id}, (1\ 2)\} \circ (1\ 3) = \{(1\ 3), (1\ 3\ 2)\}$

Achtung: Links- und Rechtsnebenklassen i.A. nicht identisch!

Normalteiler

Normalteiler: Untergruppen, bei denen Rechts- und Linksnebenklassen für beliebiges $a \in G$ identisch sind

$\Rightarrow$ in kommutativen Gruppen ist jede Untergruppe Normalteiler!

- Existieren auch in nicht-kommutativen Gruppen, bspw. ist $\langle \{\mathrm{id}, (1\ 2\ 3), (1\ 3\ 2)\}, \circ\rangle \lhd \langle S_3, \circ \rangle$

Bedeutung: Mit Nebenklassen der Normalteiler lässt sich rechnen

„Addition" von Nebenklassen

Sei N ein Normalteiler von $\langle G, \oplus\rangle$ und $a, b \in G$. Die Verknüpfung von Nebenklassen von N, $\oplus_N$, lässt sich definieren als

$$(a \oplus N) \oplus_N (b \oplus N) =_{df} (a \oplus b) \oplus N$$

und die Menge der Nebenklassen von N bildet mit $\oplus_N$ eine Gruppe, die sog. Faktorgruppe von G bzgl. N

$$G/N =_{df} \{a \oplus N \mid a \in G\}.$$

Normalteiler (Forts.)

Korollar aus dem Satz von Lagrange (für endliche Gruppen G):

$$|G/H| = |G|/|H|$$

Beispiel: $\mathbb{Z}/n\mathbb{Z}$

- Bekannt: $\langle \mathbb{Z}, + \rangle$ ist kommutative Gruppe
- Für $n \in \mathbb{N}$ ist $n\mathbb{Z} = \{n \cdot z \mid z \in \mathbb{Z}\}$ Untergruppe (also Normalteiler) von $\mathbb{Z}$
- Also ist $\mathbb{Z}/n\mathbb{Z} = \{a + n\mathbb{Z} \mid a \in \mathbb{Z}\}$ Faktorgruppe mit Verknüpfung $+_{n\mathbb{Z}}$:

$$(a + n\mathbb{Z}) +_{n\mathbb{Z}} (b + n\mathbb{Z}) = (a + b) + n\mathbb{Z}$$

Beobachtung: „Entspricht“ Addition modulo n

Homomorphismen

Homomorphismus: Strukturerhaltende Abbildung

- Für Gruppen $\langle G_1, \oplus_1 \rangle, \langle G_2, \oplus_2 \rangle$:
  - $h \colon G_1 \to G_2$ ist Homomorphismus gdw. $\forall a, b \in G_1.\ h(a \oplus_1 b) = h(a) \oplus_2 h(b)$ gilt
  - Außerdem gilt $h(e_1) = e_2$ (e_1 bzw. e_2 neutrales Element von G_1 bzw. G_2) und $h\left(a^{-1}\right) = h(a)^{-1} \ \ \forall a \in G$.

Klassifizierung (nach Injektivität/Surjektivität/Bijektivität):

- ist h injektiv, nennt man h Monomorphismus
- ist h surjektiv: Epimorphismus
- ist h bijektiv: Isomorphismus
- Spezialfall $\langle G_1, \oplus_1 \rangle = \langle G_2, \oplus_2 \rangle$: Endomorphismus, falls h bijektiv: Automorphismus)

Homomorphie – Beispiele

Beobachtung (2 Folien vorher)

- Verknüpfung $+_{n\mathbb{Z}}$ von Nebenklassen von $n\mathbb{Z}$ ($\mathbb{Z}/n\mathbb{Z}$) entspricht Addition modulo n (d.h. $\langle \mathbb{Z}_n, +_n \rangle$)
- Formal: $\langle \mathbb{Z}/n\mathbb{Z}, +_{n\mathbb{Z}} \rangle$ und $\langle \mathbb{Z}_n, +_n \rangle$ sind isomorph

Weitere Beispiele

- Für $N \triangleleft G$ ist $f_N \colon G \to G/N$, $f_N(g) = g \oplus N$ ein Gruppenepimorphismus.
- Für $b \in G$ ist $A_b \colon G \to G$ mit $A_b(g) =_{df} b^{-1} \oplus g \oplus b$ ein Gruppenautomorphismus
- Die Gruppe aller Automorphismen auf G bildet mit $\circ$ eine Gruppe