C: Algebraische Strukturen

Algebra: „Rechnen“. Menge mit Verknüpfungen: $(\mathbb{N}_0, +)$,
$(\mathbb{R}, +, \cdot)$,
$(\mathcal{P}(X), \cup, \cap)$,
$(\mathbb{R}^{n\times n}, +, \cdot)$

Informatik:
- Boolsche Algebren
- Relationenalgebra (Datenbanken)
- Computeralgebra

29 Gruppen

29.1 Bedeutung für die Informatik

- „Mathematik ist die Lehre von den guten Beschreibungen.“ (A. Beutelspacher)
  Die Gruppentheorie arbeitet grundlegende Gemeinsamkeiten hinter vielen Problemen heraus. Ihre Aussagen können dann für all diese Probleme angewandt werden.
- Gruppen sind abstrakte Modelle für Mengen, auf denen eine Verknüpfung (wie Addition oder Multiplikation) definiert ist.
- Gruppen: „einfachste Form sinnvollen Rechnens“

29.2 Definition

Sei G eine Menge. Eine Abbildung $f : G \times G \to G$ heißt *Verknüpfung* auf G. Schreibweise: Normalerweise nennen wir Verknüpfungen $+$, $\cdot$, $\circ$, $\otimes$, ... Statt $+(x, y)$ schreiben wir $x + y$. Ein Paar $(G, \circ)$ bestehend aus einer Menge G und einer Verknüpfung $\circ$ heißt Gruppe, wenn folgendes gilt:

- Für alle $x, y, z \in G$ gilt $(x \circ y) \circ z = x \circ (y \circ z)$. **„Assoziativgesetz“**
- Es existiert ein $e \in G$, so daß

(a) für alle $x \in G$ gilt: $e \circ x = x$; **„(Links-) Neutrales Element“**

(b) für alle $x \in G$ existiert ein $y \in G$ mit $y \circ x = e$. **„Inverses Element“**.

Gilt weiter $x \circ y = y \circ x$ für alle $x, y \in G$, so heißt G *kommutative Gruppe* oder *abelsche Gruppe*.
$|G|$ heißt **Ordnung** der Gruppe. Ist $|G| < \infty$, spricht man von einer **endlichen** Gruppe. (Vergleiche auch 8.2 in MfI 1.)

29.3 Beispiele

a) Die nichtnegativen ganzen Zahlen $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$ mit der Addition bilden ein kommutatives Monoid $(\mathbb{N}_0, +)$ mit 0 als neutralem Element. $(\mathbb{N}_0, +)$ ist keine Gruppe, da es kein $y \in \mathbb{N}_0$ existiert mit $y + 1 = 0$.

b) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{R}^2, +)$ sind abelsche Gruppen.

c) $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$ sind kommutative Gruppen, $(\mathbb{Q}, \cdot)$ jedoch nicht.

d) Sei X eine Menge. Sei $\mathrm{Sym}(x) = \{f : X \to X \mid f \text{ bijektiv}\}$. Mit der Hintereinanderausführung $\circ$ ist $\mathrm{Sym}(x)$ eine Gruppe. [1]

e) Sei G die Menge der invertierbaren $n \times n$-Matrizen über $\mathbb{R}$. Dann ist G mit der normalen Matrixmultiplikation eine Gruppe.

29.4 Satz: Eindeutigkeit von neutralen Elementen und inversen Elementen

Sei G eine Gruppe. Sei $e \in G$ ein neutrales Element. Dann gilt:

(a) Sei $a \in G$. Sei $b \in G$ mit $b \circ a = e$. Dann gilt $a \circ b = e$.

(b) Sei $a \in G$. Dann gilt $a \circ e = a$.

[1] Eine **Abbildung (Funktion)** zwischen zwei Mengen M, N ist eine Vorschrift $f : M \to N$, die jedem Element $x \in M$ ein eindeutiges Element $f(x) \in N$ zuordnet (vgl. MfI 1, 5.2). Die Abbildung f heißt **bijektiv**, falls zu jedem $y \in N$ ein $x \in M$ mit $f(x) = y$ existiert und für $x_1, x_2 \in M$ mit $x_1 \neq x_2$ stets $f(x_1) \neq f(x_2)$ gilt (vgl. MfI 1, 5.6).

(c) Seien e, e' (links-) neutrale Elemente. Dann gilt $e = e'$.

(d) Sei $a \in G$. Seien $a', a'' \in G$ mit $a' \circ a = e$ und $a'' \circ a = e$. Dann gilt $a' = a''$.

Beweis:

(a) Da G eine Gruppe ist, existiert ein $b' \in G$ mit $b' \circ b = e$. Dann gilt:

$$\begin{aligned} a \circ b &= e \circ (a \circ b) && \text{(Neutrales Element)} \\ &= (b' \circ b) \circ (a \circ b) && \text{(Wahl von } b') \\ &= b' \circ ((b \circ a) \circ b) && \text{(Assoziativität)} \\ &= b' \circ (e \circ b) \\ &= b' \circ b = e \ . \end{aligned}$$

(b) Es existiert ein $a' \in G$ mit $a' \circ a = e$. Dann gilt:

$$\begin{aligned} a \circ e &= a \circ (a' \circ a) && \text{(Wahl von } a') \\ &= (a \circ a') \circ a && \text{(Assoziativität)} \\ &= e \circ a && \text{(nach (a))} \\ &= a && \text{(neutrales Element) .} \end{aligned}$$

(c) Es gilt

$$e \overset{e' \text{ links-neutr.}}{=} e'e \overset{\text{(b)}}{=} e'.$$

(d) Es gilt

$$\begin{aligned} a'' &= a'' \circ e && \text{(nach (b))} \\ &= a'' \circ (a \circ a') && \text{(nach (a))} \\ &= (a'' \circ a) \circ a' && \text{(Assoziativität)} \\ &= e \circ a' && \text{(nach (*))} \\ &= a' \ . \end{aligned}$$

□

29.5 Definiton: Untergruppe

Sei $(G, \circ)$ eine Gruppe $U \subseteq G$. Ist U mit der auf $U \times U$ eingeschränkten Verknüpfung $\circ_{|U \times U}$ eine Gruppe, so heißt U Untergruppe von G. Wir schreiben $U \leq G$.

29.6 Definition: Schreibweise zu Gruppen

Sei G eine Gruppe. Wenn nichts anderes vereinfacht ist, bezeichnen wir die Verknüpfung mit $\cdot$ („Multiplikation"). Wenn keine Missverständnisse zu befürchten sind, lassen wir den Punkt weg, d.h., wir schreiben ab sofort $a \cdot b$. Das eindeutig bestimmte neutrale Element bezeichnen wir mit 1, das Inverse zu $a \in G$ bezeichnen wir mit a^{-1}. Allgemein für $z \in \mathbb{Z}$ setzen wir

$$a^z = \begin{cases} \underbrace{a \cdot \ldots \cdot a}_{z-\text{mal}}, & z \geq 1 \\ 1, & z = 0 \\ \underbrace{a^{-1} \cdot \ldots \cdot a^{-1}}_{|z|-mal}, & \text{sonst} \end{cases}$$

Abelsche Gruppen werden meist additiv geschrieben, d.h. wir bezeichnen mit

$+$ die Verknüpfungen

0 das neutrale Element

$-a$ das inverse Element zu a

$k \cdot a := \underbrace{a + \ldots + a}_{k-\text{mal}}$ für $k \in \mathbb{N}$

$0 \cdot a = 0$

$(-k) \cdot a = k \cdot (-a)$

29.7 Satz: Untergruppenkriterium

Sei G eine Gruppe, $U \subseteq G$, $U \neq \emptyset$. Folgende Aussagen sind äquivalent:

(i) $U \leq G$

(ii) $\forall a, b \in U : \; ab \in U \; \wedge \; a^{-1} \in U$

(iii) $\forall a, b \in U : \; ab^{-1} \in U$

Beweis:

(i)$\Rightarrow$ (ii): Da $\cdot_{|U \times U}$ Verknüpfung auf U, gilt $\cdot_{|_{U \times U}} : U \times U \to U$. Also ist $a \cdot b \in U$ für alle $a, b \in U$. Da U eine Gruppe ist, existiert ein $a' \in U$ mit $a'a = e$. Nach Satz 29.4 (d) ist $a' = a^{-1}$, also $a^{-1} \in U$.

(ii)$\Rightarrow$ (i) Offenbar gilt

$$\forall a, b, c \in U : (a \cdot b) \cdot c = a \cdot (b \cdot c), \tag{1}$$

da G eine Gruppe ist. Sei $a \in U$. Nach (ii) ist dann $a^{-1} \in U$, also auch $e = a^{-1}a \in U$ (wieder nach (ii)).

(i)$\Leftrightarrow$ (iii) Übung.

29.8 Beispiele

a) $(\mathbb{Z}, +)$ und $(\mathbb{Q}, +)$ sind Untergruppen von $(\mathbb{R}, +)$.

b) $(m\mathbb{Z}, +)$ mit $m\mathbb{Z} := \{mz \mid z \in \mathbb{Z}\}$ und $m \in \mathbb{N}$ ist Untergruppe von $(\mathbb{Z}, +)$.

c) Ist $(G, \bullet)$ eine Gruppe mit dem neutralen Element e, so sind $(\{e\}, \bullet)$ und $(G, \bullet)$ selbst Untergruppen von $(G, \bullet)$.

d) $U_1 \cap U_2 \leq G$

e) Ist: $M \subseteq G$, so definieren wir $\langle M \rangle := \bigcap \{U \mid M \leq U \leq G\}$ „Erzeugnis von M“
Zyklische Gruppen: Sei $g \in G$. Dann heißt

$$\langle g \rangle := \langle \{g\} \rangle \tag{2}$$

die von g erzeugte zyklische Gruppe.

29.9 Beispiel

$G = (\mathbb{Z} \times \mathbb{Z}, +)$. $U = \mathbb{Z} \times \{0\}$.
$(1, 3) + U = \mathbb{Z} \times \{3\}$.
$(7, 4) + U = \mathbb{Z} \times \{4\}$.
$(a, b) + U = \mathbb{Z} \times \{b\}$

29.10 Definition: Links- und Rechtsnebenklassen

Es sei G eine Gruppe mit Untergruppe U. Ferner sei $g \in G$. Dann nennen wir

$$gU := \{gu \mid u \in U\} \quad \textbf{Linksnebenklasse} \text{ von } g,$$
$$Ug := \{ug \mid u \in U\} \quad \textbf{Rechtsnebenklasse} \text{ von } g.$$

Bemerkung: Häufig betrachtet man nur Linksnebenklassen und nennt diese *Nebenklassen.*

29.11 Definition: Index

Es sei U eine Untergruppe von $(G, \bullet)$. Dann bezeichnen wir die Menge aller Linksnebenklassen mit G/U (gesprochen: „*G modulo U*“), und $G : U := |G/U|$ nennt man den **Index** von U in G.

29.12 Satz: Nebenklassenzerlegung einer Gruppe

Sei G eine Gruppe, $g, h \in G$ und $U \leq G$.

a) Ist $g \in U$, so gilt $gU = U$.

b) Es gilt $gU = hU$ oder $gU \cap hU = \emptyset$.

c) Die Menge der Nebenklassen von U sind in einer *Partition* von G.

d) $|gU| = |U|$ für alle $g \in G$.

Bemerkung: Für Rechtsnebenklassen gelten analoge Aussagen.

Beweis:

a) Sei $h \in gU$. Dann existiert $u \in U$ mit $h = gu$. Da $U \leq G$ und $g, u \in U$, folgt $h = gu \in U$. Also ist $gU \leq U$.
Sei $h \in U$. Da $g^{-1} \in U$ ist $g^{-1}h \in U$ und es gilt $gU \ni g(g^{-1}h) = (gg^{-1})h = h$. Also gilt $U \subseteq gU$.

b) Sei $gU \cap hU \notin \emptyset$. Dann gibt es $a, b \in U$ mit $ga = hb$ $(*)$. Es folgt

$$\begin{aligned} gU &\overset{(a)}{=} g(aU) = (ga)U \overset{(*)}{=} (hb)U \\ &= h(bU) \overset{(a)}{=} hU \ . \end{aligned}$$

c) Sei $g \in G$. Dann ist $g = ge \in gU$. Also $G \subseteq \bigcup_{g \in G} gU$. Die Disjunktheit folgt aus (b).

d) $f : U \to gU,\ u \mapsto gu$ ist bijektiv, da $\tilde{f} : gU \to U;\ x \mapsto g^{-1}$ die inverse Funktion zu f ist (d.h., $\tilde{f} \circ f = \mathrm{id}_U$ und $f \circ \tilde{f} = \mathrm{id}_{gU}$).
Damit folgt $|gU| = |U|$. □

29.13 Beispiel

$(5\mathbb{Z}, +)$ ist eine Untergruppe von $(\mathbb{Z}, +)$. Wir können $\mathbb{Z}$ in 5 (Links-) Nebenklassen zerlegen:

$$\begin{aligned} 0 + 5\mathbb{Z} &=: [0] \\ 1 + 5\mathbb{Z} &=: [1] \\ 2 + 5\mathbb{Z} &=: [2] \\ 3 + 5\mathbb{Z} &=: [3] \\ 4 + 5\mathbb{Z} &=: [4] \end{aligned}$$

Dies sind gerade die Kongruenzklassen (Restklassen) modulo 5 (vgl. MfI 1, Kap. 7).

29.14 Satz von Lagrange

Es sei G eine endliche Gruppe und $U \leq G$. Dann ist die Untergruppenordnung $|U|$ ein Teiler der Gruppenordnung $|G|$, und für die Anzahl der Linksnebenklassen gilt

$$G : U = \frac{|G|}{|U|} .$$

Beweis: Nach Satz 29.12 sind alle Nebenklassen von G bezüglich U gleich mächtig und bilden eine Partition von G. Also gilt $(G : U) \cdot |U| = |G|$. Daraus folgen die Behauptungen des Satzes. □

29.15 Korollar

Ist die Ordnung einer Gruppe G eine Primzahl, so hat G nur die trivialen Untergruppen $\{1\}$ und G. Ferner ist G zyklisch.

29.16 Beispiel

Eine Gruppe mit 30 Elementen kann nur Untergruppen mit $1, 2, 3, 5, 6, 10, 15$ oder 30 Elementen besitzen.

29.17 Definition (Normalteiler)

Sei G Gruppe und $U \leq G$. U heißt *Normalteiler* von G, geschrieben $U \trianglelefteq G$, falls für alle $g \in G$ gilt $gN = Ng$.

29.18 Satz (Faktorgruppen)

Sei G Gruppe, $N \trianglelefteq G$. Für $gN, hN \in G/N$ setze

$$(gN) \circ (hN) := (gh)N.$$

Dann ist $(G/N, \circ)$ eine Gruppe, die sogenannte Faktorgruppe von G nach N.

Beweis: Achtung: Ist $\circ$ wohldefiniert?

1) $\circ$ ist wohldefiniert, d.h. aus $gN = g'N$ und $hN = h'N$ folgt $(gN) \circ (hN) = (g'N) \circ (h'N)$:

$$\begin{aligned}(gN) \circ (hN) &= (gh)N = g(hN) = g(h'N) = g(Nh') \\ &= (gN)h' = (g'N)h' = g'(Nh') = g'(h'N) = (g'h')N \\ &= (g'N)(h'N)\end{aligned}$$

a) Die Gruppenaxiome folgen aus folgender Überlegung: Für alle $g, h \in G$ gilt

$$(gN) \circ (hN) := (gh)N = ghNN = gNhN = (gN) \cdot (hN).$$

Wir können also mit $\circ$ rechnen wie mit $\cdot$.

29.19 Beispiel

Die Untergruppe $(5\mathbb{Z}, +)$ (vgl. 29.13) ist Normalteiler in $(\mathbb{Z}, +)$, da $(\mathbb{Z}, +)$ eine kommutative Gruppe ist. Die Elemente von $\mathbb{Z}_5 := \mathbb{Z}/5\mathbb{Z}$ sind die *Kongruenzklassen* $[0], \ldots, [4]$.

Auf $\mathbb{Z}_5$ wird damit die Gruppenoperation durch

$$(a + 5\mathbb{Z}) + (b + 5\mathbb{Z}) := (a + b) + 5\mathbb{Z}$$

eingeführt, das heißt durch

$$[a] + [b] := [a + b] \; .$$

Dies ist gerade die Addition von Kongruenzklassen modulo 5 (*modulare Addition*, vgl. MfI 1, Kap. 7).

29.20 Definition: Abbildungen zwischen Gruppen

Es seien $(G_1, \circ)$, $(G_2, \bullet)$ Gruppen.

a) Ein **Homomorphismus** von G_1 nach G_2 ist eine Abbildung $f : G_1 \to G_2$ mit

$$\begin{array}{ccccc} f(a \circ b) & = & f(a) \bullet f(b) & & \forall a, b \in G_1 \; . \\ \uparrow & & \uparrow & & \\ \text{Verknüpfung} & & \text{Verknüpfung} & & \\ \text{in } G_1 & & \text{in } G_2 & & \end{array}$$

b) Ein injektiver Homomorphismus heißt **Monomorphismus**.

(Eine Abbildung $f : M \to N$ heißt injektiv, wenn für $x_1, x_2 \in M$, $x_1 \neq x_2$ stets $f(x_1) \neq f(x_2)$ ist, vgl. MfI 1, 5.6.)

c) Ein surjektiver Homomorphismus heißt **Epimorphismus**.

(Eine Abbildung $f : M \to N$ heißt surjektiv, wenn für jedes $y \in N$ ein $x \in M$ existiert mit $f(x) = y$, vgl. MfI 1, 5.6.)

d) Ein bijektiver Homomorphismus heißt **Isomorphismus**. Man schreibt dann $G_1 \cong G_2$.

e) Ein Homomorphismus von G_1 in sich selbst heißt **Endomorphismus**.

f) Ein Isomorphismus von G_1 in sich selbst heißt **Automorphismus**.

29.21 Beispiele:

a) $f : \mathbb{Z} \to 2\mathbb{Z}; z \mapsto 2z$ ist Isomorphismus.

b) $f : \mathbb{Z} \to \mathbb{Z}; z \mapsto -z$ ist Automorphismus.

c) $(\mathbb{Z}, +) \ncong (\mathbb{Q} \setminus \{0\}, \cdot)$, da es so etwas wie $(-1) \cdot (-1) = 1$ in $\mathbb{Z}$ nicht gibt.

29.22 Definition: Bild und Kern

Es sei $f : G_1 \to G_2$ ein Homomorphismus der Gruppen G_1, G_2. Dann heißt

$$\mathrm{Im}(f) := \{f(g_1) \mid g_1 \in G_1\}$$

das **Bild** von f.

Sei ferner e_2 das neutrale Element von $(G_2, \bullet)$. Dann bezeichnet man

$$\mathrm{Ker}(f) := \{g_1 \in G_1 \mid f(g_1) = e_2\}$$

als **Kern** von f.

Warum ist der Kern eines Homomorphismus wichtig? Man kann zeigen:

29.23 Satz: Homomorphiesatz für Gruppen

Sei $f : G_1 \to G_2$ ein Homomorphismus der Gruppen G_1 und G_2. Dann ist $\mathrm{Ker}(f)$ Normalteiler von G_1, und die Faktorgruppe $G_1/\mathrm{Ker}(f)$ ist isomorph zum Bild von f:

$$G_1/\mathrm{Ker}(f) \cong \mathrm{Im}(f) \; .$$

Bemerkung: Man kann also eine nicht bijektive Abbildung zwischen Gruppen bijektiv machen, indem man zum Faktorraum übergeht, also Elemente ignoriert, die auf das neutrale Element von G_2 abgebildet werden.

29.24 Bemerkung:

3 zentrale Prinzipien:

- Unterstrukturen
  - Schnitt
  - Erzeugnis
- Faktorstrukturen
  - Homomorphiesatz