TEIL B: ALGEBRA

§ 8: GRUPPEN

8.1. Bedeutung für die Informatik

- Gruppen sind abstrakte Modelle für Mengen, auf denen eine Verknüpfung (etwa Addition oder Multiplikation) definiert ist.
- Allgemeine Aussagen aus der Gruppentheorie arbeiten die Gemeinsamkeiten hinter vielen Problemen heraus. (Beutelspacher: „Mathematik ist die Lehre von den guten Beschreibungen".)

8.2. Def.:

Eine Gruppe besteht aus einer Menge G und einer Verknüpfung $\cdot$, die je zwei Elementen aus G wieder ein Element aus G zuordnet, für die gilt:

a) Assoziativgesetz: $(a\cdot b)\cdot c = a\cdot(b\cdot c) \quad \forall a,b,c\in G$.

b) Neutrales Element: $\exists e\in G: \quad e\cdot a = a \quad \forall a\in G$.

c) Inverse Elemente:

Zu jedem $a\in G$ ex. $b\in G$ mit $b\cdot a = e$.
Man schreibt auch $b =: a^{-1}$.

Gilt zusätzlich

d) Kommutativgesetz: $a\cdot b = b\cdot a \quad \forall a,b\in G$

so heißt $(G,\cdot)$ kommutative Gruppe (abelsche Gruppe). $|G|$ heißt Ordnung der Gruppe. Ist $|G|<\infty$, spricht man von einer endlichen Gruppe.

Bem.: Erfüllt $(G,\cdot)$ lediglich das Assoziativgesetz, spricht man von einer Halbgruppe (engl. semigroup). Halbgruppen mit neutralem Element heißen Monoide.

8.3. Beispiele

a) $(\mathbb{N}, +)$ ist eine Halbgruppe.

b) $(\mathbb{N}_0, +)$ ist ein Monoid (mit 0 als neutr. Element), jedoch keine Gruppe, da zu $a \in \mathbb{N}_0$ i. A. kein inverses Element existiert.

c) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ sind kommutative Gruppen

d) $(\mathbb{Z}, \cdot)$ ist ein Monoid (mit 1 als neutr. Element), aber keine Gruppe

e) $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\})$ sind kommutative Gruppen

f) Die Menge $\mathbb{Z}_m$ aller Restklassen modulo m bildet zusammen mit der modularen Addition eine kommutative Gruppe mit neutralem Element $[0]$ (vgl. Satz 7.8).

g) Sei m eine Primzahl. Dann ist $(\mathbb{Z}_m \setminus \{[0]\}, \cdot)$ eine kommutative Gruppe mit neutralem Element $[1]$ (vgl. Satz 7.12 und 7.13).

h) Die Menge aller Abbildungen $g: M \to M$ bildet mit der Komposition ein Monoid. (mit der identischen Abb. als neutr. Element). Betrachtet man nur bijektive Abb., liegt sogar eine (i. A. nicht-kommutative) Gruppe vor. (vgl. §5).

i) Spezialfall von (h):

Sei $M = \{1, \dots, n\}$. Dann bildet die Menge der bijektiven Abb. $M \to M$ mit der Komposition die Permutationsgruppe (symm. Gr.) $(S_n, \circ)$

Beispiel für $n = 3$:

$\sigma_1 := \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\sigma_2 := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\sigma_3 := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$

$\sigma_4 := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $\sigma_5 := \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $\sigma_6 := \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$

Dabei beschreibt z. B. σ_3 die Abb.

$$1 \mapsto 3$$
$$2 \mapsto 1$$
$$3 \mapsto 2$$

Die Verknüpfungstafel lautet

$\circ$	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_1	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6
σ_2	σ_2	σ_3	σ_1	σ_6	σ_4	σ_5
σ_3	σ_3	σ_1	σ_2	σ_5	σ_6	σ_4
σ_4	σ_4	σ_5	σ_6	σ_1	σ_2	σ_3
σ_5	σ_5	σ_6	σ_4	σ_3	σ_1	σ_2
σ_6	σ_6	σ_4	σ_5	σ_2	σ_3	σ_1

$\sigma_3 \circ \sigma_4$ beschreibt Abb.:

$$1 \xmapsto{\sigma_4} 2 \xmapsto{\sigma_3} 1$$
$$2 \xmapsto{\sigma_4} 1 \xmapsto{\sigma_3} 3$$
$$3 \xmapsto{\sigma_4} 3 \xmapsto{\sigma_3} 2$$

d.h. $\sigma_3 \circ \sigma_4 = \sigma_5$.

σ_1 ist neutrales Element

Beachte: S_n ist nicht kommutativ: $\sigma_4 \circ \sigma_6 \neq \sigma_6 \circ \sigma_4$

8.4 Satz (Eindeutigkeit des neutralen Elements und der inversen Elemente)

In jeder Gruppe gibt es nur ein neutrales Element, und jedes Element einer Gruppe hat genau ein inverses Element.

Beweis: Sei e ein neutrales Element. Wir gehen in 4 Schritten vor:

a) Ist $ba = e$ (d.h. $b = a^{-1}$), so ist auch $ab = e$
(d.h. „linksinverse" Elemente sind auch „rechtsinvers")

Denn:
$$\begin{aligned} ab &= e(ab) \\ &= (b^{-1}b)(ab) \\ &= b^{-1}(ba)b && \text{(Assoz.)} \\ &= b^{-1}\underbrace{eb}_{b} \\ &= b^{-1}b = e \end{aligned}$$

b) Es gilt $ae = a \quad \forall a \in G$ (d.h. e ist auch „rechtsneutral")

Denn:
$$\begin{aligned} ae &= a(a^{-1}a) \\ &= (aa^{-1})a && \text{(Assoz.)} \\ &= ea && \text{(nach (a))} \\ &= a && \text{(Def. des Linksneutralen)} \end{aligned}$$

c) Es gibt nur ein neutrales Element.

Denn: Sei e^* ein weiteres neutr. Element

$\Rightarrow e^* a = a \quad \forall a \in G$

$\Rightarrow e = e^* e \overset{(b)}{=} e e^* = e^*$.

d) Zu jedem $a \in G$ gibt es nur ein $a^{-1} \in G$.

Denn: Sei c ein weiteres inv. Element zu a.

$\Rightarrow \quad ca = e \qquad (*)$

$\Rightarrow \quad c = ce \qquad$ (nach b)

$= c a a^{-1} \qquad$ (nach a)

$= e a^{-1} \qquad$ (nach $*$)

$= a^{-1}$ $\square$

Gibt es Gruppen, die selbst wieder Gruppen enthalten?

8.5 Satz (<u>Untergruppenkriterium</u>)

Sei $(G, \cdot)$ eine (kommutative) Gruppe und $U \subset G$. Dann ist $(U, \cdot)$ genau dann eine (kommutative) Gruppe, wenn gilt

$$a, b \in U \Rightarrow a \cdot b \in U \text{ und } a^{-1} \in U$$

U heißt dann <u>Untergruppe</u> von G.

Beweis: Aus $a \cdot b \in U$ folgt, dass $\cdot$ abgeschlossen auf U ist. Das Assoziativgesetz überträgt sich aus G. (ebenso das Kommutativgesetz im Fall einer kommutativen Gruppe).
Aus $a \cdot b \in U$ und $a^{-1} \in U$ folgt für alle $a \in U$:

$$e = a^{-1} a \in U.$$

Ferner ist $a^{-1} \in U$ nach Voraussetzung. $\square$

8.6 Beispiele

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

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

c) Ist $(G,\cdot)$ eine Gruppe mit neutralem Element e, so sind $(\{e\},\cdot)$ und $(G,\cdot)$ selbst wieder Untergruppen von $(G,\cdot)$.

d) Jede Permutation einer Menge $M=\{1,\dots,n\}$ läßt sich durch eine Sequenz von Vertauschungen zweier Elemente (Transpositionen) darstellen.
Die Menge aller Permutationen von $M=\{1,\dots,n\}$ mit einer geraden Anzahl von Transpositionen bildet eine Untergruppe der symmetrischen Gruppe $(S_n,\circ)$, die alternierende Gruppe $(A_n,\circ)$

z.B. besteht A_3 aus den Permutationen $\delta_1, \delta_2, \delta_3$ (Notation aus 8.3.i) und wird beschrieben durch die Verknüpfungstafel

$\circ$	δ_1	δ_2	δ_3
δ_1	δ_1	δ_2	δ_3
δ_2	δ_2	δ_3	δ_1
δ_3	δ_3	δ_1	δ_2

A_n ist sogar kommutativ (obwohl S_n nicht kommut. ist).

8.7. Zykelschreibweise für Permutationen

Sei σ eine Permutation von $M = \{1, \dots, n\}$. Dann wird jedes Element von M nach spätestens n-maligem Anwenden von σ auf sich selbst abgebildet

Bsp.:

a) $\sigma_1 := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$

$$1 \xmapsto{\sigma_1} 3 \xmapsto{\sigma_1} 2 \xmapsto{\sigma_1} 4 \xrightarrow{\sigma_1} 1$$

b) $\sigma_2 := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$

$$1 \xmapsto{\sigma_2} 3 \xmapsto{\sigma_2} 2 \xmapsto{\sigma_2} 1$$
$$4 \xmapsto{\sigma_2} 4$$

c) $\sigma_3 := \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$

$$1 \xmapsto{\sigma_3} 3 \xmapsto{\sigma_3} 1$$
$$2 \xmapsto{\sigma_3} 4 \xmapsto{\sigma_3} 2$$

Das motiviert die Zykelschreibweise

a) $\sigma_1 = (1\ 3\ 2\ 4)$

b) $\sigma_2 = (1\ 3\ 2)$

(Der Einerzyklus (4) wird weggelassen)

c) $\sigma_3 = (1\ 3)(2\ 4)$

8.8. Mit Hilfe von Äquivalenzrelationen kann man eine Menge in Äquivalenzklassen zerlegen (Bsp.: $\mathbb{Z}$ wird in m Äquivalenzklassen modulo m zerlegt). Gibt es eine ähnliche Zerlegung bei Gruppen?

Def.: Sei $(G,\cdot)$ eine Gruppe mit Untergruppe $(U,\cdot)$. Ferner sei $g \in G$. Dann nennen wir

$gU := \{ g\cdot u \mid u \in U \}$ <u>Linksnebenklasse</u> von g,

$Ug := \{ u\cdot g \mid u \in U \}$ <u>Rechtsnebenklasse</u> von g.

Bem.: Häufig betrachtet man nur Linksnebenklassen und nennt diese Nebenklassen.

8.9. Satz (<u>Nebenklassenzerlegung einer Gruppe</u>)

Sei $(G,\cdot)$ eine Gruppe, $g,h \in G$ und $(U,\cdot)$ eine Untergruppe. Dann gilt:

a) $g \in U \Rightarrow gU = U$

b) Zwei (Links-)Nebenklassen gU, hU sind entweder gleich oder disjunkt.

c) Jedes $a \in G$ liegt in einer eindeutig bestimmten (Links-)Nebenklasse, d.h. die Nebenklassen von U bilden eine Partition von G.

d) Alle (Links-)Nebenklassen bzgl. einer festen Untergruppe U sind gleichmächtig:

$$|gU| = |U| \quad \forall g \in G.$$

Beweis:

a) Aus der Abgeschlossenheit folgt $gU \subset U$. Mit (d) folgt schließlich $gU = U$.

b) Ann.: gU und hU haben ein gemeinsames Element

$\Rightarrow \exists\ a, b \in U: \quad ga = hb \quad (*)$

$\Rightarrow gU \overset{(a)}{=} g(aU) = (ga)U \overset{(*)}{=} (hb)U = h(bU) \overset{(a)}{=} hU$

c) $a \in G$ liegt in aU, da U das neutr. El. e enthält. Die Eindeutigkeit folgt aus (b).

d) Es gilt $|gU| = |U|$, denn:

- Zu jedem $a \in U$ ex. Element $ga \in gU$, d.h. $|U| \leq |gU|$.
- Zu jedem $ga \in gU$ ex. $a \in U$, d.h. $|gU| \leq |U|$. □

8.10. Beispiele

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

$0 + 5\mathbb{Z} = [0]$
$1 + 5\mathbb{Z} = [1]$
$2 + 5\mathbb{Z} = [2]$
$3 + 5\mathbb{Z} = [3]$
$4 + 5\mathbb{Z} = [4]$

Dies sind gerade die 5 Kongruenzklassen modulo 5.

b) Die alternierende Gruppe $(A_3, \circ)$ ist eine Untergruppe der symmetrischen Gruppe $(S_3, \circ)$; vgl. 8.3.(i), 8.6.(d).

$S_3 = \{\sigma_1, \sigma_2, \dots, \sigma_6\}$ hat die Linksnebenklassen

$$A_3 = \{\sigma_1, \sigma_2, \sigma_3\} \qquad (= \sigma_1 A_3 = \sigma_2 A_3 = \sigma_3 A_3)$$

$$\sigma_4 A_3 = \{\sigma_4, \sigma_5, \sigma_6\} \qquad (= \sigma_5 A_3 = \sigma_6 A_3)$$

denn:

$$\begin{array}{lll} \sigma_4 \sigma_1 = \sigma_4 & \sigma_5 \sigma_1 = \sigma_5 & \sigma_6 \sigma_1 = \sigma_6 \\ \sigma_4 \sigma_2 = \sigma_5 & \sigma_5 \sigma_2 = \sigma_6 & \sigma_6 \sigma_2 = \sigma_4 \\ \sigma_4 \sigma_3 = \sigma_6 & \sigma_5 \sigma_3 = \sigma_4 & \sigma_6 \sigma_2 = \sigma_5 . \end{array}$$

Wie viele Nebenklassen besitzt eine Nebenklassenzerlegung von G bzgl. einer Untergruppe U?

8.11. Sei $(U, \cdot)$ eine Untergruppe von $(G, \cdot)$. Dann bezeichnen wir die Menge aller Linksnebenklassen mit G/U (gesprochen: „<u>G modulo U</u>"), und $G:U := |G/U|$ nennt man den <u>Index</u> von U in G.

8.12. <u>Satz von Lagrange</u>

Sei $(G, \cdot)$ eine endliche Gruppe mit Untergruppe $(U, \cdot)$. Dann ist die Untergruppenordnung $|U|$ Teiler der Gruppenordnung $|G|$. Für die Zahl der Linksnebenklassen gilt:

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

Beweis: Nach Satz 8.9 sind alle Nebenklassen von G bzgl. U gleichmächtig und bilden eine Partition von G. Also muss $|U|$ Teiler von $|G|$ sein, und $\frac{|G|}{|U|}$ ist die Zahl d. Nebenklassen. □

8.13. Beispiele:

a) $|S_3| = 6$, $|A_3| = 3$

$S_3 / A_3 = \{ A_3, \delta_4 A_3 \}$

$S_3 : A_3 = |S_3 / A_3| = 2 = \frac{6}{3}$

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

8.14. Wichtig sind Untergruppen $(N, \cdot)$ einer Gruppe $(G, \cdot)$, für die Links- und Rechtsnebenklassen identisch sind:

$$gN = Ng \quad \forall g \in G.$$

Sie heißen Normalteiler. Offensichtlich ist in einer kommutativen Gruppe $(G, \cdot)$ jede Untergruppe ein Normalteiler.

Warum sind Normalteiler wichtig?

Ist eine Untergruppe $(N, \cdot)$ Normalteiler von $(G, \cdot)$, so kann man zeigen, dass die Nebenklassenmenge G/N zu einer Gruppe wird, indem man sie mit der Verknüpfung

$$(gN)(hN) := (gh)N$$

ausstattet. Diese Gruppe heißt Faktorgruppe von G nach N.

8.15. Beispiel

Die Untergruppe $(6\mathbb{Z},+)$ ist Normalteiler in $(\mathbb{Z},+)$, da $(\mathbb{Z},+)$ eine kommutative Gruppe ist. In 7.6. hatten wir auf der Restklassenmenge $\mathbb{Z}_6 = \mathbb{Z}/6\mathbb{Z}$ die modulare Addition definiert durch

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

Wegen $[a] = a+6\mathbb{Z}$, $[b] = b+6\mathbb{Z}$ ist dies nichts anderes als die in 8.14 eingeführte Verknüpfung

$$(a+6\mathbb{Z})+(b+6\mathbb{Z}) := (a+b)+6\mathbb{Z}.$$

8.16. Abbildungen zwischen Gruppen

Def.: Seien $(G_1,\circ)$, $(G_2,\bullet)$ Gruppen.

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

$$\underset{\substack{\uparrow\\ \text{Verknüpfung}\\ \text{in } G_1}}{f(a\circ b)} = \underset{\substack{\uparrow\\ \text{Verknüpfung}\\ \text{in } G_2}}{f(a)\bullet f(b)} \qquad \forall\, a,b \in G_1$$

b) Ein injektiver Homomorphismus heißt Monomorphismus.

c) " surjektiver " " Epimorphismus.

d) " bijektiver " " Isomorphismus. Man schreibt $G_1 \simeq G_2$.

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

f) Ein Isomorphismus von G_1 in G_1 heißt Automorphismus.

8.17. Def.:

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 <u>Bild</u> von f.

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

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

den <u>Kern</u> von f.

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

Satz (<u>Homomorphiesatz für Gruppen</u>)

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

$$G_1 / \mathrm{Ker}(f) \simeq \mathrm{Im}(f)$$

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