Halbgruppen

Sei G eine Menge, $\cdot : G \times G \to G$ und $e \in G$. Es gelte

- $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ für alle $a, b, c \in G$.
- $a \cdot e = e \cdot a = a$ für alle $a \in G$.

Dann heißt G eine Halbgruppe mit neutralem Element e.

G heißt kommutativ (oder abelsch), wenn $a \cdot b = b \cdot a$ für alle $a, b \in G$ gilt.

Das Element b heißt Inverses von a und a invertierbar in G, wenn $a \cdot b = b \cdot a = e$ gilt.

Halbgruppen

Beispiel:

- $(\mathbb{Z}, \cdot)$, $(\mathbb{Z}, +)$.
- In $(\mathbb{Z}, \cdot)$ sind nur $1, -1$ invertierbar. In $(\mathbb{Z}, +)$ sind alle Elemente invertierbar: $a + (-a) = (-a) + a = 0$.

Beispiel:

- Strings A^* und Aneinanderhängen $\cdot$. EINS $\cdot$ ZWEI = EINSZWEI.
- ZWEI $\cdot$ EINS = ZWEIEINS. Sind ungleich, daher nicht kommutativ.
- Neutrales Element: Der leere String.
- Inverse Elemente: Gibt es für nicht-leere Strings nicht.

Halbgruppen und Gruppen

Kürzungsregel für invertierbares c mit Inversem d:

- Aus $ac = bc$ folgt $a = b$, denn es gilt $a = (ac)d = (bc)d = b$.
- Aus $ca = cb$ folgt $a = b$, denn es gilt $a = d(ca) = d(cb) = b$.

Neutrale Elemente und Inverse sind eindeutig:

- $e_1 = e_1 e_2 = e_2$, aus $cd_1 = e = cd_2$ folgt durch Kürzen $d_1 = d_2$.

Kombinierte Inverse:

- $(ab)^{-1} = b^{-1} a^{-1}$, $(a^{-1})^{-1} = a$.

Eine Gruppe G ist eine Halbgruppe mit neutralem Element, in dem jedes Element invertierbar ist.

Das Inverse von $c \in G$ wird mit c^{-1} bezeichnet.
Die Ordnung von G ist $\#G$.

Gruppen

Minimale Axiome für eine Gruppe:

- $(ab)c = a(bc)$ für alle $a, b, c \in G$.
- Es gibt $e \in G$ mit $ea = a$ für alle $a \in G$. (Linksneutrales Element).
- Für jedes $a \in G$ gibt es $b \in G$ mit $ba = e$. (Linksinverses Element).

Bew: Sei $b \in G$ mit $ba = e$.

1. Aus $a^2 = a$ folgt $a = e$. Denn es gilt $a = ea = (ba)a = b(aa) = ba = e$.
2. Es gilt $ab = e$. Denn $(ab)(ab) = a(ba)b = ab$ und nach 1 auch $ab = e$.
3. Es gilt $ae = a$. Denn $ae = a(ba) = (ab)a = ea = a$.

Die Existenz eines linksneutralen Elements und von linksinversen Elementen impliziert also, daß diese auch rechtsneutral und rechtsinvers sind.

Homomorphismen von Gruppen

Seien G, H Gruppen mit den neutralen Elementen 1_G, 1_H und $f : G \to H$. Es gelte $f(ab) = f(a)f(b)$ für alle $a, b \in G$. Dann heißt f ein Homomorphismus.

Epimorphismus = surjektiv.
Monomorphismus = injektiv.
Isomorphismus = bijektiv.
Endomorphismus = $H = G$.
Automorphismus = $H = G$ und bijektiv.

Es gilt:

- $f(1_G) = f(1_G)f(1_G)$, daher $f(1_G) = 1_H$ nach der Kürzungsregel.
- $1_H = f(1_G) = f(bb^{-1}) = f(b)f(b^{-1})$, also $f(b^{-1}) = f(b)^{-1}$ wegen der Eindeutigkeit der Inversen.

Untergruppen und Normalteiler

Ist $U \subseteq G$ eine Gruppe und die Multiplikation in U die gleiche wie die in G, so heißt U eine Untergruppe von G.

Setze $aU := \{au \mid u \in U\}$, $Ua := \{ua \mid u \in U\}$, $aUa^{-1} := \{aua^{-1} \mid u \in U\}$.
Die Abbildungen $u \mapsto au$, $u \mapsto ua$, $u \mapsto aua^{-1}$ sind bijektiv.

Gilt für eine Untergruppe U von G zusätzlich $aUa^{-1} \subseteq U$ für alle $a \in G$, so heißt U normal in G bzw. ein Normalteiler von G. Hier gilt sofort $aUa^{-1} = U$, weil $u \mapsto aua^{-1}$ bijektiv ist.

In einer abelschen Gruppe ist jede Untergruppe normal, denn $aua^{-1} = aa^{-1}u = u$ und $aUa^{-1} = U$.

Kerne und Bilder

Die Menge $U := f^{-1}(\{1_H\})$ ist ein Normalteiler von G.

- Für $a, b \in U$ gilt $f(ab^{-1}) = f(a)f(b)^{-1} = 1_H$, also $ab^{-1} \in U$ und U ist eine Untergruppe von G.
- Für $a \in G$ und $b \in U$ gilt $f(aba^{-1}) = f(a)f(b)f(a^{-1}) = 1_H$, also $aba^{-1} \in U$.

Man nennt U den Kern von f und schreibt $U = \ker(f)$.
f ist ein Monomorphismus $\Leftrightarrow \ker(f) = \{1_G\}$.

Die Menge $V := f(G)$ ist eine Untergruppe von H.

- Für $c, d \in V$ gibt es $a, b \in G$ mit $c = f(a)$, $d = f(b)$. Dann $cd^{-1} = f(a)f(b)^{-1} = f(ab^{-1})$. Wegen $ab^{-1} \in G$ folgt $cd^{-1} \in V$.

Man nennt V das Bild von f und schreibt $V = \mathrm{im}(f)$.
f ist ein Epimorphismus $\Leftrightarrow \mathrm{im}(f) = H$.

Nebenklassen

Sei G eine Gruppe und $U \subseteq G$ eine Untergruppe. Wir bezeichnen aU als eine Nebenklasse von U in G.

Thm (Lagrange): Die Menge $\mathcal{U} = \{aU \mid a \in G\}$ ist eine Partition von G in Mengen gleicher Kardinalität, G ist also disjunkte Vereinigung der Nebenklassen aU.

Bew: Da $u \mapsto au$ injektiv ist, gilt $\#U = \#aU$ für alle a.
Für $a \in G$ gilt $a \in aU$ wegen $e \in U$, daher $G = \cup_{a \in G} aU$.
Ist $c \in aU \cap bU$, so gilt $c = au_1 = bu_2$, also $a = bu_2u_1^{-1}$. Dann $a \in bU$ und $aU = bU$. Daher entweder $aU = bU$ oder $aU \cap bU = \{\}$. $\square$

Folgerung: Man nennt $(G : U) = \#\mathcal{U}$ den Index von U in G. Es gilt $\#G = (G : U)\#U$.

Faktorgruppen

Sei G eine Gruppe und $N \subseteq G$ ein Normalteiler.

Wir wollen in G modulo N rechnen. Zwei Elemente sollen als gleich gelten, wenn sie sich um ein Element aus N unterscheiden: Also wenn $a = bn$ für ein $n \in N$ bzw. $a \in bN$.

Wir betrachten die Nebenklassenzerlegung $G/N = \{aN \mid a \in G\}$ und definieren $aN \cdot bN = (ab)N$.

- Dies ist wohldefiniert: Für $a' \in aN$ und $b' \in bN$ gilt $a'N = aN$, $b'N = bN$ und $bN = Nb$ wegen $bNb^{-1} = N$, und dann $(a'b')N = a'bN = a'Nb = aNb = (ab)N$.
- $bN \cdot N = bN$ und $N \cdot bN = bN$, also ist N das neutrale Element.
- $bN \cdot b^{-1}N = (bb^{-1})N = N$, also ist $b^{-1}N$ das Inverse von bN.

Damit wird G/N eine Gruppe und $f : G \to G/N$, $x \mapsto xN$ ein Epimorphismus (Restklassenhomomorphismus).

Beispiel

$G = \mathbb{Z}$, $U = 4\mathbb{Z}$ mit +. Dann $\mathbb{Z}/4\mathbb{Z} = \{0+4\mathbb{Z}, 1+4\mathbb{Z}, 2+4\mathbb{Z}, 3+4\mathbb{Z}\}$.
Hier $i+4\mathbb{Z} = \{i+4j \mid j \in \mathbb{Z}\}$.
Es gilt $(2+4\mathbb{Z})+(3+4\mathbb{Z}) = (2+3)+4\mathbb{Z} = (1+4)+4\mathbb{Z} = 1+4\mathbb{Z}$.
Also modulo 4 Rechnen!

$G = \mathbb{Z}$, $H = \mathbb{Z}/25\mathbb{Z}$, $f : \mathbb{Z} \to \mathbb{Z}/25\mathbb{Z}$, $x \mapsto 5x + 25\mathbb{Z}$.
Dann $\ker(f) = 5\mathbb{Z}$ und $\mathrm{im}(f) = \{5i + 25\mathbb{Z} \mid 0 \leq i \leq 4\}$.

Stets $\#(G/N) = (G : N)$.