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 $a \cdot b = e$ 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 $\mathrm{im}(f) = \{5i+25\mathbb{Z} \mid 0 \le i \le 4\}$.

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

Isomorphiesatz

Thm: Ist $f : G \to H$ ein Homomorphismus, so ist $h : G/\ker(f) \to \mathrm{im}(f)$, $x\ker(f) \mapsto f(x)$ ein Isomorphismus.

Bew: Wegen $f(xn) = f(x)$ für alle $n \in \ker(f)$ ist h wohldefiniert. Außerdem ist es auch surjektiv. Weiter ergibt sich $h((x\ker(f))(y\ker(f))) = h((xy)\ker(f)) = f(xy)\ker(f) = (f(x)f(y))\ker(f) = (f(x)\ker(f))(f(y)\ker(f)) = h(x\ker(f))h(y\ker(f))$, also ist h ein Homomorphismus. Schließlich folgt aus $h(x\ker(f)) = f(x) = 1_H$, daß $x \in \ker(f)$ ist, also $x\ker(f) = \ker(f)$. Daher ist h auch injektiv. $\square$

Beispiel

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

Bekommen Isomorphismus $h : \mathbb{Z}/5\mathbb{Z} \to \{5i+25\mathbb{Z} \mid 0 \le i \le 4\}$ durch $x+5\mathbb{Z} \mapsto 5x+25\mathbb{Z}$.

Direktes Produkt

Seien G und H Gruppen. Dann in $G \times H$ koordinatenweise die Gruppengesetze definieren: $(a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2)$. Einheitselement $(1_G, 1_H)$.

Damit wird $G \times H$ zur Gruppe.

Einbettung $G \to G \times H$, $x \mapsto (x, 1_H)$ von G ist Monomorphismus.
Projektion $G \times H \to G$, $(x, y) \mapsto x$ auf G ist Epimorphismus.

Kern der Projektion auf G ist Untergruppe $\{1_G\} \times H$ von $G \times H$.

Erzeuger

Seien $g_1, \ldots, g_r \in G$. Die von den g_i erzeugte Untergruppe U von G besteht aus allen Elementen von G, die durch Verknüpfung und Inversion aus den g_i erhalten werden können.
Schreibweise $U = \langle g_1, \ldots, g_r \rangle$.

Äquivalent kann U als der Schnitt aller Untergruppen von G definiert werden, welche die g_i enthalten.

Ist die von den g_i erzeugte Untergruppe gleich G, so heißen die g_i ein Erzeugendensystem von G.

Gilt $G = \langle g_1, \ldots, g_r \rangle$ mit $r < \infty$, so heißt G endlich erzeugt.
Gilt $G = \langle g \rangle$, so heißt G zyklisch.

Homomorphismen sind bereits durch ihre Bildwerte auf Erzeugern definiert.

Ordnungen

Sei G eine Gruppe und $a \in G$. Dann heißt $\#\langle a \rangle$ die Ordnung von a.
Es gilt $\#\langle a \rangle = \min\{n \in \mathbb{Z}^{\geq 1} \mid a^n = e\}$ und $\#\langle a \rangle \mid \#G$ nach Lagrange.

Thm (Fermat): Ist G endlich, so gilt $a^{\#G} = e$ für $a \in G$.
Bew: Es gilt $a^{\#G} = (a^{\#\langle a \rangle})^{\#G/\#\langle a \rangle} = e^{\#G/\#\langle a \rangle} = e$. $\square$

Thm: Ist $\#G$ prim, so ist G zyklisch.
Bew: Für $a \in G \backslash \{e\}$ folgt $\#\langle a \rangle > 1$ und $\#\langle a \rangle \mid \#G$, also $\#\langle a \rangle = \#G$.

Thm: Sind U, V Untergruppen von G mit teilerfremden Ordnungen, so gilt $U \cap V = \{e\}$.

Bew: Es gilt $\#(U \cap V) \mid \#U$ und $\#(U \cap V) \mid \#V$ nach Lagrange. Also $\#(U \cap V) \mid \gcd\{\#U, \#V\} = 1$ und daher $\#(U \cap V) = 1$. $\square$

Endlich erzeugte abelsche Gruppen

Sei G eine endlich erzeugte abelsche Gruppe.

Thm (Version 1): Es gibt ein eindeutig bestimmtes n und eindeutig bestimmte $c_i \in \mathbb{Z}^{\geq 0}$ mit $c_i \mid c_{i+1}$ für $1 \leq i \leq n-1$, so daß gilt:

$$G \cong \prod_{i=1}^{n} \mathbb{Z}/c_i\mathbb{Z}.$$

Thm (Version 2): Es gibt $r \in \mathbb{Z}^{\geq 0}$, Primzahlen p_i und Exponenten $e_i \geq 1$, so daß

$$G \cong \mathbb{Z}^r \times \prod_{i=1}^{m} \mathbb{Z}/p_i^{e_i}\mathbb{Z}$$

gilt. Die Zahl r und die Paare (p_i, e_i) sind bis auf die Reihenfolge eindeutig bestimmt.

Bemerkung: Die Äquivalenz von Version 1 und 2 beruht auf dem chinesischen Restsatz.

Beispiel

Ein direktes Produkt $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z} \times 5\mathbb{Z}$.
Erzeuger: $(1+3\mathbb{Z},0,0),(0+3\mathbb{Z},1,0),(0+3\mathbb{Z},0,5)$.
Ist nicht zyklisch.

$\mathbb{Z}/5\mathbb{Z}$ hat Erzeuger $1+5\mathbb{Z}$. Ist zyklisch.

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ ist auch zyklisch (!):
Erzeuger $(1+2\mathbb{Z},1+3\mathbb{Z})$.

Als Gruppen sind $\mathbb{Z}$ und $5\mathbb{Z}$ unter $x \mapsto 5x$ isomorph.

Gruppe wie in Thm (Version 1) ist genau dann zyklisch,
wenn $n = 1$ gilt.

Für einen endlichen Körper $\mathbb{F}_q$ gilt $\mathbb{F}_q^\times \cong \mathbb{Z}/(q-1)\mathbb{Z}$.

Exponentiation in Gruppen

Wie g^n effizient ausrechnen? Z.B. für $n = 27354268183173165356$.

Schreibe $n = \sum_{i=0}^{k} r_i 2^i$, $r_i \in \{0,1\}$. Dann $g^n = g^{(\cdots(r_k 2 + r_{k-1})2+\cdots)2+r_0}$.

Eingabe: g und $n \geq 0$.
Ausgabe: g^n.

1. Wenn $n = 0$ dann Ausgabe von 1.
2. Berechne rekursiv $b \leftarrow g^{n \text{ div } 2}$. Berechne $b \leftarrow b^2$.
3. Wenn n ungerade, dann $b \leftarrow bg$.
4. Ausgabe von b.

Aufwand $\leq 2(\log_2(n)+1)$ Operationen (Quadrieren und Multiplizieren).
Von diesem Verfahren gibt es einige Varianten (mit vorberechneter Tabelle, links-rechts, rechts-links, sliding windows, ...).