

Einführung in die Algebra

Sebastian Bechtel, Isburg Knof

15. April 2015

1 Gruppen

Definition. Eine (innere) Verknüpfung auf einer Menge $M \neq \emptyset$ ist eine Abbildung $M \times M \rightarrow M, (a,b) \mapsto a \cdot b$.

Definition. Eine Gruppe ist eine Menge $G \neq \emptyset$ zusammen mit einer Verknüpfung \cdot , sodass Assoziativität (A), Existenz eines neutralen Elements (N) und Existenz inverser Elemente (I) erfüllt sind. G ist abelsch, falls Kommutativität (K) gilt.

Beispiel 1. 1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind abelsche Gruppen mit $+$ als Verknüpfung.

2. $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}, \mathbb{R}^*, \mathbb{C}^*$ mit Multiplikation sind abelsche Gruppen.

3. Für eine Menge M ist $\text{Sym}(M)$ ist eine Gruppe, aber nicht abelsch.

Lemma 1. 1. Das neutrale Element ist eindeutig.

2. Inverse Elemente sind eindeutig.

Beweis. 1. Seien e, f neutrale Elemente, dann gilt $e = ef = f$.

2. Sei $a \in G$ und $b, b' \in G$ inverse Elemente. Dann gilt $b' = b'e = b'(ab) = (b'a)b = eb = b$.

□

Notation. multiplikativ: $a \cdot b$ oder ab , neutrales Element e oder 1, inverses Element von $a \in G$ ist a^{-1} .

Lemma 2. Es sei $\mathcal{G} = (G, \cdot)$ eine Menge mit assoziativer Verknüpfung, einem linksneutralen Element und linksinversen Elementen, dann ist \mathcal{G} eine Gruppe.

Beweis. Sei $a \in G$ und $b \in G$ mit $ba = e$. Nach (I') gibt es $c \in G$ mit $cb = e$. Also $ab = eab = cbab = ceb = cb = e$.

Sei nun $a \in G$, es gilt $ae = a(a^{-1}a) = ea = e$.

□

Lemma 3. 1. $(a^{-1})^{-1} = a$, $(ab)^{-1} = b^{-1}a^{-1}$

2. $ab = ac \implies b = c$ für alle $a, b, c \in G$.

3. für $a, b \in G$ gibt es genau ein $x \in G$, sodass $ax = b$.

Beweis. 1. $(a^{-1})^{-1} = a$ klar. Für $a, b, c \in G$: $(b^{-1}a^{-1})ab = b^{-1}(a^{-1}a)b = b^{-1}eb = b^{-1}b = e$ (andere Richtung analog)

2. $ab = ac \implies a^{-1}(ab) = a^{-1}(ac) \implies b = c$

3. Setze $x = a^{-1}b$, dann erhält man $ax = a(a^{-1}b) = (aa^{-1})b = eb = b$

□

Definition. Sei $a \in G$, (G, \cdot) Gruppe. Für $n \in \mathbb{Z}$ definiere:

$$a^0 := e, \quad a^n := a^{n-1}a \quad \text{für } n \geq 1$$

$$a^n := (a^{-1})^{-n} \quad \text{für } n < 0$$

Lemma 4. Für $a \in G$ gilt: $a^n a^m = a^{n+m} = a^m a^n$, $(a^m)^n = a^{n \cdot m}$, $ab = ba \implies (ab)^n = a^n b^n$

Beispiel 2. 1. K Körper, dann ist $\text{GL}_n(K)$ eine Gruppe bzgl. Matrixmultiplikation.

2. $M \neq \emptyset$ Menge, (G, \cdot) Gruppe, definiere $\text{Abb}(M, G) := G^M$. Für $f, g \in \text{Abb}(M, G)$ ist $f \cdot g$ gegeben durch $(f \cdot g)(m) = f(m) \cdot g(m)$ für $m \in M$. Dann ist $(\text{Abb}(M, G), \cdot)$ eine Gruppe.

2 Untergruppen

Definition. Sei (G, \cdot) Gruppe. Eine Teilmenge $H \subset G$ heißt Untergruppe von G , falls (H, \cdot) eine Gruppe ist.

Äquivalent dazu:

1. Für $a, b \in H$ gilt $ab \in H$ (Abgeschlossenheit)

2. $e \in H$

3. für $a \in H$ ist $a^{-1} \in H$

Theorem 1. Sei (G, \cdot) Gruppe und $H \subset G$ nicht-leer. Dann gilt: H induziert Untergruppe von (G, \cdot) gdw. $ab^{-1} \in H$ für $a, b \in H$.

Beweis. „ \implies “: ✓

„ \impliedby “:

- $a = b \implies e \in H$

- $e, a \in H \implies ea^{-1} \in H \implies a^{-1} \in H$
- $a, b^{-1} \in H \implies a(b^{-1})^{-1} \in H \implies ab \in H$

□

Beispiel 3. 1. $\{e\}, G$ induziert Untergruppe für alle Gruppen (G, \cdot) .

2. K Körper. $SL_n(K) = \{A \in M_n(K) : \det(A) = 1\}$ induziert Untergruppe von $GL_n(K)$, die spezielle lineare Gruppe.

Definition. Eine Untergruppe heißt echt, falls sie nicht trivial ist.

Lemma 5. Es sei $(H_j)_{j \in J}$ eine Familie von Untergruppen $H_j \subset G$. Dann ist $\bigcap_{j \in J} H_j$ eine Untergruppe von G .

Beweis. Übung

□

Definition. Es sei M eine Teilmenge von G . Die von M erzeugte Untergruppe ist der Durchschnitt aller Untergruppen, die M enthalten.

Notation. $\langle M \rangle = \bigcup_{M \subset H \subset G} H$, wobei H Untergruppe

Bemerkung. 1. $\langle \emptyset \rangle = \{e\}$

2. Für $M \neq \emptyset$ gilt: $\langle M \rangle = \{m_1^{\varepsilon_1} \cdot \dots \cdot m_n^{\varepsilon_n} : m_1, \dots, m_n \in M, \varepsilon_1, \dots, \varepsilon_n \in \{-1, +1\}, n \geq 0\}$
3. Für $M = \{g\}$ gilt: $\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$. Von g erzeugte zyklische Untergruppe von G .

Definition. G heißt zyklisch, falls $G = \langle g \rangle$ für ein $g \in G$ gilt.

Ist $G = \langle M \rangle$ mit M endlich, so heißt G endlich erzeugt.

Definition. 1. Die Ordnung einer Gruppe G ist $ord(G) = |G|$.

2. Die Ordnung eines Elements $g \in G$ ist $ord(g) = ord(\langle g \rangle)$.

3. Ist $ord(g)$ endlich, dann hat g endliche Ordnung.

Notation. (n, s) bezeichnet den größten gemeinsamen Teiler.

Theorem 2. Sei G Gruppe, $g \in G$

1. g hat endliche Ordnung \iff alle Potenzen von g sind verschieden

2. g hat endliche Ordnung $\iff \exists m > 0 : g^m = e$

Dann gilt:

- a) $n := ord(g) = \min\{m > 0 : g^m = e\}$
- b) $g^m = e \iff m = nk$ mit $k \in \mathbb{Z}$
- c) $\langle g \rangle = \{e, g^1, \dots, g^{n-1}\}$

3. $\text{ord}(g^s) = \frac{n}{(n,s)}$ für $n = \text{ord}(g)$ endlich

Beweis. 1. Wir nehmen an: Für $i, j \in \mathbb{Z}$, oBdA $j > i$ gilt $g^i = g^j$.

Dann gilt $g^{j-i} = g^j(g^i)^{-1} = e$.

Es sei dann n die kleinste positive Zahl, die $g^n = e$ erfüllt. Sei $m \in \mathbb{Z}$ beliebig. Der Divisionsalgorithmus liefert: $m = kn + r$ für $0 \leq r < n$ und $k, r \in \mathbb{Z}$. Dann gilt:

$$g^m = g^{kn+r} = g^{kn}g^r = (g^n)^k g^r = e g^r = g^r.$$

Daraus folgt $\langle g \rangle = \{g^m : m \in \mathbb{Z}\} = \{g^r : r = 0, \dots, n-1\}$. Besonders gilt $\text{ord}(g) = n$ ist endlich.

[Dies zeigt \Rightarrow , \Leftarrow klar, dann ist $\langle g \rangle = \{g^m : m \in \mathbb{Z}\}$ unendlich]

2. Alle g^r mit $0 \leq r \leq n-1$ sind verschieden, da:

$$g^i = g^j \Rightarrow g^{j-i} = e \Rightarrow j - i = kn \text{ mit } k \in \mathbb{Z} \Rightarrow i \equiv j \pmod{n} \Rightarrow i = j \text{ falls } 0 < i, j < n-1.$$

Dies liefert g^r mit $0 \leq r \leq n-1$ sind paarweise verschieden und es gilt:

$$\text{ord}(g) = n. \text{ [a und c]}$$

Aus dem Divisionsalgorithmus folgt b: $g^m = e \Leftrightarrow e = g^{kn+r} = g^r$ mit $m = kn + r, 0 \leq r < n \Leftrightarrow r = 0$. Also $m = kn$ mit $k \in \mathbb{Z}$.

3. Es sei $m = \text{ord}(g^s), n = \text{ord}(g)$. Aus $(g^s)^m = e$ folgt (siehe 2), dass n ein Teiler von sm ist. Dies liefert: $\frac{n}{(s,n)} \mid \frac{s}{(s,n)}m$. Somit $\frac{n}{(s,n)} \mid m$.

Nun möchten wir noch zeigen: $m \mid \frac{n}{(s,n)}$. $(g^s)^{\frac{n}{(s,n)}} = (g^n)^{\frac{s}{(s,n)}} = e^{\frac{s}{(s,n)}} = e$. Daraus folgt $m \mid \frac{n}{(s,n)}$ (wegen 2).

Also gilt $m = \frac{n}{(s,n)}$.

□

Lemma 6. Wir können alle Untergruppen einer zyklischen Gruppe beschreiben mit $G = \langle g \rangle, H \subset G$, es sei $h \in H, h \neq e$. Dann gilt: $h = g^k$.

Beweis. Wir setzen: $m = \min\{k > 0 : g^k \in H\}$.

[Existiert: $G = \langle g \rangle = \langle g^{-1} \rangle, h = g^k, k < 0$, dann ersetzen wir h durch h^{-1}]

Wir wollen zeigen: $\langle g^m \rangle = H$

1. $\langle g^m \rangle \subset H$ gilt wegen $g^m \in H$

2. Es sei $j \in \mathbb{Z}$ mit $g^j \in H$. Divisionsalgorithmus liefert $j = lm + r$ mit $0 \leq r < m$:
 $g^j \in H \Rightarrow g^r = g^{-lm} g^{lm+r} = (g^m)^{-l} g^j$. Also $g^r \in H$. Aus der Minimalität von m folgt $r = 0$. Dies liefert $g^j = (g^m)^l \in \langle g^m \rangle$ und somit gilt: $H \subset \langle g^m \rangle$ und die zwei Untergruppen stimmen überein.

□

Ähnlich kann man zeigen:

Theorem 3. Alle Untergruppen einer zyklischen Gruppe sind zyklisch. Ist $\text{ord}(G) = n$ endlich und m ein Teiler von n , so ist $H = \langle g^{\frac{n}{m}} \rangle$ die einzige Untergruppe der Ordnung m .

Definition. Sei H eine Untergruppe der Gruppe G . Dann kann man die folgende Äquivalenzrelation definieren:

$$(x, y) \in G^2 : x \sim_H y \Leftrightarrow x = yh \text{ für } h \in H$$

[Äquivalenzrelation wegen Gruppenaxiomen für H]

Definition. Die Äquivalenzklassen bzgl. \sim_H heißen Linksnebenklassen.

Notation. Für $a \in G, aH = \{ah : h \in H\}$

Bemerkung. Es gelten folgende Eigenschaften:

- Die Abbildung $H \rightarrow aH, h \mapsto ah$ ist eine Bijektion. Besonders gilt: $|aH| = |H|$ für alle $a \in G$.
[Die Abbildung ist bijektiv, da sie umkehrbar ist: $aH \rightarrow H, b \mapsto a^{-1}b$ ist die Umkehrfunktion]
- $aH \neq bH \Rightarrow aH \cap bH = \emptyset$, d.h. sie sind disjunkt.
[$x \in aH \neq bH \Rightarrow x = ah_1 = bh_2$ für $h_1, h_2 \in H \Rightarrow a = bh_2h_1^{-1} \in bH \Rightarrow ah = b(h_2h_1^{-1}h) \in bH$ für alle $h \in H \Rightarrow aH \subset bH$. Ähnlich gilt $bH \subset aH$. Daraus folgt $aH = bH$.]

Definition. $G/H = \{aH : a \in G\}$ ist die Menge der Linksnebenklassen.

Der Index von H ist die Mächtigkeit von G/H , d.h. Index $[G : H] := |G/H|$

Bemerkung. • $|G| = [G : H]|H|$

- Analog ist $a \sim_H b$ mit $a, b \in G \Leftrightarrow a = hb$ für ein $h \in H$ („rechtsäquivalent bzgl. H “) eine Äquivalenzrelation.
Rechtsnebenklassen: $Ha = \{ha : h \in H\}$ mit $a \in G$
Bijektion: Für $a \in G, aH \rightarrow Ha, x \mapsto a^{-1}xa$

Definition. $H \backslash G$ ist die Menge der Rechtsnebenklassen. Dann gilt: $|H \backslash G| = |G/H|$

[Bijektion: $H \backslash G \rightarrow G/H, Hb \mapsto b^{-1}H$]