Einführung in die Algebra

Sebastian Bechtel

15. April 2015

1 Gruppen

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

Definition. Eine <u>Gruppe</u> ist eine Menge $G \neq \emptyset$ zusammen mit einer Verknüpfung ·, sodass Assoziativität (A), Existenz eines neutralen Elements (N) und Existenz inverser Elemente (I) erfüllt sind. G ist <u>abelsch</u>, 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 Sym(M) ist eine Gruppe, aber nicht abelsch.

Lemma 1. a) Das neutrale Element ist eindeutig.

b) Inverse Elemente sind eindeutig.

Beweis. a) Seien e, f neutrale Elemente, dann gilt e = ef = f.

b) 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. $ab = ac \implies b = c \text{ für alle } a, b, c \in G.$
- 3. $f\ddot{u}r\ a,b\in G\ gibt\ es\ genau\ ein\ x\in G,\ sodass\ ax=b.$

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:

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

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

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 $GL_n(K)$ ein Gruppe bzgl. Matrixmultiplikation.

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

- (i) Für $a, b \in H$ gilt $ab \in H$ (Abgeschlossenheit)
- (ii) $e \in H$
- (iii) 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. "
$$\Rightarrow$$
" \checkmark

• $a = b \implies e \in H$

$$\bullet \ e,a \in H \implies ea^{-1} \in H \implies a^{-1} \in H$$

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

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

(b) 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.