Einführung in die Algebra

Arthur Henninger

October 8, 2024

Contents

Kapitel 1

Gruppen

1.1 Grundbegriffe

Definition 1.1: (abelsche) Gruppe

Eine Gruppe ist eine Menge G zusammen mit einer Abbildung

$$\begin{aligned} \cdot : G \times G &\to G \\ (a, b) &\mapsto a \cdot b = ab, \end{aligned}$$

sodass:

1) Assoziativität

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

2) Existenz eines linksneutralen Elements:

$$\exists e \in G : \forall a \in G : e \cdot a = a.$$

3) Existenz von Linksinversen:

$$\forall a \in G \exists b \in G : b \cdot a = e.$$

Bemerkung 1.2

Eine Gruppe G heißt abelsch oder kommutativ, wenn zusätzlich gilt:

4) Kommutativität:

$$\forall a, b \in G : a \cdot b = b \cdot a.$$

Notation 1.2

Wir schreiben $a \cdot b = ab$ und $a^n = \underbrace{a \cdot \ldots \cdot a}_{n \text{ mal}} \forall n \in \mathbb{N} \setminus \{0\}$ und falls G abelsch ist $a + b := a \cdot b, n \cdot a = a^n$

Lemma 1.3

Sei G eine Gruppe. Dann gilt

(1) $G \neq \emptyset$

(2) Linksinverse sind eindeutig und rechtsinvers, d.h.

$$\forall a, b, c \in G : ba = ca = e \implies b = c \text{ und } ab = e.$$

(3) Das linksneutrale Element ist eindeutig und rechtsneutral, d.h.

$$\forall e' \in G \text{ mit } e' \cdot a = a \forall a \in G \text{ gilt } e = e' \text{ und } a \cdot e = a \forall a \in G.$$

Proof: (1) Da $e \in G$ ist $G \neq \emptyset$

(2) Seien $a, b \in G$ mit $ba = e$. Sei $a' \in G$ das linksinverse zu b also $a'b = e$. Dann gilt

$$ab = eab = a' \underbrace{ba}_{e} b = a'eb = a'b = e.$$

Also ist b rechtsinvers zu a.
Sind $b, c \in G$ mit $ba = ca = e$. Dann gilt

$$c = ec = bac = be = bab = eb = b.$$

(3) Seien $a, b \in G$ mit $ba = ab = e$. Dann ist

$$ae = aba = ea = a.$$

Also ist e rechtsneutral.
Ist $e' \in G$ ein linksneutrales Element, dann gilt $e = e'e = e'$.

□

Notation 1.4

Für $a \in G$ schreiben wir a^{-1} für das Inverse (rechts- und links-) von a und $a^{-n} = (a^{-1})^n$. Wir nennen das (links- und rechts-) Neutrale Element $e \in G$ auch Einheit oder Eins.

Fakt 1.5

Analog zu 1.3:
Sei G eine Gruppe. Dann gilt

(1) $(a^{-1})^{-1} = a$

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

(3) Ist $ab = ac$, so ist $b = c$

(4) Ist $a^2 = a$, so ist $a = e$.

Definition 1.6: Untergruppe

Sei G eine Gruppe. Eine Untergruppe von G ist eine Teilmenge $H \subseteq G$ sodass

(1) $e \in H$

(2) $\forall a \in H$ ist $a^{-1} \in H$

(3) $\forall a, b \in H$ ist $ab \in H$.

Dann ist H mit $\cdot|_{H \times H}$ selbst eine Gruppe.

Bemerkung 1.7

Schneller: $\emptyset \neq H \subseteq G$ ist eine Untergruppe $\iff \forall a, b \in H : ab^{-1} \in H$.

Definition 1.8: Gruppenhomomorphismus und Gruppenisomorphismus

Eine Abbildung $\varphi : G_1 \to G_2$ zwischen zwei Gruppen G_1 und G_2 heißt

1) Gruppenhomomorphismus (oder Homomorphismus oder Morphismus), falls

$$\varphi(ab) = \varphi(a) \cdot \varphi(b) \forall a, b \in G_1.$$

2) Gruppenisomorphismus (oder Isomorphismus), falls φ ein bijektiver Homomorphismus ist.

G_1 und G_2 heißen dann isomorph und wir schreiben $G_1 \cong G_2$, falls ein Isomorphismus zwischen den Gruppen existiert.

Bemerkung 1.9

Sei $\varphi : G_1 \to G_2$ ein Homomorphismus:

(1) φ ist ein Isomorphismus

$$\iff \exists \psi : G_2 \to G_1 \text{ Hom.} \quad \text{mit } \varphi \circ \psi = \mathrm{Id} \quad \varphi \circ \psi = \mathrm{Id}\,.$$

($\Longleftarrow$ ist klar, für $\Longrightarrow$ prüft man, dass φ^{-1} ein Hom. ist)

(2) $\varphi(e) = e$, denn

$$\varphi(e)^2 = \varphi(e^2) = \varphi(e) \implies \varphi(e) = e.$$

(3) $\varphi(a^{-1}) = \varphi(a)^1$, denn

$$e = \varphi(e) = \varphi(aa^{-1}) = \varphi(a)\varphi(a^{-1}).$$

(4) φ ist injektiv $\iff \varphi^{-1}(e) = \{e\}$, denn:

$$\text{Für } a \neq b \in G_1 \text{ mit } \varphi(a) = \varphi(b) \text{ gilt } \varphi(\underbrace{ab^{-1}}_{\neq e}) = e.$$

Definition 1.10: Kern und Bild

Sei $\varphi : G_1 \to G_2$ ein Homomorphismus.

(1) Der Kern von φ ist

$$\mathrm{Ker}(\varphi) = \{a \in G_1 : \varphi(a) = e\}\,.$$

(2) Das Bild von φ ist

$$\mathrm{Im}(\varphi) = \{b \in G_2 : \exists a \in G_1, \varphi(a) = b\}\,.$$

Aus 1.9 (4) folgt dann: φ injektiv $\iff \mathrm{Ker}(\varphi) = \{e\}$

Lemma 1.11

Sei $\varphi : G_1 \to G_2$ ein Homomorphismus. Dann sind $\mathrm{Ker}(\varphi) \subseteq G_1, \mathrm{Im}(\varphi) \subseteq G_2$ Untergruppen.

Proof: Klar ist $\mathrm{Ker}(\varphi), \mathrm{Im}(\varphi) \neq \emptyset$.
Für $a, b \in \mathrm{Ker}(\varphi)$ gilt:

$$\begin{aligned} \varphi(ab^{-1}) &= \varphi(a)\varphi(b^{-1}) \\ &= \varphi(a)\varphi(b)^{-1} \\ &= ee^{-1} \\ &= e \\ &\implies ab^{-1} \in \mathrm{Ker}(\varphi). \end{aligned}$$

Für $c, d \in \mathrm{Im}(\varphi)$, wähle $a, b \in G_1$ mit $\varphi(a) = c, \varphi(b) = d$. Dann gilt

$$\begin{aligned} \varphi(ab^{-1}) &= \varphi(a)\varphi(b^{-1}) \\ &= \varphi(a)\varphi(b)^{-1} \\ &= cd^{-1} \\ &\implies cd^{-1} \in \mathrm{Im}(\varphi). \end{aligned}$$

□

Beispiel 1.12

(1) Die triviale Gruppe ist $G = \{e\}$ mit der eindeutigen Abbildung

$$G \times G \to G.$$

Bis auf Isomorphie gibt es nur eine Gruppe mit einem Element.

(2) Sind G_1 und G_2 Gruppen, so ist $G = G_1 \times G_2$ mit

$$\begin{aligned} G \times G &\to G \\ (a_1, a_2), (b_1, b_2) &\mapsto (a_1 b_1, a_2 b_2) \end{aligned}$$

eine Gruppe. Sind G_1, G_2 abelsch, dann schreiben wir

$$G_1 \oplus G_2 := G_1 \times G_2.$$

(3) Ist K ein Körper, so sind

$$(K, +) \text{ und } (K \setminus \{0\}, \cdot)$$

Gruppen.

(4) Die Paare $(\mathbb{N}, +), (\mathbb{Z} \setminus \{0\}, \cdot)$ sind jeweils keine Gruppen, sondern sogenannte Monoide da lediglich Inverse fehlen.

(5) $\forall$ Mengen M ist

$$\mathrm{Bij}(M) = \{f : M \to M : f \text{ bijektiv } \}$$

mit Komposition eine Gruppe.

(6) Die symmetrische Gruppe aus n Elementen ist $S_n = \mathrm{Bij}(\{1, \dots, n\})$.

(7) Die Abbildung

$$\mathrm{sgn} : S_n \to (\{\pm 1\}, \cdot)$$

ist ein Homomorphismus. Die alternierende Gruppe auf n Elementen ist $A_n := \mathrm{Ker}(\mathrm{sgn}) \subseteq S_n$.

(8) Die linearen Gruppen $Gl_n(K), SL_n(K), O_n(K), SO_n(K), U_n(K)$, etc. sind Gruppen (wobei teilweise nicht jeder Körper die Grundlage für die Gruppen bilden kann oder Skalarprodukte existieren müssen).

(9) Ist K ein Körper, so ist die Automorphismengruppe von K

$$\mathrm{Aut}(K) = \{\varphi : K \to K : \varphi \in \mathrm{Bij}(K), \varphi(a+b) = \varphi(a) + \varphi(b), \varphi(ab) = \varphi(a)\varphi(b) \forall a, b \in K\}.$$

(10) Allgemeiner: Ist $\mathscr{C}$ eine Kategorie, sodass $\forall A, B \in \mathrm{Ob}(\mathscr{C})$ die Abbildungen zwischen A und B eine Menge $\mathrm{Hom}_{\mathscr{C}}(A, B)$ bilden. Dann ist

$$\mathrm{Aut}_{\mathscr{C}}(A) = \{\varphi : A \to A : \varphi \text{ invertierbar}\} \subseteq \mathrm{Hom}(A, A)$$

eine Gruppe via Komposition. Beispiele sind

- $\mathrm{Bij}(M)$ mit $\mathscr{C}$ = Mengen
- $\mathrm{Gl}_n(M)$ mit $\mathscr{C}$ = endlich dimensionale Vektorräume
- $\mathrm{Aut}(M)$ mit $\mathscr{C}$ = Körper

Kapitel 2

Ringe

Kapitel 3

Körper

Kapitel 4

Galoistheorie