

Algebra I - HS 2025

Franz Nowak

September 24, 2025

Vorlesung 1

Definition 1. Eine **Gruppe** ist eine Menge G zusammen mit einer Verknüpfung

$\ast: G \rightarrow G, \quad (g, h) \rightarrow g \ast h$, sodass:

- (1) (Assoziativität) $\forall g, h, k \in G: (g \ast h) \ast k = g \ast (h \ast k)$
- (2) (Neutrales Element) $\exists e \in G: g \ast e = e \ast g = g \quad \forall g \in G$
- (3) (Inverses Element) $\forall g \in G \exists g^{-1} \in G$ s.d. $g \ast g^{-1} = g^{-1} \ast g = e$

Eine Gruppe ist **abelsch** (kommutativ), wenn $\forall g, h \in G, g \ast h = h \ast g$.

Wir schreiben oft 1 oder 1_G für e und gg' für $g \ast g'$ mit $g, g' \in G$. Wenn G kommutativ ist, dann schreiben wir $e = 0$ und $a + b$ für $a \ast b$. Des Weiteren ist

$a^n := \overbrace{a \cdots a}^{n\text{-mal}}$ und $a^0 := 1$.

Bemerkung 1. Wenn G assoziativ ist, dann ist $g_1 g_2 \cdots g_n$ eindeutig definiert (für $g_1, g_2, \dots, g_n \in G$).

Satz 1. (a) Das neutrale Element ist eindeutig.

(b) Das Inverse von jedem Element ist eindeutig.

Beweis: (a) Seien $e, e' \in G$ neutrale Elemente. Dann ist $e = ee' = e'$.

(b) Seien \bar{g}, g^{-1} Inverse von $g \in G$. Dann ist $\bar{g} = \bar{g}e = \bar{g}gg^{-1} = eg^{-1} = g^{-1}$.

□

Satz 2. Seien G eine Gruppe und $a, b, c \in G$, sodass $ab = ac$. Dann ist $b = c$.

Beweis:

$$ab = ac \implies \underbrace{a^{-1}a}_e b = \underbrace{a^{-1}a}_e c \implies b = c$$

□

Beispiele

- Ganze Zahlen mit Addition, $(\mathbb{Z}, +)$ oder \mathbb{Z}^+
- Reelle Zahlen mit Addition, $(\mathbb{R}, +)$ oder \mathbb{R}^+
- Körper K mit Addition, $(K, +)$ oder K^+ . (Bemerkung: Keine Gruppe mit Multiplikation, wenn 0 enthalten ist.)
- Vektorraum V mit Addition, $(V, +)$ oder V^+ .
- Allgemeine lineare Gruppe, $GL_n(K)$
- Spezielle lineare Gruppe, $SL_n(K) := \{A \in GL_n(K) \mid \det A = 1\}$
- Orthogonale Gruppe, O_n
- Unitäre Gruppe, U_n

Permutationsgruppen

Sei $\text{Sym}(M)$ die Menge der Bijektionen von einer Menge M zu sich selbst, zusammen mit der Verknüpfung von Abbildungen. Die **symmetrische Gruppe** $S_n := \text{Sym}(\{1, 2, \dots, n\})$ ist eine Gruppe mit $n!$ Elementen.

Bemerkung 2. Jedes Element in S_n ist ein Produkt von Transpositionen.

Erinnerung: Eine **Transposition** ist eine Permutation, die genau zwei Elemente vertauscht und die übrigen gleich lässt.

Beispiel 1. S_3 , die Gruppe der Permutationen von $\{1, 2, 3\}$. Seien $\sigma, \tau \in S_3$,

$$\sigma: \begin{cases} 1 \rightarrow 2 \\ 2 \rightarrow 1 \\ 3 \rightarrow 3 \end{cases} \quad \tau: \begin{cases} 1 \rightarrow 2 \\ 2 \rightarrow 3 \\ 3 \rightarrow 1 \end{cases}$$

Dann sind $\sigma^2 = \text{id}$ und $\tau^3 = \text{id}$.

$$\left. \begin{array}{l} \sigma\tau(1) = 1 \\ \tau\sigma(1) = 3 \end{array} \right\} \rightarrow \sigma\tau \neq \tau\sigma$$

D.h. S_3 ist nicht abelsch.

Untergruppen

Definition 2. Sei G eine Gruppe. Eine **Untergruppe** $H \leq G$ ist eine Teilmenge $H \subseteq G$ sodass

- (a) $\forall a, b \in H, ab \in H$
- (b) $1_G \in H$
- (c) $\forall a \in H, a^{-1} \in H$

Bemerkung 3. Jede Untergruppe ist eine Gruppe $(H, *_{\mathcal{H}})$. $*_G$ induziert $*_{\mathcal{H}}$.

Bemerkung 4. $H \subseteq G$ mit $H \neq \{\emptyset\}$ ist eine Untergruppe von G genau wenn $\forall a, b \in H, ab^{-1} \in H$.

Beweis: " \Rightarrow ": klar.

" \Leftarrow ": Bedingung: Seien $a, b \in H$.

- (a) $\Rightarrow b^{-1} \in H$
 $\Rightarrow ab = a(b^{-1})^{-1} \in H$
- (b) $\Rightarrow aa^{-1} \in H, \text{ d.h. } 1_G \in H$
- (c) $\Rightarrow 1_G a^{-1} \in H \text{ d.h. } a^{-1} \in H$

□

Bemerkung 5. Jede Gruppe G hat als Untergruppen immer $\{1\}$ (die triviale Untergruppe) und G selbst. Andere Untergruppen heissen **echte** Untergruppen.

Beispiele

- $SL_n(K) \leq GL_n(K)$
- $n\mathbb{Z} \leq \mathbb{Z} \quad \forall n \in \mathbb{Z}$
- Sei $S^1 := \{c \in \mathbb{C}^* \mid |c| = 1\}$. $S^1 \leq \mathbb{C}^*$. ($\mathbb{C}^* := (\mathbb{C} \setminus \{0\}, \cdot)$)
- $B_n(K) := \{A \in GL_n(K) \mid \text{Aobere Dreiecksmatrix}\}$. $B_n \leq GL_n(K)$.
- $O_n \leq GL_n(\mathbb{R})$
- Die alternierende Gruppe $A_n \leq S_n$ ist die Untergruppe aller Permutationen, die das Produkt einer geraden Anzahl von Transpositionen sind.

Bemerkung 6. Seien G eine Gruppe und $a \in G$. Dann ist

$$\langle a \rangle := \{\dots, a^{-2}, a^{-1}, a^0, a, a^2, \dots\}$$

eine Untergruppe von G , genannt die von a erzeugte **zyklische Gruppe**.

Bemerkung 7. $\langle a \rangle$ ist abelsch: $a^m a^n = a^{m+n} = a^{n+m} = a^n a^m$

Lemma 1. Sei $X \subseteq \mathbb{Z}$ die Menge der Zahlen n , sodass $a^n = 1$. Dann ist $X = m\mathbb{Z}$ für ein $m \in \mathbb{Z}$.

Beweis: X ist eine Untergruppe von \mathbb{Z} :

- (a) Seien $m, n \in X$, dann ist $a^{m+n} = a^m a^n = 1_G \Rightarrow m+n \in X$
- (b) $a^0 = 1_G \Rightarrow 0 \in X$
- (c) $n \in X \Rightarrow a^{-n} = a^n a^{-n} = 1_G \Rightarrow -n \in X$

Gemäss Übung ist X von der Form $m\mathbb{Z}$ für ein $m \in \mathbb{Z}$.

□

Falls $m \neq 0$:

Für $n \in \mathbb{Z}$, schreibe $n = km + r$ für ein $k \in \mathbb{Z}$ s.d. $0 \leq r < m$. Dann ist $a^n = a^{km+r} = a^{km}a^r = a^r$. $\implies \langle a \rangle = \{1, a, \dots, a^{m-1}\}$ und all diese Elemente sind verschieden. (Falls $a^r = a^{r'} \implies a^{r-r'} = 1 \implies r - r' \in m\mathbb{Z} \implies r = r' \quad 0 \leq r, r' < m$)

Falls $m = 0$:

Dann ist $\langle a \rangle = \{\dots, a^{-2}, a^{-1}, 1, a, a^2, \dots\}$ und alle Partitionen sind verschieden.

Vorlesung 2

Definition 3. Die **Ordnung** $|G|$ einer Gruppe G ist die Anzahl der Elemente in G (kann ∞ sein). Die **Ordnung des Elements** $a \in G$ ist $|\langle a \rangle|$, wobei $\langle a \rangle = \{1, a, \dots, a^{m-1}\}$ mit $m > 0$ die kleinste Zahl s.d. $a^m = 1$.

Beispiele

- $A = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \in GL_2(\mathbb{R})$ hat Ordnung 6.
- $B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \in GL_2(\mathbb{R})$ hat Ordnung ∞ .

Homomorphismen

Definition 4. Seien G, G' zwei Gruppen. Ein **Homomorphismus** ist eine Abbildung $\phi: G \rightarrow G'$ s.d. $\phi(ab) = \phi(a)\phi(b) \quad \forall a, b \in G$.

Definition 5. Ein **Isomorphismus** ist ein bijektiver Homomorphismus.

Beispiele

- $\det: GL_n(K) \rightarrow K^*$
- signum - sign: $S_n \rightarrow \mathbb{Z}/2\mathbb{Z}$,

$$\text{sign}(x) = \begin{cases} 0 & \text{gerade Anzahl von Transpositionen} \\ 1 & \text{ungerade Anzahl von Transpositionen} \end{cases}$$
- Fixiere $a \in G$. $\phi: \mathbb{Z} \rightarrow G$, $\phi(n) = a^n$. ϕ ist injektiv $\Leftrightarrow \text{Ord}(a) = \infty$.
- $H \leq G$, die Inklusion $\iota: H \rightarrow G$, $\iota(x) = x$.

Satz 3.

- (1) Falls $\phi: G \rightarrow G'$ und $\psi: G' \rightarrow G''$ Homomorphismen sind, so auch $\psi \circ \phi: G \rightarrow G''$.
- (2) Falls $\phi: G \rightarrow G'$ ein Isomorphismus ist, so auch $\phi^{-1}: G' \rightarrow G$.

Beweis: (1) $\psi \circ \phi(ab) = \psi(\phi(a)\phi(b)) = \psi \circ \phi(a)\psi \circ \phi(b)$

(2) zu zeigen: ϕ^{-1} ist ein Homomorphismus.

Seien $a', b' \in G'$. Dann gibt es $a, b \in G$ s.d. $\phi(a) = a', \phi(b) = b'$

Es gilt $\phi(ab) = \phi(a)\phi(b) = a'b' \implies \phi^{-1}(a'b') = \phi^{-1}(a')\phi^{-1}(b')$

□

Bemerkung 8. Zwei zyklische Gruppen gleicher Ordnung sind immer isomorph.

Beweis: Seien $G = \langle a \rangle, G' = \langle b \rangle$ und $\phi: G \rightarrow G', \phi(a^n) \mapsto b^n$.

Falls $|G| = |G'|$ endlich ist, so ist $G = \{1, a, \dots, a^{m-1}\}, G' = \{1, b, \dots, b^{m-1}\}$. Somit ist ϕ wohldefiniert, bijektiv und ein Homomorphismus.

Falls $|G| = |G'| = \infty$, so ist ϕ wohldefiniert, bijektiv und ein Homomorphismus. □

Wir schreiben C_n für die zyklische Gruppe der Ordnung n .

Satz 4. Sei $\phi: G \rightarrow G'$ ein Homomorphismus. Dann sind $\phi(1_G) = 1_{G'}$ und $\phi(a^{-1}) = \phi(a)^{-1} \forall a \in G$

Beweis:

$$\begin{aligned} 1_G &= 1_G 1_G \\ \implies \phi(1_G) &= \phi(1_G 1_G) = \phi(1_G)\phi(1_G) \\ &\stackrel{\text{kürzen}}{\implies} 1_{G'} = \phi(1_G) \end{aligned}$$

Ausserdem:

$$\begin{aligned} \phi(a^{-1}\phi(a)) &= \phi(a^{-1}a) = \phi(1_G) = 1_{G'} \\ \implies \phi(a^{-1}) &= \phi(a)^{-1} \end{aligned}$$

□

Definition 6. Ein **Automorphismus** ist ein Isomorphismus $\phi: G \rightarrow G$ von einer Gruppe G zu sich selbst.

Beispiel 2. Für $f \in G$ definiere $\phi: G \rightarrow G, \phi(g) := f g f^{-1}$ ($f g f^{-1}$ ist das Konjugierte von g unter f). ϕ ist ein Automorphismus.

Beweis: Homomorphismus: $\phi(gh) = f g h f^{-1} = f g (f^{-1} f) h f^{-1} = \phi(g)\phi(h)$.
Bijektiv: $\phi^{-1}(g) = f^{-1} g f$ □

Definition 7. Für einen Homomorphismus $\phi: G \rightarrow G'$ definiere:

$\text{Bild } \phi := \{x \in G' \mid x = \phi(a) \text{ für ein } a \in G\}$

$\text{Kern } \phi := \{a \in G \mid \phi(a) = 1\}$

Übung: Zeige, dass beides Untergruppen von G' bzw. G sind.

Beispiele

- $\det: GL_n(K) \rightarrow K^*$, $\text{Kern } \det = SL_n(K)$
- $\text{sign} S_N \rightarrow C_2$, $\text{Kern } \text{sign} = A_n$

Bemerkung 9. Seien $\phi: G \rightarrow G'$ ein Homomorphismus und $a \in \text{Kern } \phi$ und $b \in G$. Dann ist

$$\begin{aligned}\phi(bab^{-1}) &= \phi(b)\phi(a)\phi(b)^{-1} = 1 \\ \implies bab^{-1} &\in \text{Kern } \phi\end{aligned}$$

Definition 8. Eine Untergruppe $N \leq G$ heisst **Normalteiler**, falls $a \in N$ und $\forall b \in G \quad bab^{-1} \in N$.

$\stackrel{\text{Bem. 9}}{\implies}$ $\text{Kern } \phi$ ist immer ein Normalteiler.

Vorlesung 3

Erinnerung: Eine Untergruppe $N \leq G$ ist ein Normalteiler, falls:

$$\forall a \in N, \forall b \in G : bab^{-1} \in N$$

. Clicker Frage zu Normalteilern \trianglelefteq :

1. $B_n(K) \leq GL_n(K)$ ist kein Normalteiler.
2. $Z^+ \trianglelefteq R^+$ ist Normalteiler (weil R^+ abelsch)
3. $SL_n(K) \trianglelefteq GL_n(K)$, weil $\det(ABA^{-1}) = \det(A) \det(B) \det(A)^{-1} = \det(B)$,
oder bemerke, dass $SL_n(K) = \text{Kern det}$
4. $A_n \trianglelefteq S_n$ weil $A_n = \text{Kern sign}$.

Partitionen

Sei $\phi: G \rightarrow G'$ ein Homomorphismus. Für jedes Element $h \in H$ betrachte die **Faser** $\phi^{-1}(h) = \{g \in G \mid \phi(g) = h\}$ (Urbild von G in H). Die Fasern bilden eine Partition von G .

Beispiel 3. Sei $\phi: \mathbb{C}^* \rightarrow \mathbb{R}_{>0}^*$, $\phi(z) \mapsto |z|$. Allgemein: $\phi^{-1} = \text{Kern } \phi$.

Satz 5. Sei $U: G \rightarrow G'$ ein Homomorphismus mit Kern N . Für $a, b \in G$ gilt $\phi(a) = \phi(b) \Leftrightarrow \exists n' \in N$ s.d. $b = an$, d.h. $a^{-1}b \in N$.

Beweis: “ \Rightarrow ”: Falls $\phi(a) = \phi(b)$, dann ist $U(a)^{-1}\phi(b) = \phi(a^{-1}b) = 1$, d.h. $\exists n \in N$, s.d. $a^{-1}b = n \implies b = an$.

“ \Leftarrow ” Falls $b = an$ für $n \in N$, dann ist $\phi(b) = \phi(a)\phi(n) = \phi(a)$. □

Aus dem Satz folgt, dass die Fasern von ϕ alle von der folgenden Form sind:

$$aN = \{g \in G \mid g = an \text{ für ein } n \in N\}$$

Korollar 1. Ein Homomorphismus $\phi: G \rightarrow G'$ ist injektiv $\Leftrightarrow \text{Kern } \phi = \{1\}$.

Beweis: “ \Rightarrow ” klar.

“ \Leftarrow ” Man nehme an, dass der Kern $\phi = \{1\}$. $\phi(a) = \phi(b) \Leftrightarrow a^{-1}b \in \text{Kern } \phi$, d.h. $a^{-1} + b = 1 \Rightarrow a = b$. \square

Nebenklassen

Erinnerung: Sei X eine Menge. Eine **Äquivalenzrelation** auf X ist eine binäre Relation \sim so dass:

- i) (Transitivität) Falls $a \sim b$ und $b \sim c$, dann ist $a \sim c$.
- ii) (Symmetrie) Falls $a \sim b$, so ist $b \sim a$.
- iii) (Reflexivität) $a \sim a$ für alle $a \in X$.

Gesehen: Jede Äquivalenzrelation definiert eine Partition von X . Diese besteht aus den **Äquivalenzklassen**, d.h. Teilmengen von der Form $[a] := \{b \in X \mid b \sim a\}$.

Sei \bar{X} die Menge der Äquivalenzklassen. Dann erhalten wir eine surjektive Abbildung $\pi: X \rightarrow \bar{X}$, $\pi(a) := [a]$. Dann ist $\pi^{-1}([a]) = \{b \in X \mid b \sim a\}$.

Gesehen: “Rechnen modulo m ”. \mathbb{Z} mit Äquivalenzrelation \equiv , wobei $a \equiv b$ falls $a - b \in m\mathbb{Z}$.

Menge der Äquivalenzklassen: $\mathbb{Z}/m\mathbb{Z}$. $\mathbb{Z}/m\mathbb{Z} = \{[0], [1], \dots, [m-1]\}$.

Ausserdem können wir die Klassen in $\mathbb{Z}/m\mathbb{Z}$ miteinander addieren, so dass $[a + b] = [a] + [b]$.

$\mathbb{Z}/m\mathbb{Z}$ mit Addition ist somit eine Gruppe, und die Quotientenabbildung $\pi: \mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$, $\pi(n) := [n]$ ist ein Homomorphismus.

Definition 9. Sei $H \leq G$ eine Untergruppe. Eine **Linksnebenklasse** von H ist eine Teilmenge von der Form $aH = \{ah \mid h \in H\}$ für ein $a \in G$.

Beispiel 4. $m\mathbb{Z}^+ \leq \mathbb{Z}^+$. Dann sind die Linksnebenklassen $m\mathbb{Z}$ die Teilmengen von der Form $0 + m\mathbb{Z}, 1 + m\mathbb{Z}, \dots, (m-1) + m\mathbb{Z}$.

Wir schreiben $a \equiv b$, falls ein $h \in H$ existiert, so dass $b = ah$, d.h. falls $b \in aH$.

Satz 6. Die Relation “ \equiv ” ist eine Äquivalenzrelation.

Beweis: 1. Falls $a \equiv b$ und $b \equiv c \Rightarrow \exists h, h' \in H$, so dass $b = ah$ und $c = bh' \Rightarrow c = a \underbrace{hh'}_{\in H} \Rightarrow c \equiv a$.

2. falls $a \equiv b$, so $\exists h \in H$ s.d. $b = ah \Rightarrow a = b \underbrace{h^{-1}}_{\in H} \Rightarrow b \equiv a$.

3. $a = a \cdot 1$ und $1 \in H \implies a \equiv a$.

$\phi: X \rightarrow Y$ Abbildung $\phi^{-1}(y) = \{x \in X \mid \phi(x) = y\}$ für $y \in Y$. □

Korollar 2. Die Linksnebenklassen bilden eine Partition von G .

Beweis: $aH = bH \Leftrightarrow a \equiv b$. □

Definition 10. Die Anzahl der Linksnebenklassen von H in G ist der sogenannte **Index von H in G** . Wir schreiben $[G : H]$ für den Index. ($[G \text{ in } H]$ kann ∞ sein.)

Beispiel 5. $m \geq 1$, $[\mathbb{Z} : m\mathbb{Z}] = m$.

Satz 7. Sei G eine endliche Gruppe und $H \leq G$. Dann ist $|G| = |H|[G : H]$.

Beweis: Die Abbildung $\phi: H \rightarrow aH$, $\phi(h) = ah$.

ϕ ist eine Bijektion. $\implies |H| = |aH|$.

Die Linksnebenklassen bilden eine Partition von G . $\implies |G| = |H|[G : H]$ □

Daraus folgt direkt:

Korollar 3 (Satz von Lagrange). Seien G eine Gruppe und $H \leq G$ eine Untergruppe. Dann ist $|H|$ ein Teiler von $|G|$.

Bemerkung 10. Falls $a \in G$, dann folgt mit Lagrange, dass $|\langle a \rangle| \mid |G|$, d.h. $\text{Ord}(a)$ teilt die Ordnung von G .

Korollar 4. Sei G eine Gruppe, s.d. $|G|$ prim ist. Sei $a \in G, a \neq 1$, dann ist $G = \langle a \rangle$.

Beweis: $\text{ord } a \mid p$, da $\text{ord } a > 1$ ist, $\text{ord } a = p$, d.h. $|\langle a \rangle| = p \implies \langle a \rangle = G$. □

Korollar 5. Seien G, G' endliche Gruppen und $\phi: G \rightarrow G'$ ein Homomorphismus. Dann gilt:

$$|G| = |\text{Kern } \phi| \cdot |\text{Bild } \phi|$$

Beweis: Gesehen: Die Linksnebenklassen von $\text{Kern } \phi$ sind die Fasern von ϕ .

$$\implies |\text{Bild } \phi| = [G : \text{Kern } \phi]$$

$$\implies |G| = |\text{Kern } \phi| \cdot [G : \text{Kern } \phi]$$

$$= |\text{Kern } \phi| \cdot |\text{Bild } \phi| \quad \square$$

Definition 11. Sei G eine Gruppe und $H \leq G$. Die **Rechtsnebenklassen** von H in G sind die Mengen $Ha := \{ha \mid h \in H\}$.

Definiere $a \equiv_R b$, falls es ein $h \in H$ gibt, so dass $b = ha$.

Dies definiert eine Äquivalenzrelation auf G und die Rechtsnebenklassen sind die Äquivalenzklassen bezüglich dieser Relation. \sim Partition von G .

Satz 8. *Eine Untergruppe $H \leq G$ ist ein Normalteiler \Leftrightarrow jede Linksnebenklasse ist auch eine Rechtsnebenklasse. In diesem Fall ist $aH = Ha$.*

Beweis: " \Rightarrow " H Normalteiler. Sei $h \in H$ und $a \in G$.

$$\begin{aligned} \Rightarrow ah &= \underbrace{(aha^{-1})}_{=:k \in H} a = ka \\ \Rightarrow aH &\subset Ha \end{aligned}$$

Analog zeigt man $Ha \subset aH$. $\Rightarrow aH = Ha$.

" \Leftarrow " Man nehme an, H ist kein Normalteiler.

$$\Rightarrow \exists h \in H, g \in G \text{ s.d. } aha^{-1} \notin H, \text{ d.h. es gibt kein } h' \in H \text{ s.d. } ah = h'a.$$

$$\Rightarrow ah \in aH, \text{ aber } ah \notin Ha, \text{ d.h. } aH \neq Ha.$$

Gleichzeitig ist $a \in aH \cap Ha \neq \emptyset$

$\Rightarrow aH$ ist in keiner anderen Rechtsnebenklasse enthalten. D.h. Rechts- und Linksnebenklassen definieren zwei verschiedene Partitionen. \square