Algebra I – Prof. Christian Urech

Mitschrift: Franz Nowak

Herbstsemester 2025

Vorlesung 1

Definition 1. *Eine **Gruppe** ist eine Menge G zusammen mit einer Verknüpfung $*\colon G \to G, \qquad (g,h) \to g*h$, sodass:*

(1) (Assoziativität) $\forall g,h,k \in G\colon (g*h)*k = g*(h*k)$

(2) (Neutrales Element) $\exists e \in G\colon g*e = e*g = g \quad \forall g \in G$

(3) (Inverses Element) $\forall g \in G \exists g^{-1} \in G$ *s.d.* $g*g^{-1} = g^{-1}*g = e$

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

Wir schreiben oft 1 oder 1_G für e und gg' für $g*g'$ mit $g,g' \in G$. Wenn G kommutativ ist, dann schreiben wir $e=0$ und $a+b$ für $a*b$. Des Weiteren ist $a^n := \overbrace{a\cdots a}^{\text{n-mal}}$ und $a^0 := 1$.

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

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 $\overline{g}, g^{-1}$ Inverse von $g \in G$. Dann ist $\overline{g} = \overline{g}e = \overline{g}gg^{-1} = eg^{-1} = g^{-1}$.

□

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 $\mathrm{Sym}(M)$ die Menge der Bijektionen von einer Menge M zu sich selbst, zusammen mit der Verknüpfung von Abbildungen. Die **symmetrische Gruppe** $S_n := \mathrm{Sym}(\{1, 2, \ldots, n\})$ 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 $\sigma, \tau \in S_3$,*

$$\sigma\colon \begin{cases} 1 \to 2 \\ 2 \to 1 \\ 3 \to 3 \end{cases} \qquad \tau\colon \begin{cases} 1 \to 2 \\ 2 \to 3 \\ 3 \to 1 \end{cases}$$

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

$$\left.\begin{aligned} \sigma\tau(1) &= 1 \\ \tau\sigma(1) &= 3 \end{aligned}\right\} \to \sigma\tau \neq \tau\sigma$$

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* $(H, *_H)$. $*_G$ *induziert* $*_H$.

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

(b) $\implies aa^{-1} \in H, d.h. 1_G \in H$

(c) $\implies 1_G a^{-1} \in H$ 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 $S^1 := \{c \in \mathbb{C}^* \mid |C| = 1\}$. $S^1 \leq \mathbb{C}^*$. $(\mathbb{C}^* := (\mathbb{C}\backslash\{0\}, \cdot)$
- $B_n(K) := \{A \in GL_n(K) \mid A$obere 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*

$$<a> := \{\ldots, a^{-2}, a^{-1}, a^0, a, a^2, \ldots\}$$

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

Bemerkung 7. $<a>$ *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 $a^{m+n} = a^m a^n = 1_G \implies m + n \in X$

(b) $a^0 = 1_G \implies 0 \in X$

(c) $n \in X \implies a^{-n} = a^n a^{-n} = 1_G \implies -n \in X$

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 $a^n = a^{km+r} = a^{km}a^r = a^r$. $\implies$ $<a> = \{1, a, \ldots, a^{m-1}\}$ 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 $<a> = \{\ldots, a^{-2}, a^{-1}, 1, a, a^2, \ldots\}$ 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 $|<a>|$, wobei $<a> = \{1, a, \ldots, a^{m-1}\}$ 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 $\phi\colon G \to G'$ s.d. $\phi(ab) = \phi(a)\phi(b) \quad \forall a, b \in G$.*

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

Beispiele

- $\det\colon GL_n(K) \to K^*$
- signum - sign: $S_n \to \mathbb{Z}/2\mathbb{Z}$,
  $\operatorname{sign}(x) = \begin{cases} 0: & \text{gerade Anzahl von Transpositionen} \\ 1: & \text{ungerade Anzahl von Transpositionen} \end{cases}$
- Fixiere $a \in G$. $\phi\colon \mathbb{Z} \to G$, $\phi(n) = a^n$. ϕ ist injektiv $\Leftrightarrow \operatorname{Ord}(a) = \infty$.
- $H \leq G$, die Inklusion $\iota\colon H \to G, \quad \iota(x) = x$.

Satz 3.

(1) Falls $\phi\colon G \to G'$ und $\psi\colon G' \to G''$ Homomorphismen sind, so auch $\psi \circ \phi\colon G \to G''$.

(2) Falls $\phi\colon G \to G'$ ein Isomorphismus ist, so auch $\phi^{-1}\colon G' \to G$.

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 zuklische Gruppen gleicher Ordnung sind immer isomorph.*

Beweis: Seien $G = <a>, G' = <b>$ und $\phi\colon G \to G', \quad \phi(a^n) \mapsto b^n$.

Falls $|G| = |G'|$ endlich ist, so ist $G = \{1, a, \ldots, a^{m-1}\}$, $G' = \{1, b, \ldots, b^{m-1}\}$. 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 $\phi\colon G \to G'$ ein Homomorphismus. Dann sind $\phi(1_G) = 1_{G'}$ und $\phi(a^{-1}) = \phi(a)^{-1}$ $\forall a \in G$*

Beweis:

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

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 $\phi\colon G \to G$ von einer Gruppe G zu sich selbst.*

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

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

Definition 7. *Für einen Homomorphismus $\phi\colon G \to G'$ definiere:*

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

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

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

Beispiele

- $\det\colon GL_n(K) \to K^*, \quad \operatorname{Kern}\det = SL_n(K)$
- $\operatorname{sign} S_N \to C_2, \quad \operatorname{Kern}\operatorname{sign} = A_n$

Bemerkung 9. *Seien $\phi\colon G \to G'$ ein Homomorphismus und $a \in$ Kern ϕ 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 $\forall b \in G$ $bab^{-1} \in N$.*

$\overset{\text{Bem. 9}}{\implies}$ Kern ϕ 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 $SL_n(K) = \operatorname{Kern}\det$
4. $A_n \trianglelefteq S_n$ weil $A_n = \operatorname{Kern}\operatorname{sign}$.

Partitionen

Sei $\phi\colon G \to G'$ 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* $\phi\colon \mathbb{C}^* \to \mathbb{R}^*_{>0}$, $\quad \phi(z) \mapsto |z|$. $\quad$ *Allgemein:* $\phi^{-1} = Kern\,\phi$.

Satz 5. *Sei* $U : G \to G'$ *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 it $U(a)^{-1}\phi(b) = \phi(a^{-1}b) = 1$, 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* $\phi\colon G \to G'$ *ist injektiv* $\Leftrightarrow Kern\,\phi = \{1\}$.

Beweis: "$\Rightarrow$" klar.

"$\Leftarrow$" Man nehme an, dass der Kern $\phi = \{1\}$. $\phi(a) = \phi(b) \Leftrightarrow a^{-1}b \in \operatorname{Kern}\phi$, d.h. $a^{-1} + b = 1 \implies a = b$. □

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 $\overline{X}$ die Menge der Äquivalenzklassen. Dann erhalten wir eine surjektive Abbildung $\pi\colon X \to \overline{X}, \qquad \pi(a) := [a]$. 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: $\mathbb{Z}/m\mathbb{Z}$. $\qquad \mathbb{Z}/m\mathbb{Z} = \{[0], [1], \ldots, [m-1]\}$.

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 $\pi\colon \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, \quad \pi(n) := [n]$ 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 $0 + m\mathbb{Z}, 1 + m\mathbb{Z}, \ldots, (m-1) + m\mathbb{Z}$.*

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

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

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

$\phi\colon X \to Y$ 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. ($[G$ in $H]$ kann ∞ sein.)*

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

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

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

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

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

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 $|<a>| \mid |G|$, d.h. $Ord(a)$ 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 $G = <a>$.*

Beweis: $\operatorname{ord} a \big| p$, da $\operatorname{ord} a > 1$ ist, $\operatorname{ord} a = p$, d.h. $|<a>| = p \implies <a> = G$. $\square$

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

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

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

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

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

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

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. $\rightsquigarrow$ 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 $a \in G$.

$$\implies ah = \underbrace{(aha^{-1})}_{=:k \in H} a = ka$$

$$\implies aH \subset Ha$$

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

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

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

$\implies ah \in aH$, aber $ah \notin Ha$, d.h. $aH \neq Ha$.

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

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