

Algebra I – Prof. Christian Urech

Mitschrift: Franz Nowak

Herbstsemester 2025

Vorlesung 1

Definition 1. Eine **Gruppe** ist eine Menge G zusammen mit einer Verknüpfung $\ast: G \rightarrow G, (g, h) \rightarrow g \ast h$, 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 sind

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

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

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 $\phi: G \rightarrow G, \phi(g) := fgf^{-1}$ (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 $\phi: G \rightarrow G'$ definiere:

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

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

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

Beispiele

- $\det: GL_n(K) \rightarrow K^*$, Kern $\det = SL_n(K)$
- $\text{sign} S_n \rightarrow C_2$, 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 $\forall b \in G \quad bab^{-1} \in N$.

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

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 $\phi(a) = \phi(b) \Leftrightarrow \exists n' \in N \text{ s.d. } b = an', \text{ d.h. } a^{-1}b \in N$.

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 $\phi(b) = \phi(a)\phi(n) = \phi(a)$. \square

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. $a^{-1}b = 1 \implies a = b$. \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 \overline{X} die Menge der Äquivalenzklassen. Dann erhalten wir eine surjektive Abbildung $\pi: X \rightarrow \overline{X}$, $\pi(a) := [a]$. 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 $b \equiv a \implies \exists h, h' \in H$, 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 $1 \in H \implies a \equiv a$.

$\phi: X \rightarrow Y$ 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. ($[G : H]$ 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 .

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

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

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

□

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 $a \in G$.

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

$$\implies aH \subseteq Ha$$

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

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

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

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

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. □

Vorlesung 4

Clicker Frage zu Homomorphismen $\phi: G \rightarrow G'$:

- Gesehen in Übung: $\text{Bild } \phi \leq G'$.
- Dann folgt mit Kor. 3: $|\text{Bild } \phi| \mid |G'|$
- Und mit Kor. 5: $|\text{Bild } \phi| \mid |G|$.

Seien G eine Gruppe und $H \leq G \rightsquigarrow G/H$ Linksnebenklassen von H in G . Können wir auf G/H eine Gruppenstruktur definieren, so dass die Abbildung $\pi: G \rightarrow G/H, \pi(g) = gH$ ein Gruppenhomomorphismus ist?

Ja, wenn $H \trianglelefteq G$ (siehe Übung).

Faktorgruppen

Lemma 2. Seien G eine Gruppe und X eine Menge mit einer Verknüpfung. Sei $\phi: G \rightarrow X$ eine surjektive Abbildung, so dass $\phi(ab) = \phi(a)\phi(b) \quad \forall a, b \in G$. Dann ist X eine Gruppe.

Beweis: (i) Seien $u, v, w \in X$. $\exists a, b, c \in G$ s.d. $\phi(a) = u, \phi(b) = v, \phi(c) = w$.
Dann ist

$$\begin{aligned} u(vw) &= \phi(a)(\phi(b)\phi(c)) = \phi(a)\phi(bc) \\ &= \phi(abc) = \phi(ab)\phi(c) \\ &= (\phi(a)\phi(b))\phi(c) = (uv)w \end{aligned}$$

\rightsquigarrow Assoziativität der Verknüpfung auf X .

(ii) Sei $e := \phi(1)$ und $u \in X$. Dann

$$\exists u \in G, \text{ s.d. } u = \phi(a) \implies eu = \phi(1)\phi(a) = \phi(1a) = \phi(a) = u.$$

Analog: $ue = u$. $\rightsquigarrow e$ ist ein neutrales Element.

(iii) Sei $u \in X \implies \exists a \in G$ s.d. $u = \phi(a)$. Sei $u' := \phi(a^{-1})$. Dann ist

$$u'u = \phi(a^{-1})\phi(a) = \phi(a^{-1}a) = \phi(1) = e.$$

Analog: $uu' = e$. \rightsquigarrow es existieren Inverse.

□

Notation: Seien G eine Gruppe, $A, B \subseteq G$. Dann definieren wir

$$AB := \{ab \mid a \in A, b \in B\} \subseteq G.$$

Lemma 3. Seien G eine Gruppe, $N \trianglelefteq G$ ein Normalteiler und $a, b \in G$. Dann ist $(aN)(bN) = abN$. Das Produkt von zwei Nebenklassen ist also wieder eine Nebenklasse.

Beweis: In Vorlesung 3 gesehen:

$$Nb = bN \quad \forall b \in G$$

Da N eine Untergruppe ist, ist $NN = N$ (Übung).

$$\implies (aN)(bN) = a(Nb)N = a(bN)N = abNN = abN.$$

□

Wir erhalten also eine Verknüpfung auf die Nebenklassen. Falls $K_1, K_2 \in G/N$: Sei $a \in K_1, b \in K_2$. $\implies K_1 = aN, K_2 = bN$. Dann ist $K_1K_2 = abN$ (gemäss Lemma), d.h. K_1K_2 ist die Nebenklasse, die das Element ab enthält.

Satz 9. Seien G eine Gruppe und $N \trianglelefteq G$. Mit dieser Verknüpfung bildet $G/N =: \overline{G}$ eine Gruppe und die Abbildung $\pi: G \rightarrow G/N = \overline{G} \quad a \mapsto aN =: \overline{a}$ ist ein Homomorphismus.

Beweis: Bereits beobachtet: $\pi(a)\pi(b) = (aN)(bN) = abN = \pi(ab)$.

Aus Lem. 2 folgt, dass $\overline{G} = G/N$ eine Gruppe ist und daher π ein Homomorphismus ist. \square

Korollar 6. Jeder Normalteiler $N \leq G$ ist Kern von einem Homomorphismus. Nämlich vom Homomorphismus $\pi: G \rightarrow G/N$.

Beweis: Das neutrale Element von G/N ist N . $\rightsquigarrow \text{Kern } \pi = N$ \square

Satz 10 (erster Isomorphiesatz). Sei $\phi: G \rightarrow G'$ ein surjektiver Homomorphismus und $N := \text{Kern } \phi$. Dann ist die Gruppe G/N isomorph zur Gruppe G' unter dem Homomorphismus $\overline{\phi}: G/N \rightarrow G' \quad \overline{a} = aN \mapsto \phi(a)$

Beweis: 1. $\overline{\phi}$ ist wohldefiniert: $\phi(an) = \phi(a)\phi(n) = \phi(a)$, d.h. $\overline{\phi}(aN)$ hängt nicht von der Wahl des Repräsentanten ab.

2. $\overline{\phi}$ ist ein Homomorphismus:

$$\begin{aligned} \overline{\phi}((aN)(bN)) &= \overline{\phi}(abN) \\ &= \phi(ab) = \phi(a)\phi(b) \\ &= \overline{\phi}(aN)\overline{\phi}(bN) \end{aligned}$$

3. $\overline{\phi}$ ist bijektiv: $\overline{\phi}$ ist surjektiv, da ϕ surjektiv ist. $\overline{\phi}$ ist injektiv, da $\text{Kern } \overline{\phi} = \{N\}$ und N ist das neutrale Element in G/N . $\implies \overline{\phi}$ ist injektiv. \square

Definition 12. Seien G, G' Gruppen, dann ist $G \times G'$ eine Gruppe mit der Verknüpfung $(a, a')(b, b') = (ab, a'b')$. Neutrales Element: $(1_G, 1_{G'})$. Inverses Element: $(a, a')^{-1} = (a^{-1}, a'^{-1})$. Es heisst das **direkte Produkt** von G und G' .

Vorlesung 5

Clicker Frage: Sei $S^1 \leq \mathbb{C}^*$ die Untergruppe der komplexen Zahlen bestehend aus den Elementen mit Betrag 1. Dann ist der Quotient \mathbb{C}^*/S^1 isomorph zu $\mathbb{R}_{>0}^*$. (Wahr)

Begründung: Die Abbildung $\phi: \mathbb{C}^* \rightarrow \mathbb{R}_{>0}^*$, $z \mapsto |z|$ ist ein surjektiver Homomorphismus. $\text{Kern } \phi = S^1 \stackrel{\text{Isosatz}}{\xrightarrow{1.}} \mathbb{C}^*/S^1 \simeq \mathbb{R}_{>0}^*$

Clicker Frage: Sei G eine Gruppe und $H_1, H_2 \leq G$ Untergruppen. Dann ist $H_1 \cap H_2$ eine Untergruppe von G . (Wahr)

Begründung:

$$\begin{aligned} 1 &\in H_1 \cap H_2 \\ a, b \in H_1 \cap H_2 &\implies ab \in H_1 \cap H_2 \\ a^{-1} &\in H_1 \cap H_2 \end{aligned}$$

AllgemeinL Falls $H_i \leq G, i \in I$ eine Familie von Untergruppen ist, so ist $\bigcap_{i \in I} H_i \leq G$ eine Untergruppe (selber Beweis).

Definition 13. Sei $S \subseteq G$ eine Teilmenge. Dann ist $\langle S \rangle := \bigcap_{H \leq G, S \subseteq H} H$ die **von S erzeugte Untergruppe**.

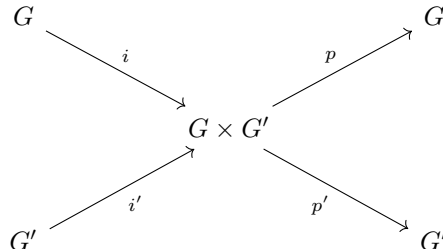
Erinnerung: G, G' Gruppen $\rightsquigarrow G \times G'$ ist Gruppe mit Verknüpfung $(a, a')(b, b') = (ab, a'b')$.

Bsp: Kleinsche Vierergruppe (die "Maträtzengruppe").

$$C_2 \times C_2 = \{(1, 1), (1, -1), (-1, 1), (-1, -1)\}$$

Bsp: $m, n > 0$ s.d. $\text{ggT}(m, n) = 1$ dann ist $C_{mn} \simeq C_m \times C_n$

Wir haben vier Homomorphismen:



$$\begin{aligned} i(x) &= (x, 1) \\ i'(x) &= (1, x') \\ p(x, x') &= x \\ p'(x, x') &= x' \end{aligned}$$

Bemerkung 11. i, i' sind injektiv, d.h.

$$\begin{aligned} G \times 1 &= \text{Bild } i \simeq G \\ 1 \times G' &= \text{Bild } i' \simeq G' \end{aligned}$$

p und p' sind surjektiv

$$\text{Kern } p = 1 \times G', \text{ Kern } p' = G \times 1$$

Sei H eine Gruppe und $\phi: H \rightarrow G, \phi': H \rightarrow G'$ Homomorphismen. Dann ist $\Phi: H \rightarrow G \times G' \quad \Phi(h) = (\phi(h), \phi'(h))$ ein Homomorphismus.

Umgekehrt ist jeder Homomorphismus $\Phi: H \rightarrow G \times G'$ von dieser Form mit $\phi = \Phi \circ p$ und $\phi' = \Phi \circ p'$.

Bemerkung 12. $\Phi(h) = (1, 1) \Leftrightarrow \phi(h) = 1$ und $\phi'(h) = 1$ d.h. $\text{Kern } \Phi = \text{Kern } \phi \cap \text{Kern } \phi'$.

Seien $H, K \leq G$. Betrachte $HK = \{hk \mid h \in H, k \in K\}$. Wann ist HK eine Untergruppe? Wann ist $\pi: H \times K \rightarrow G \quad \pi(h, k) = hk$ ein Homomorphismus?

Satz 11. (a) Ist $H \cap K = \{1\}$, so ist π injektiv.

(b) Ist H oder K ein Normalteiler, so ist $HK = KH$ und HK ist eine Untergruppe von G .

(c) Sind H und K Normalteiler und gilt $H \cap K = \{1\}$ und $HK = G$ so ist $\pi: H \times K \rightarrow G$ ein Isomorphismus.

Beweis: (a) Seien $(h_1, k_1), (h_2, k_2) \in H \times K$ s.d. $h_1 k_1 = h_2 k_2$.

$$\begin{aligned} \implies \underbrace{k_1 k_2^{-1}}_{\in K} &= \underbrace{h_1^{-1} h_2}_{\in H} \stackrel{H \cap K = \{1\}}{=} 1 \\ \implies k_1 &= k_2 \text{ und } h_1 = h_2 \\ \implies \pi &\text{ ist injektiv.} \end{aligned}$$

(b) oBdA. H ist Normalteiler. Seien $h \in H, k \in K$.

$$\begin{aligned} \implies kh &= \underbrace{(khk^{-1})}_{\in H} k \in HK \\ \implies KH &\subset HK \end{aligned}$$

Analog: $HK \subset KH \implies KH = HK$. Z.z: HK ist Untergruppe.

(i) Seien $hk, h'k' \in HK$.

$$\begin{aligned} \implies (hk)(h'k') &= h \underbrace{(kh')}_{\in KH=HK} k' \\ &= h(h''k'')k' \\ &= (hh'')(k''k') \in HK \end{aligned}$$

(ii) $1 \in HK$

(iii) $hk \in HK \implies (hk) = k^{-1}h^{-1} \in kh = HK$

(c) Seien $h \in H, k \in K$

$$\implies \underbrace{\underbrace{(hkh^{-1})}_{\in K}}_{\in K} k^{-1} = h \underbrace{\underbrace{(kh^{-1}k^{-1})}_{\in H}}_{\in H}$$

$$\implies hkh^{-1}k^{-1} = 1$$

$$\implies hk = kh$$

$$\implies \pi(h_1, k_1)\pi(h_2, k_2) = h_1k_1h_2k_2 = h)1h_2k_1k_2 = \pi((h_1, k_1)(h_2, k_2))$$

$\implies \pi$ ist Homomorphismus. Gemäss (a) ist π injektiv. Da $HK = G$ ist π surjektiv $\implies \pi$ ist Isomorphismus.

□

Beispiele

- Gruppen von der Ordnung 1: nur $\{1\}$
- Gruppen von der Ordnung 2: nur C_2
- Gruppen von der Ordnung 3: nur C_3
- Gruppen von der Ordnung 4: $C_4, C_2 \times C_2$ (s. Übung).
- Gruppen von der Ordnung 5: C_5

Behauptung 1. Die einzigen Gruppen von Ordnung 6 sind C_6 und S_3 (bis auf Isomorphie).

Beweis: Sei G eine Gruppe mit $|G| = 6$. Falls G ein Element der Ordnung 6 enthält, so ist $G \simeq C_6$. Ansonsten 3 mögliche Fälle:

- Alle $g \in G, g \neq 1$ haben Ordnung 2
- Alle $g \in G, g \neq 1$ haben Ordnung 3
- Es gibt $g \in G$ von Ordnung 2 und $h \in G$ von Ordnung 3.

Falls (a), so ist G abelsch. Sei $g \in G$

$$\begin{aligned} \implies \langle g \rangle &= \{1, g\} \trianglelefteq G \\ \implies |G/\langle g \rangle| &= 3 \\ \implies G/\langle g \rangle &\simeq C_3 \end{aligned}$$

$\pi: G \rightarrow G/\langle g \rangle$ Quotient

$\forall g \in G$ ist $\pi(g)^2 = \pi(g^2) = 1$. Widerspruch zu $|G/\langle g \rangle| = 3$.

Falls (b), so gilt $g = g^{-1}$ nur wenn $g = 1$. $\implies G = \{1, g, g^{-1}, h, h^{-1}, \dots\}$.
Nicht möglich, da G eine gerade Ordnung hat.

D.h. wir sind im Fall (c). G enthält $1, g, h, h^2, gh, gh^2$. (kleine Übung: Diese Elemente sind alle verschieden). $\implies G = \{1, g, h, h^2, gh, gh^2\}$.

Wir haben $hg = gh$ oder $hg = gh^2$. Falls $hg = gh$, so hätte (gh) Ordnung 6. Das haben wir aber ausgeschlossen. Also ist $hg = gh^2$.

Die Relation $gh = h^2g$ definiert die Verknüpfung auf G eindeutig. Jedes Produkt in g und h lässt sich mit dieser Regel in die Form $g^i h^j$ bringen, wobei $0 \leq i \leq 1, 0 \leq j \leq 2$.

Im Fall (c) gibt es also höchstens eine Gruppe. Diese muss S_3 sein. \square

Bemerkung 13. Seien $g, h \in S_3$, mit

$$g: \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 1 \\ 3 \mapsto 3 \end{cases} \quad h: \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 1 \end{cases}$$

Dann ist $S_3 = \{1, g, h, h^2, gh, gh^2\}$.

Bemerkung 14. Jede echte Untergruppe von S_3 ist zyklisch (da von Ordnung 2 oder 3).

Bemerkung 15. $A_3 = \langle h \rangle$

Symmetrie

Isometrien von \mathbb{R}^n

Definition 14. Eine **Isometrie** von \mathbb{R}^n ist eine Abbildung $f: \mathbb{R}^n \rightarrow \mathbb{R}^n$ von der Form $f(X) = BX + a$ wobei $B \in O(n), a \in \mathbb{R}^n$. Wir bezeichnen mit $\text{Isom}(\mathbb{R}^n)$ die Gruppe der Isometrien von \mathbb{R}^n .

Bemerkung 16. Man kann zeigen, dass Isometrien genau die Abbildungen $\mathbb{R}^n \rightarrow \mathbb{R}^n$ sind, welche die Distanzen erhalten.

Zwei wichtige Untergruppen:

- (1) $\mathcal{T}_n \leq \text{Isom}(\mathbb{R}^n)$: Die Untergruppe der **Translationen**, d.h. Abbildung on der Form $t_a: X \mapsto X + a$ für $a \in \mathbb{R}^n$. Es gilt $t_a t_{a'} = t_{a+a'}$.
- (2) $O \leq \text{Isom}(\mathbb{R}^n)$: Die Untergruppe der Isometrien von der Form $d_B: X \mapsto BX$ für $B \in O(n)$. Es gilt $d_B d_{B'} = d_{BB'}$.

Jedes $f \in \text{Isom}(\mathbb{R}^n)$ lässt sich eindeutig schreiben als $t_a d_B$ für $B \in O(n), a \in \mathbb{R}^n$. Falls $f(X) = BX + a, g(X) = B'X + a'$, dann ist

$$\begin{aligned} f \circ g(X) &= B(B'X + a') + a \\ &= BB'X + Ba' + a \end{aligned}$$

D.h. falls $F = t_a d_B, g = t_{a'} + d_{B'}$, so ist

$$\begin{aligned} f \circ g &= t_a d_B t_{a'} d_{B'} \\ &= t_{Ba' + a} d_{BB'}. \end{aligned}$$

Wir haben also insbesondere Homomorphismus $\psi: \text{Isom}(\mathbb{R}^n) \rightarrow O, \psi(t_a d_B) = d_B$.

Kern $\psi = \mathcal{T}_n$.

Bemerkung 17. Die Abbildung $\text{Isom}(\mathbb{R}^n) \rightarrow \mathcal{T}_n, t_a d_B \mapsto t_a$ ist kein Homomorphismus.

Vorlesung 6

Gestern: $\text{Isom}(\mathbb{R}^n)$ Abbildung $\mathbb{R}^n \rightarrow \mathbb{R}^n$ von der Form $f(x) = t_a d_B(x) = BX + a$ $B \in O(n), a \in \mathbb{R}^n$.

$O \leq \text{Isom}(\mathbb{R}^n)$: Isometrien, die den Ursprung fixieren, d.h. von der Form $f(X) = d_B(X) = BX$.

$\mathcal{T}_n \leq \text{Isom}(\mathbb{R}^n)$ Translationen

Orientierung

Falls $n = 2$:

$$\text{Erinnerung: } SO(2) = \left\{ \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix} \mid 0 \leq \theta \leq 2\pi \right\}$$

$$O(2)/SO(2) = \{\pm 1\} \simeq C_2$$

$$\implies SO(2) \text{ hat zwei Nebenklassen: } O(2) = SO(2) \cup \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} SO(2).$$

Definition 15. Sei $f \in \text{Isom}(\mathbb{R}^2)$, $f = t_a d_B$.

Falls $B \in SO(2)$ ist, heisst f **orientierungserhaltend**.

Falls $B \in \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} SO(2)$, so heisst f **orientierungsumkehrend**.

Bemerkung 18. Falls $B \in SO(2)$, so ist d_B eine Drehung um O um den Winkel θ .

Bemerkung 19. Falls $B \in \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}$, so definiert d_B eine Spiegelung an der Geraden mit Winkel $\theta/2$ zur x -Achse.

Satz 12. Die Untergruppe von $\text{Isom}(\mathbb{R}^n)$ der Elemente, die einen Punkt $p \in \mathbb{R}^n$ fixieren, ist die konjugierte Untergruppe $O' = t_p O t_p^{-1} \leq \text{Isom}(\mathbb{R}^n)$

Beweis:

$$\begin{aligned}
f(p) = p &\Leftrightarrow t_p^{-1}f(p) = t_p^{-1}(p) = 0 \\
&\Leftrightarrow t_p^{-1}f(t_p(0)) = 0 \\
&\Leftrightarrow t_p^{-1}ft_p \in O \\
&\Leftrightarrow f \in t_p O t_p^{-1}
\end{aligned}$$

□

Satz 13. Sei $G \leq \text{Isom}(\mathbb{R}^n)$ eine endliche Untergruppe. So hat G einen Fixpunkt.

Beweis: Sei $m = |G|$, sei $G = \{f_1, \dots, f_m\}$. Sei $q \in \mathbb{R}^n$ beliebig. Betrachte die Bilder $q_i := f_i(q)$ für $i \in 1, \dots, m$. Sei $p := \frac{1}{m}(q_1 + \dots + q_m)$.

Behauptung: $f_j(p) = p \quad \forall f_j \in G$.

Beweis: Schreibe $f_j(X) = B_j X + a_j$.

$$\begin{aligned}
&\Rightarrow f_j(p) = B_j \left(\frac{1}{m}(q_1 + \dots + q_m) \right) + a_j \\
&= \frac{1}{m}(B_j q_1 + \dots + B_j q_m + m a_j) \\
&= \frac{1}{m}((B_j q_1 + a_j) + \dots + (B_j q_m + a_j)) \\
&= \frac{1}{m}(f_j(q_1) + \dots + f_j(q_m)) \\
&= \frac{1}{m}(f_j f_1(q) + \dots + f_j f_m(q)) \\
&\stackrel{(*)}{=} \frac{1}{m}(q_1 + \dots + q_m) = p
\end{aligned}$$

$$(*) : \{f_1, \dots, f_m\} = \{f_j f_1, \dots, f_j f_m\}$$

□

Korollar 7. Sei $G \leq \text{Isom}(\mathbb{R}^n)$. eine endliche Untergruppe. So gibt es ein $a \in \mathbb{R}^n$ so dass $t_a^{-1} G t_a \leq O$.

Beweis: Sei $a \in \mathbb{R}^n$ der Fixpunkt von G . Dann ist $G \leq t_a O t_a^{-1}$

$$\Rightarrow t_a^{-1} G t_a \leq O.$$

□

Satz 14. Sei $n = 2$ und sei $G \leq O$ eine endliche Untergruppe. So ist G eine der folgenden Gruppen:

- (a) Die zyklische Gruppe der Ordnung n erzeugt von der Drehung um den Winkel $\theta = 2\pi/n$.

(b) Die **Diedergruppe** D_n von Ordnung $2n$ erzeugt von zwei Elementen: der Drehung um den Winkel $\theta = 2\pi/n$ und einer Spiegelung S an einer geraden durch den Nullpunkt.

Beweis: **1. Fall:** Alle Elemente in G sind in $SO(2)$, d.h. Drehungen.

Behauptung: G ist zyklisch.

Beweis: Falls $G=\{1\}$, klar. Sonst: Sei θ der kleinste positive Drehwinkel der Elemente in G . Sei $d_\theta \in G$ diese Drehung.

Z.Z: $\langle d_\theta \rangle = G$.

Sei $d_\alpha \in G$ eine Drehung um den Winkel $\alpha > 0$. Schreibe $\alpha = n\theta + \beta$ mit $0 \leq \beta < \theta$ und $n \in \mathbb{Z}$.

$$d + B = d_\alpha d_{-n\theta} = d_\alpha (d_\theta^{-1})^n \in G$$

$$\implies \beta = 0$$

$$\implies d_\alpha (d_\theta^{-1})^n = 1$$

$$\implies d_\alpha = (d_\theta)^n \in \langle d_\theta \rangle$$

Sei $n \in \mathbb{N}$ minimal, s.d. $n\theta \geq 2\pi$.

D.h. $2\pi \leq n\theta < 2\pi + \theta$. Da θ der kleinste Drehwinkel in G ist, folgt daraus:
 $\implies 2\pi = n\theta \implies \theta = 2\pi/n$.

2. Fall: G enthält Spiegelung. Betrachte $\phi: G \rightarrow \{\pm 1\}$ gegeben durch Det.
 $\xrightarrow{1.Fall}$ Kern ϕ ist zyklisch erzeugt von Drehung $\implies G = \text{Kern } \phi + S \text{ Kern } \phi$
mit S Spiegelung. \square