Algebra I – Prof. Christian Urech

Mitschrift: Franz Nowak

Herbstsemester 2025

Vorlesung 1

Definition 1. *Eine **Gruppe** ist eine Menge G zusammen mit einer Verknüpfung $*\colon G \to G,\ (g,h) \to g*h$, 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 sind $a^n := \overbrace{a\cdots a}^{\text{n-mal}}$ und $a^0 := 1$.

Bemerkung 1. *Wenn G assoziativ ist, dann ist $g_1g_2\cdots g_n$ 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 $m \in \mathbb{Z}$. $\square$

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 $a^r = a^{r'} \implies a^{r-r'} = 1 \implies r - r' \in m\mathbb{Z} \implies r = r'$ $0 \leq r, r' < m$)

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. $\phi(ab) = \phi(a)\phi(b)$ $\forall a, b \in G$.*

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

Beispiele

- $\det\colon GL_n(K) \to K^*$
- signum - $\operatorname{sign}\colon S_n \to \mathbb{Z}/2\mathbb{Z}$,
  $\operatorname{sign}(x) = \begin{cases} 0: & \text{gerade Anzahl von Transpositionen} \\ 1: & \text{ungerade Anzahl von Transpositionen} \end{cases}$
- 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 $\iota\colon H \to G$, $\iota(x) = x$.

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:*

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

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

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 $a \in \operatorname{Kern}\phi$ und $b \in G$. Dann ist*

$$\phi(bab^{-1}) = \phi(b)\phi(a)\phi(b)^{-1} = 1$$
$$\implies bab^{-1} \in \operatorname{Kern}\phi$$

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

$\overset{\text{Bem. } 9}{\implies}$ $\operatorname{Kern}\phi$ 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 $SL_n(K) = \operatorname{Kern}\det$
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 $\phi\colon \mathbb{C}^* \to \mathbb{R}^*_{>0}, \qquad \phi(z) \mapsto |z|.$ Allgemein: $\phi^{-1} = \operatorname{Kern}\phi$.*

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: "⇒": 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. $a^{-1}b = n \implies b = an$.

"⇐" 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 $\Leftrightarrow \operatorname{Kern}\phi = \{1\}$.*

Beweis: "⇒" klar.

"⇐" 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 $\pi\colon X \to \overline{X}$, $\quad \pi(a) := [a]$. 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: $\mathbb{Z}/m\mathbb{Z}$. $\quad \mathbb{Z}/m\mathbb{Z} = \{[0], [1], \ldots, [m-1]\}$.

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. $\implies |G| = |H|[G : H]$ □

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. $|<a>| = p \implies <a> = G$. □

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.

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

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

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

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

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

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

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

$\implies \exists h \in H, g \in G$ 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. □

Vorlesung 4

Clicker Frage zu Homomorphismen $\phi\colon G \to G'$:

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

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 $\pi\colon G \to G/H, \pi(g) = gH$ 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 $\phi\colon G \to X$ 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 $\pi\colon G \to G/N = \overline{G} \quad a \mapsto aN =: \overline{a}$ 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. □

Korollar 6. *Jeder Normalteiler $N \leq G$ ist Kern von einem Homomorphismus. Nämlich vom Homomorphismus $\pi\colon G \to G/N$.*

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

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

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 $\operatorname{Kern}\overline{\phi} = \{N\}$ und N ist das neutrale Element in G/N. $\implies \overline{\phi}$ ist injektiv.

□

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 bestehnd aus den Elementen mit Betrag 1. Dann ist der Quotient $\mathbb{C}^*/S^1$ isomorph zu $\mathbb{R}^*_{>0}$. (Wahr)

Begründung: Die Abbildung $\phi\colon \mathbb{C}^* \to R^*_{>0}, \quad z \mapsto |z|$ ist ein surjektiver Homomorphismus. $\operatorname{Kern}\phi = S^1 \overset{\text{1. Isosatz}}{\implies} C^*/S^1 \simeq \mathbb{R}^*_{>0}$

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

Begründung:

$$1 \in H_1 \cup H_2$$
$$a, b \in H_1 \cup H_2 \implies ab \in H_1 \cup H_2$$
$$a^{-1} \in H_1 \cup H2$$

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

Definition 13. *Sei $S \subseteq G$ eine Teilmenge. Dann ist $<s> := \cup_{H \leq G s.d. S \subseteq H} H$ die **von S erzeugte Untergruppe**.*

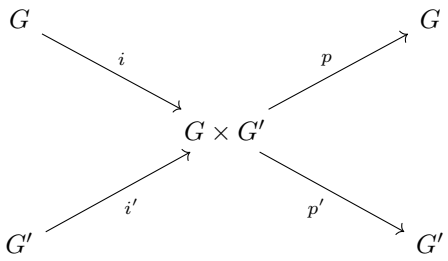
Erinnerung: G, G' Gruppen $\rightsquigarrow G \times G'$ ist Gruppe mit Verknüpfung $(a, a')(b, b') = (ab, a'b')$.

Bsp: Kleinsche Vierergruppe (die "Matratzengruppe").

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

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

Wir haben vier Homomorphismen:



$$i(x) = (x, 1)$$
$$i'(x) = (1, x')$$
$$p(x, x') = x$$
$$p'(x, x') = x'$$

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

$$G \times 1 = \mathrm{Bild}\, i \simeq G$$
$$1 \times G' = \mathrm{Bild}\, i' \simeq G'$$

p und p' sind surjektiv

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

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

Umgekehrt ist jeder Homomorphismus $\Phi\colon H \to G \times G'$ 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.* $\operatorname{Kern}\Phi = \operatorname{Kern}\phi \cup \operatorname{Kern}\phi'$.

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

Satz 11. *(a) Ist $H \cup K = \{1\}$, 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 $H \cup K = \{1\}$ und $HK = G$ so ist $\pi\colon H \times K \to G$ ein Isomorphismus.

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

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

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

$$\Longrightarrow kh = \underbrace{(khk^{-1})}_{\in H} k \in HK$$

$$\Longrightarrow KH \subset HK$$

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

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

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

(ii) $1 \in HK$

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

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

$$\begin{aligned}
&\implies \underbrace{\underbrace{(hkh^{-1})}_{\in k}k^{-1}}_{\in K} = \underbrace{h\underbrace{(kh^{-1}k^{-1})}_{\in H}}_{\in H} \\
&\implies hkh^{-}1k^{-}1 = 1 \\
&\implies hk = kh \\
&\implies \pi(h_1,k_1)\pi(h_2,k_2) = h_1k_1h_2k_2 = h)1h_2k_1k_2 = \pi((h_1,k_1)(h_2,k_2))
\end{aligned}$$

$\implies$ π ist Homomorphismus. Gemäss (a) ist π injetiv. Da $HK = G$ ist π surjektiv $\implies$ π 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 $|G| = G$. Falls G ein Element der Ordnung 6 enthält, so ist $G \simeq C_6$. Ansonsten 3 mögliche Fälle:

(a) Alle $g \in G, g \neq 1$ haben Ordnung 2

(b) Alle $g \in G, g \neq 1$ haben Ordnung 3

(c) Es gibt $g \in G$ von Ordnung 2 und $h \in G$ von Ordnung 3.

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

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

$\pi \colon G \to G/<g>$ Quotient

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

Falls (b), so gilt $g = g^{-1}$ nur wenn $g = 1$.. $\implies$ $G = \{1, g, g^{-1}, h, h^{-1}, \ldots\}$. 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 hate (gh) Ordnung 6. Das haben wir aber ausgeschlossen. Also ist $hg = gh^2$.

Die Relation $gh = h^2g$ definiert die Verknüpfung aug G eindeutig. Jedes Produkt in g und h lässt sich mit dieser Regel in die Form g^ih^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. □

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

$$g\colon \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 1 \end{cases} \qquad h\colon \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 1 \end{cases}$$

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. $A_3 = <h>$

Symmetrie

Isometrien von $\mathbb{R}^n$

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

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

Zwei wichtige Untergruppen:

(1) $\mathcal{T}_n \leq$ Isom($\mathbb{R}^n$: Die Untergruppe der **Translationen**, d.h. Abbildung on der Form $t_a\colon X \mapsto X + a$ für $a \in R^n$. Es gilt $t_at_{a'} = t_{a+a'}$.

(2) $O \leq$ Isom($\mathbb{R}^n$): Die Untergruppe der Isometrien von der Form $d_B\colon X \mapsto BX$ für $B \in O(n)$. Es gilt $d_Bd_{B'} = d_{BB'}$.

Jedes $f \in$ Isom($\mathbb{R}^n$) lässt sich eindeutig schreiben als t_ad_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 $\psi\colon \mathrm{Isom}(R^n) \to O, \psi(t_a d_B) = d_B$.

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

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