Algebra I – Prof. Christian Urech

Mitschrift: Franz Nowak

Herbstsemester 2025

Vorlesung 1

Definition 1. *Eine **Gruppe** ist eine Menge G zusammen mit einer Verknüpfung $*: G \to G,\ (g,h) \to g*h$, 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 $g_1, g_2, \dots, g_n \in G$).*

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 $\overline{g}, g^{-1}$ 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 $\tau^3 = \mathrm{id}$.

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

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 $S^1 := \{c \in \mathbb{C}^* \mid |C| = 1\}$. $S^1 \leq \mathbb{C}^*$. $(\mathbb{C}^* := (\mathbb{C}\backslash\{0\}, \cdot)$
- $B_n(K) := \{A \in GL_n(K) \mid A \text{obere Dreiecksmatrix}\}$. $B_n \leq GL_n(K)$.
- $O_n \leq GL_n(\mathbb{R})$
- 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 $a^n = a^{km+r} = a^{km}a^r = a^r$. $\implies$ $<a> = \{1, a, \dots, a^{m-1}\}$ 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 $<a> = \{\dots, a^{-2}, a^{-1}, 1, a, a^2, \dots\}$ 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* $|<a>|$*, wobei* $<a> = \{1, a, \dots, a^{m-1}\}$ *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* $\phi\colon G \to G'$ *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: $S_n \to \mathbb{Z}/2\mathbb{Z}$,
  $\mathrm{sign}(x) = \begin{cases} 0: & \text{gerade Anzahl von Transpositionen} \\ 1: & \text{ungerade Anzahl von Transpositionen} \end{cases}$
- Fixiere $a \in G$. $\phi\colon \mathbb{Z} \to G$, $\phi(n) = a^n$. ϕ ist injektiv $\Leftrightarrow$ $\mathrm{Ord}(a) = \infty$.
- $H \leq G$, 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 $G = \{1, a, \dots, a^{m-1}\}$, $G' = \{1, b, \dots, b^{m-1}\}$. 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 $\phi\colon G \to G'$ 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 $\forall b \in G$ $bab^{-1} \in N$.*

$\overset{\text{Bem. 9}}{\Longrightarrow}$ $\operatorname{Kern}\phi$ 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 $\phi\colon \mathbb{C}^* \to \mathbb{R}^*_{>0}$, $\qquad \phi(z) \mapsto |z|$. $\qquad$ 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: "$\Rightarrow$": 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 $\phi(b) = \phi(a)\phi(n) = \phi(a)$. $\square$

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 $\phi\colon G \to G'$ ist injektiv* $\Leftrightarrow$ $\operatorname{Kern}\phi = \{1\}$.

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. $a^{-1} + b = 1 \implies a = b$. $\square$

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 $\pi\colon X \to \overline{X}$, $\quad \pi(a) := [a]$. 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 $|{<}a{>}| \bigm| |G|$, 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: $\operatorname{ord} a \bigm| p$, 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 $a \in G$.

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

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.

$\square$

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).

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

$\square$

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 $N :=$ Kern ϕ. 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 $H_1 \cap H_2$ eine Untergruppe von G. (Wahr)

Begründung:

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

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

Definition 13. *Sei $S \subseteq G$ eine Teilmenge. Dann ist $<s> := \bigcap\limits_{\substack{H \leq G \\ s.d. S \subseteq H}} H$ 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:

$$\begin{tikzcd}
G \arrow[dr, "i"] & & G \\
& G \times G' \arrow[ur, "p"] \arrow[dr, "p'"'] & \\
G' \arrow[ur, "i'"] & & G'
\end{tikzcd}$$

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

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.* $\operatorname{Kern}\Phi = \operatorname{Kern}\phi \cap \operatorname{Kern}\phi'$.

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 $H \cap K = \{1\}$, 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 $\pi\colon H \times K \to G$ ein Isomorphismus.

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

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

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

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

$$\implies KH \subseteq HK$$

Analog: $HK \subseteq KH$. $\implies KH = HK$. 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 $h \in H, k \in K$

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

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

$\square$

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 $gh = h^2 g$ definiert die Verknüpfung aug 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*

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

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

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

Jedes $f \in \mathrm{Isom}(\mathbb{R}^n)$ 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 $\psi\colon \operatorname{Isom}(R^n) \to O, \psi(t_a d_B) = d_B$.

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

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

Vorlesung 6

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

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

$\mathcal{T}_n \trianglelefteq \operatorname{Isom}(\mathbb{R}^n)$ Translationen

Orientierung

Falls $n = 2$:

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

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

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

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

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 Isom*$(\mathbb{R}^n)$ *der Elemente, die einen Punkt* $p \in \mathbb{R}^n$ *fixieren, ist die Konjugierte Untergruppte* $O' = t_p O t_p^{-1} \leq \mathit{Isom}(\mathbb{R}^n)$

Beweis:

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

□

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

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

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

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

$$\begin{aligned} &\implies f_j(p) = B_j(\frac{1}{m}(q_1 + \cdots + q_m)) + a_j \\ &= \frac{1}{m}(B_j q_1 + \cdots + B_j q_m + m a_j) \\ &= \frac{1}{m}((B_j q_1 + a_j) + \cdots + (B_j q_m + a_j)) \\ &= \frac{1}{m}(f_j(q_1) + \cdots + f_j(q_m)) \\ &= \frac{1}{m}(f_j f_1(q) + \cdots + f_j f_m(q)) \\ &\overset{(*)}{=} \frac{1}{m}(q_1 + \cdots + q_m) = p \end{aligned}$$

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

Korollar 7. *Sei $G \leq Isom(\mathbb{R}^n)$. 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 $G \leq t_a O t_a^{-1}$

$\implies t_a^{-1} G t_a \leq O$. □

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: $<d_\theta> = G$.

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

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

$$\begin{aligned}
&\implies \beta = 0 \\
&\implies d_\alpha (d_\theta^{-1})^n = 1 \\
&\implies d_\alpha = (d_\theta)^n \in <d_\theta>
\end{aligned}$$

Sei $n \in \mathcal{N}$ 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 $\phi\colon G \to \{\pm 1\}$ gegeben durch Det. $\overset{1.Fall}{\implies}$ Kern ϕ ist zyklisch erzeugt von Drehung $\implies G = \text{Kern}\,\phi + S\,\text{Kern}\,\phi$ mit S Spiegelung. □

Vorlesung 7

$|D_3| = 6$ und D_3 ist nicht zyklisch $\implies D_3 \simeq S_3$

Die Diedergruppe D_n von Ordnung $2n$ enthält die Symmetrien vom n-gon.

$D_n \subseteq \text{Isom}(\mathbb{R}^2)$ bestehend aus allen $g \in \text{Isom}(R^2)$ s.d. $gP = P$.

Bemerkung 20. *Sei* x *eine Drehung um den Winkel* $2\pi/n \implies ord\, x = n$

Sei y *eine Spiegelung* $\implies ord\, y = 2$. *Dann ist* xy *wieder eine Spiegelung.*

$$\begin{aligned}
&\implies 1 = (xy)^2 = xyxy \\
&\implies xy = yx^{-1} = yx^{n-1}
\end{aligned}$$

Dies definiert alle Relationen in D_n.

Satz 15. D_n *ist erzeugt von zwei Elementen* x, y, *die die Relationen* $x^n = 1, y^2 = 1, xy = yx^{-1}$ *erfüllen, d.h.*

$$D_n = \{1, x, \ldots, x^{n-1}, y, xy, \ldots, x^{n-1}y\}$$

Wir überspringen die unendlichen diskreten Untergruppen der **Gitter** (siehe Artin).

Gruppenoperationen

Gruppe der Gruppenautomorphismen.

Definition 16. *Sei G eine Gruppe und X eine Menge. Eine **(Links-)Operation** oder **Aktion** oder **Wirkung** von G auf X ist eine Abbildung*

$$G \times X \to X \quad (g, x) \mapsto gx$$

so dass

(a) $1x = x \quad \forall x \in X$

(b) $(gg')x = g(g(g'x) \quad \forall g \in G, x \in X$

*X heisst **G-Menge**. Wir schreiben $G \curvearrowright X$ für "G operiert auf X.*

Für jedes $g \in G$ erhalten wir eine Abbildung

$$m_g \colon X \to X \quad m_g(x) = gx$$

m_g heisst **Linksmultiplikation** mit g.

Bemerkung 21. *m_g ist bijektiv und $(m_g)^{-1} = m_{g^{-1}}$.*

Beweis:

$$\begin{aligned} m_{g^{-1}}(m_g(x)) &= g^{-1}(gx) \\ &= g^{-1}gx = 1x = x \end{aligned}$$

Analog: $m_g(m_{g^{-1}}(x)) = x$ □

Definition 17. *Für zwei $x \in X$ ist die **Bahn** oder das **Orbit** von x:*

$$B_x := \{y \in X \mid y = gx \text{ für ein } g \in G\} = Gx$$

Bemerkung 22. *Für $x, y \in X$ definieren wir $x \sim y$ falls $y = gx$ für ein $g \in G$. Dann ist $\sim$ eine Äquivalenzrelation (kleine Übung) und die Bahnen sind genau die Äquivalenzklassen von $\sim$.*

Beispiel 6.

- *Isom$(\mathbb{R}^2)$ operiert auf R^2. (Hat nur einen Orbit)*
- *Sei $D = \{\text{Dreiecke in } \mathbb{R}^2\}$ Isom$(\mathbb{R}^2)$ operiert auf D.*
- *Zwei Dreiecke Δ, Δ' sind **kongruent**, falls es ein $g \in$ Isom$(\mathbb{R}^2)$ gibt, so dass $g\Delta = \Delta'$. Die Bahn B_Δ ist die Menge aller zu Δ kongruenten Dreiecke.*

Definition 18. *Eine Operation $G \curvearrowright X$ heisst* ***transitiv****, falls es nur eine Bahn gibt. D.h.*

$$\forall x, x' \in X \ \exists g \in G \ s.d. \ gx = x'$$

Definition 19. *Der* ***Stabilisator*** *von $x \in X$ ist $G_x := \{g \in G \mid gx = x\}$*

Bemerkung 23. *$G_x \leq G$ ist eine Untergruppe.*

Bemerkung 24. *Für $g, h \in G$ gilt:*

$$\begin{aligned} gx = hx &\Leftrightarrow h^{-1}gx = x \\ &\Leftrightarrow h^{-1}g \in G_x \end{aligned}$$

Beispiel 7.

- *$Isom(\mathbb{R}^2) \curvearrowright \mathbb{R}^2$ Der Stabilisator von O ist die Untergruppe $O \leq Isom(\mathbb{R}^2)$. $O \simeq O(2)$.*
- *$Isom(R^2) \curvearrowright D$. Sei Δ ein gleichseitiges Dreieck. Dann ist der Stabilisator von Δ isomorph zu der Diedergruppe D_3 von Ordnung 6.*

Operation auf Nebenklassen

Beobachtung: $H \leq G \rightsquigarrow G$ operiert auf G/H.

Für $K \in G/H$ definieren wir

$$gK := \{gk \mid k \in K\}$$

Das heisst, falls $K = aH$, so ist $gK = gaH$.

Bemerkung 25.

- *Diese Operation ist transitiv, denn $B_H = G/H$.*
- *Sei $g \in G$, dann gilt $gH = H \Leftrightarrow g \in H$. D.h., der Stabilisator von H ist H: $D_H = H$.*

Beispiel 8. *D_3, erzeugt von x, y und $x^3 = y^2 = 1$ sowie $yx = x^2y$. Sei $H = <y> = \{1, y\}$. Nebenklassen:*

$$\begin{aligned} K_1 &= \{1, y\} \\ K_2 &= \{x, xy\} \\ K_3 &= \{x^2, x^2y\} \\ G/H &= \{K_1, K_2, K_3\} \end{aligned}$$

Beobachtung: $m_x \colon G/H \to G/H \quad K_i \mapsto xK_i, \quad i \in \{1, 2, 3\}$

$$m_x \colon \begin{cases} K_1 \mapsto K_2 \\ K_2 \mapsto K_3 \\ K_3 \mapsto K_1 \end{cases} \qquad m_y \colon \begin{cases} K_1 \mapsto K_1 \\ K_2 \mapsto K_3 \\ K_3 \mapsto K_2 \end{cases}$$

$\rightsquigarrow$ *Wir erhalten einen Isomorphismus $G \xrightarrow{\sim} Sym(G/H) \quad g \mapsto m_g$*

Satz 16. *Sei X eine $G-Menge$ und $x \in X$. Sei $H = G_x \leq G$. Dann ist die Abbildung*

$$\phi\colon G/H \to B_x \quad aH \mapsto ax$$

eine Bijektion und $\forall K \in G/H$ und $\forall g \in G$ gilt $\phi(gK) = g\phi(K)$.

Beweis:

- ϕ ist wohldefiniert. Seien $a, b \in G$ s.d. $aH = bH \Leftrightarrow b = ah$ für ein $h \in H \implies bx = a\underbrace{hx}_{x} = ax$.
- ϕ ist surjektiv: klar, da B_x genau aus den Elementen der Form ax besteht, $a \in G$.
- ϕ ist inketiv: falls $ax = bx \implies x = a^{-1}bx \implies a^{-1}b \in H \implies aH = bH$.
- Die letzte Aussage folgt aus der Definition von ϕ.

$\square$

Bemerkung 26. *Sei $x \in X$ und $y = ax$ für $a \in G$. Dann*

(a) $\{g \in G \mid gx = y\} = aG_x$

(b) $G_y = aG + xa^{-1}$

Beweis: (a) $gx = y = ax \Leftrightarrow a^{-1}g \in G_x \Leftrightarrow g \in aG_x$

(b)

$$\begin{aligned} gy = y &\Leftrightarrow gax = ax \\ &\Leftrightarrow a^{-1}yax = x \\ &\Leftrightarrow a^{-1}ya \in G_x \\ &\Leftrightarrow g \in aG_x a^{-1} \end{aligned}$$

$\square$

Korollar 8 (Bahnformel)**.** $|G| = |G_x| \cdot |B_x|$

(Ordnung G)=(Ordnung des Stabilisators)·(Ordnung der Bahn)

Beweis: Wir haben $|G| = |G_x| \cdot [G : G_x]$. Die Bahnformel folgt nun direkt aus Satz 16. $\square$

Bemerkung 27.

- *Es folgt direkt, dass $|Bx| = [G : G_x]$. Die Länge jeder Bahn muss die Gruppenordnung teilen.*
- *Falls X endlich ist: Seien $B_1, \ldots, B_k$ die Bahnen. Dann ist*

$$|X| = |B_1| + \cdots + |B_k|$$

.

Beispiel: Dodekaeder

$D \subseteq R^3$ Dodekaeder. Sei $G \leq \operatorname{Isom} \mathbb{R}^3$ die orientierungserhaltenden Symmetrien g, so dass $gD = D$. D.h., die Elemente in G sind gegeben durch Matrizen in $SO(3)$. Diese sind Drehungen um Achsen. Was ist $|G|^2$?

G operiert auf den Seiten von D. Sei S eine Seite. G_S besteht aus den Drehungen um Vielfache von $2\pi/5$.

$\implies |G_S| = 5$.

G operiert transitiv auf den Seiten. Es gibt 12 Seiten.

$\implies |G| = |G_S| \cdot 12 = 60$.

G_S fixiert zwei Seiten $\rightsquigarrow$ zwei Bahnen von Länge 1 + zwei von Länge 5.

$\rightsquigarrow 1 + 1 + 5 + 5 = 12$

Definition 20. *G heisst die* ***Ikosaeder Gruppe****.*

Vorlesung 8

Satz 17. *Sei G eine Gruppe, $H \leq G, K \leq G$ Untergruppen. Dann gilt $[H : H \cap K] \leq [G : K]$.*

Beweis: Sei $X = G/K$ und sei $x = K \in X$. D.h. $|X| = [G : K]$ und $G \curvearrowright X$. Dann ist $G_x = K$. Betrachte die Operation $H \curvearrowright X$. Dann ist $H_x = H \cap K$. Sei B die Bahn von x unter H. Dann ist $|B| \leq |X|$. Gemäss Bahnformel ist $|B| = [H : H \cap K] \implies [H : H \cap K] \leq |X| = [G : K]$. $\square$

Sei X eine Menge und G eine Gruppe. Jede Operation $G \curvearrowright X$ liefert einen Homomorphismus $\phi \colon G \to \operatorname{Sym}(X) \quad \phi(g) := m_g$.

ϕ ist tatsächlich ein Homomorphismus:

$\phi(gh) = m_{gh}$

$\phi(g)\phi(h) = m_g m_h$ und $m_g h(x) = (gh)x = g(hx) = m_g(m_h(x)) \quad \forall x \in X$.

d.h. $\phi(gh) = \phi(g)\phi(h)$.

Umgekehrt definiert jeder Homomorphismus $\phi \colon G \to \operatorname{Sym}(X)$ eine Operation $G \curvearrowright X$ durch $gx := \phi(g)(x)$.

Mit dieser Beobachtung zeigt man:

Satz 18. *Es gibt eine Bijektion*

$$\{\textit{Operationen } G \curvearrowright X\} \leftrightarrow \{\textit{Homomorphismen } G \to \textit{Sym}(X)\}$$

$$G \curvearrowright X \mapsto \phi \colon G \to \textit{Sym}(X) \quad g \mapsto m_g$$

Definition 21. *Eine Operation $G \curvearrowright X$ heisst **treu**, falls der entsprechende Homomorphismus $\phi\colon G \to Sym(X)$ injektiv ist. D.h., falls für ein $g \in G$ gilt $gx = x \quad \forall x$, dann ist $g = 1$.*

Satz 19. *Sei $\mathbb{F}_2$ der Körper mit 2 Elementen. Dann ist $G = GL_2(\mathbb{F}_2)$ isomorph zu S_3.*

Beweis: Sei $V = \mathbb{F}_2^2$, $V = \{0, e_1, e_2, e_1 + e_2\}$.

$G \curvearrowright V$ durch Linksmultiplikation. 0 ist Fixpunkt. $\{e_1, e_2, e_1 + e_2\}$ bildet eine weitere Bahn. Das gibt einen Homomorphismus $\phi\colon G \to S_3$. Für $P \in GL_2(\mathbb{F}_2)$ s.d. $Pe_1 = e_1$ und $Pe_2 = e_2 \Leftrightarrow P = 1$, d.h. Diese Operation ist treu und somit effektiv. G ist nicht abelsch $\implies |G| \geq 6$. $\implies \phi$ ist ein Isomorphismus. □

Satz 20. *Für $g \in S_3$ sei $k_g : S_3 \to S_3 \quad k_g(a) = gag^{-1}$ ist ein Automorphismus von S_3. Dann ist $f\colon S^3 \to Aut(S_3) \quad f(g) = k_g$ ein Isomorphismus.*[1]

Beweis:

- f ist Homomorphismus:

$$\begin{aligned} k_{gh}(x) &= (gh)x(gh)^{-1} \\ &= ghxh^{-1}g^{-1} \\ & k_g k_h(x) \end{aligned}$$

  D.h. $k_{gh} - k_g k_h$. $\implies f(gh) = f(g)f(h)$.

- f ist injektiv: Falls $gag^{-1} = a \quad \forall a \in S_3$ so ist $g = 1$ (kleine Übung).

- f ist surjektiv: Beobachtung: $\mathrm{Aut}(S_3)$ operiert auf die Menge der Elemente von Ordnung 2 $\{y, xy, x^2y\}$:

$$y\colon \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 1 \\ 3 \mapsto 3 \end{cases} \qquad x\colon \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 1 \end{cases}$$

- Die Operation $\mathrm{Aut}(S_3) \curvearrowright \{y, xy, x^2y\}$ ist treu: Falls $\alpha \in \mathrm{Aut}(S_3)$ s.d. $\alpha(y) = y$ und $\alpha(xy) = xy$, so ist auch $\alpha(x) = \alpha(xyy0 = xyy = x$. Da x und y S_3 erzeugen, ist $\alpha = id$.

  D.h., die Abbildung $\mathrm{Aut}(S_3) \to \mathrm{Sym}(\{y, xy, x^2y\})$ ist injektiv

$$\begin{aligned} &\implies |\,\mathrm{Aut}(S_3)| \leq 6 \\ &\implies |\,\mathrm{Aut}(S_3)| = 6 \\ &\implies S_3 \to \mathrm{Aut}(S_3) \text{ ist bikektiv, d.h. ein Isomorphismus.} \end{aligned}$$

□

[1] Gilt für fast alle symmetrischen Gruppen .

Satz 21. *Die endlichen Untergruppen von $SO(3)$ sind die folgenden:*

- C_k*: Die zyklische Gruppe der Drehungen um Vielfache von $2\pi/k$ um eine Achse.*
- D_k*: Die Diedergruppe, also die Symmetrien eines regelmässigen k-Ecks in einer Ebene gegeben durch räumliche Drehungen.*
- T*: Die Tetraedergruppe, also die 12 Drehungen, die ein Tetraedron erhalten.*
- W*: Die Würfelgruppe, also die 24 Drehungen, die den Würfel erhalten.*
- I*: Ikosaedergruppe, also die 60 Drehungen, die ein Dodekaeder/Ikosaeder erhalten.*

Beweis: Siehe Artin. □

Vorlesung 9

Mehr über Gruppen

Eine Gruppe operiert auf sich selbst durch Linksmultiplikation:

$$G \times G \to G \qquad (g, x) \mapsto gx$$

. Diese Operation ist transitiv. Sei $x \in G$, dann ist der Stabilisator $G_x = \{1\}$. Insbesondere ist der Homomorphismus injektiv:

$$G \to \mathrm{Sym}(G) \qquad g \mapsto m_g$$

$\implies$ die Operation ist treu.

Satz 22 (Cayley)**.** *Sei G eine endliche Gruppe. Dann ist G isomorph zu einer Untergruppe von S_n, wobei $n = |G|$.*

Beweis: Der Homomorphismus

$$\phi\colon G \to \mathrm{Sym}(G) \simeq S_n \qquad g \mapsto m_g$$

ist injektiv. $\implies$ G ist isomorph zu Bild $\phi \leq \mathrm{Sym}(G) \simeq S_n$. □

G operiert auch auf sich selbst durch Konjugation:

$$G \times G \to G \qquad (g, x) \mapsto gxg^{-1}$$

Sei $x \in G$.

Definition 22. *Der Stabilisator von x bezüglich Konjugation heisst **Zentralisator**. Wir schreiben $Z(x)$ mit*

$$\begin{aligned} Z(x) &= \{g \in G \mid gxg^{-1} = x\} \\ &= \{g \in G \mid gx = xg\} \end{aligned}$$

*Die Bahn von x unter Konjugation heisst **Konjugiertenklasse** oder **Konjugationsklasse** von x in G. Wir schreiben $K(x)$ mit*

$$K(x) = \{x' \in G \mid x' = gxg^{-1} \text{ für ein } g \in G\}$$

Bemerkung 28.

- *Aus der Bahnformel folgt $|G| = |K(x)||Z(x)|$.*
- $|K(1)| = 1$.

Falls $|G|$ endlich ist, so gilt die sog. **Klassengleichung**:

$$|G| = \sum_{K \text{ Konj. klasse}} |K| = |K_1| + \cdots + |K_l|$$

Bemerkung 29. *Die Zahlen auf der rechten Seite sind Teiler von $|G|$ und mindestens eine davon ist 1.*

Beispiel 9. *Konjugationsklassen in D_3. Erzugende: x (Drehung) und y (Spiegelung). $\{1\}, \{x, x^2\}, \{y, xy, x^y\}$. (Kleine Übung). $\xrightarrow{\textit{Klassengleichung}} |G| = 1 + 2 + 3$.*

Definition 23. *Das **Zentrum** Z einer Gruppe G ist der Normalteiler*

$$Z = \{x \in G \mid gx = xg \quad \forall g \in G\}$$

Bemerkung 30.

- $x \in Z \Leftrightarrow Z(x) = G$
- $x \in Z \Leftrightarrow |K(x)| = 1$

Definition 24. *Sei p eine Primzahl. Eine **p-Gruppe** ist eine Gruppe G, sodass $|G| = p^e$ für ein $e \geq 1$.*

Beispiel 10.

- *$C_p, C_{p^2}, C_{p^3}, \ldots$ sind p-Gruppen*
- $C_p \times C_p \times \cdots \times C_p$
- *$U_3(\mathbb{F}_p) = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{F}_p \right\} \leq GL_3(\mathbb{F}_p)$ ist eine p-Gruppe von Ordnung p^3.*

Satz 23. *Das Zentrum von einer p-Gruppe ist strikt grösser als die triviale Gruppe* $\{1\}$.

Beweis: Klassengleichung:

$$|G| = p^e = \sum_{KKonj.klassen} |K| = 1 + \sum_{KKonj.klassen} |K|$$

alle $|K|$ sind Teiler von p^e.

$\implies$ es gibt weitere Konjugationsklassen mit nur einem Element.

$\implies$ es gibt $x \in G \backslash \{1\}$ sodass $x \in Z$. $\square$

Beispiel 11. *Das Zentrum von* $U_3(\mathbb{F}_p)$ *ist die Untergruppe*

$$\left\{ \begin{pmatrix} 1 & 0 & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \mid c \in \mathbb{F}_p \right\} \simeq \mathbb{F}_p$$

Satz 24. *Sei* G *eine p-Gruppe und* X *eine endliche Menge, sodass* $p \nmid |X|$. *Falls* $G \curvearrowright X$, *dann gibt es ein* $x \in X$ *sodass* $gx = x \quad \forall g \in G$.

Beweis: Seien $B_1, \ldots, B_k$ die Bahnen von G. Dann ist $|X| = |B_1| + \ldots + |B_k|$. Gemäss Bahnformel gilt $|B_i| \big| |G_i| \quad \forall i = 1, \ldots, k$. Da $p \nmid |X|$, ist $|B_i| = 1$ für mindestens ein i. $\square$

Satz 25. *Jede Gruppe* G *der Ordnung* p^2 *ist abelsch.*

Beweis: Nehmen wir an, dass G nicht abelsch ist. Dann gibt es ein $x \in G$, sodass $x \notin Z$ und somit $Z \subsetneq Z(x)$. Wir wissen, dass $|Z| \geq p$. Da $|Z(x)| \big| |G|$, d.h. $|Z(x)| = p^2 \implies Z(x) = G$, damit folgt aber, dass $x \in Z \quad ↯$.

$\implies G$ ist abelsch. $\square$

Bemerkung 31. *Es gibt nichtabelsche Gruppen von Ordnung* p^3, *z.B.* $|U_3(\mathbb{F}_p)| = p^3$ *und* $|D_4| = 8 = 2^3$.

Korollar 9. *Sei* G *eine Gruppe mit* p^2 *Elementen. Dann ist entweder* $G \simeq C_{p^2}$ *oder* $G \simeq C_p \times C_p$.

Beweis: Jedes Element in G hat Ordnung $1, p$ oder p^2.

1. Fall: G enthält ein Element von Ordnung p^2. $\implies G$ ist zyklisch.

2. Fall: Alle Elemente in $G\backslash\{1\}$ haben Ordnung p. Sei $x \in G\backslash\{1\}$ und $H_1 = <x>$. Sei $y \in G\backslash H$, und $H_2 = <y>$ Dann ist $H_1 \cap H_2 \lneq H_2$ und somit $H_1 \cap H_2 = \{1\}$.

G ist abelsch $\implies$ H_1 und H_2 sind Normalteiler. $\implies$ $H_1 H_2 \leq G$.

Da $H_1 \lneq H_1 H_2$ ist, ist $|H_1 H_2| = p^2 \implies H_1 H_2 = G$. Wir haben gesehen, dass daraus folgt:

$$G \simeq H_1 \times H_2$$

□

Ikosaedergruppe

Erinnerung: $I \leq SO(3)$ die Untergruppe der Drehungen, die das Dodekaeder $D \subseteq R^3$ erhalten.

Gesehen: $|I| = 60$

- Identität (Ord. 1)
- Drehungen, die Eckpunkte von D fixieren: Es gibt 20 Ecken, also 10 Drehachsen $\implies 2 \cdot 10 = 20$ solche Drehungen $\neq$ id. (Ord. 3) Sind alle konjugiert zueinander (s. unten).
- Drehungen um Mittelpunkte von Seiten. Es gibt 12 Flächen, also 6 mögliche Drehachsen. $\implies 6{\cdot}4 = 24$ solche Drehungen $\neq$ id. (Ord. 5)
- Drehungen um Mittelpunkte von Kanten. Es gibt 30 Kanten, also 15 mögliche Drehachsen. $\implies$ 15 solche Drehungen. (Ord. 2)

$60 = 1 + 20 + 24 + 15 \rightsquigarrow$ Das sind alle möglichen Elemente in I.

Was sind die Konjugationsklassen?

Bemerkung 32. *Seien $g, x \in G$, so ist $ord(gxg^{-1}) = ord(x)$.*

- Die Identität bildet eine Konjugationsklasse.
- Alle Rotationen um $2\pi/3$ (im Gegenuhrzeigersinn) um Achsen durch Ecken sind konjugiert.
- Alle Rotationen um $2\pi/5$ um Achsen durch Seiten sind konjugiert zueinander und zu den Rotationen um den Winkel $-2\pi/5 = 8\pi/5$.
- Alle Rotationen um Achsen durch Seiten um $4\pi/5$ und um $-4\pi/5$=$6\pi/5$. sind konjugiert.
- Alle Rotationen um Achsen durch Kanten um den Winkel π sind konjugiert.

$\implies$ 5 Konjugationsklassen. Klassengleichung: $60 = 1 + 20 + 12 + 12 + 15$.

Vorlesung 10

Einfache Gruppen

Definition 25. *Eine Gruppe G ist* ***einfach****, falls $\{1\}$ und G die einzigen Normalteiler von G sind.*

Bemerkung 33. *G ist einfach $\Leftrightarrow$ für alle surjektiven Homomorphismen $\phi\colon G \to G'$ gilt $G = G'$ oder $G' = \{1\}$.*

Bemerkung 34. *Einfache Gruppen sind die "Bausteine" von Gruppen.*

Beispiel 12. *C_p für p prim.*

Satz 26. *Die Ikosaedergruppe I ist einfach.*

Beweis: Klassengleichung von I:

$$60 = 1 + 15 + 20 + 12 + 12$$

Sei $N \trianglelefteq G \implies gNg^{-1} = N \quad \forall g \in G$.

$\implies$ falls $x \in N$, so ist auch die Konjugationsklasse $K(x) \subseteq N$. Das heisst $N = \bigcup\limits_{x_i \in N} K(x_i)$. $|N|$ teilt 60.

Es folgt:

$$\begin{aligned} N &= 1 + \text{ Terme aus } \{15, 20, 12, 12\} \\ &\implies |N| = 1 \text{ oder } |N| = 60 \\ &\implies N = \{1\} \text{ oder } |N| = I \\ &\implies I \text{ ist einfach.} \end{aligned}$$

$\square$

Satz 27. *I ist isomorph zu A_5.*

Beweis: Wir suchen eine Menge mit 5 Elementen, auf welche I operiert. Es gibt 5 Möglichkeiten, einen Würfel in ein Dodekaeder D einzubetten, sodass die Ecken auch Ecken von D sind und die Kanten in den Seiten von D sind. Jede Seite von D enthält genau eine Würfelkante. Die Wahl von einer solchen Kante definiert die Einbettung.

$\rightsquigarrow$ 5 mögliche Einbettungen vom Würfel. I operiert darauf.

$\rightsquigarrow \phi\colon I \to S_5$.

$\implies$ Kern $\phi = I$ oder Kern $\phi = \{I\}$ einfach.

Kern $\phi = I$ ist nicht möglich, da die Operation nicht trivial ist.

$\implies$ Kern $\phi = \{1\}$ und ϕ injektiv.

Betrachte $I \xrightarrow{\phi} S_5 \xrightarrow{\text{sign}} \{\pm 1\}$.

Dann ist $\operatorname{Kern} \text{sign} \phi = I$ da I keine Normalteiler von Ordnung 30 enthält.

$\implies \phi(I) \subseteq A_5$.

Da $|I| = |A_5| = 60$, folgt: $\phi\colon I \to A_5$ ist ein Isomorphismus. $\square$

Korollar 10. $A + 5$ *ist einfach.*[2]

Operationen auf Teilmengen

Falls $G \curvearrowright X$, so operiert G auch auf die Menge der Teilmengen $\mathcal{P}(X)$ von X.

$G \times \mathcal{P}(X) \to \mathcal{P}(X)$ für $U \subseteq X,\ gU = \{gu \mid u \in U\} \subseteq X$.

Dies definiert eine Gruppenoperation.

Bemerkung 35. $|gU| = |U|$, *das heisst, wir können auch auf Teilmengen von gegebener Grösse beschränken.*

Sei $U \subseteq X$. Der Stabilisator G_U von U besteht aus den $g \in G$ sodass $gU = U$, das heisst, $gu \in U\ \forall u \in U$.

[2] Tatsächlich sind alle alternierenden Gruppen ausser A_4 einfach.