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 $\tau^3 = \mathrm{id}$.

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

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

Satz 3.

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

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

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

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

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

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

□

Bemerkung 8. *Zwei zuklische Gruppen gleicher Ordnung sind immer isomorph.*

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

Falls $|G| = |G'|$ endlich ist, so ist $G = \{1, a, \dots, a^{m-1}\}$, $G' = \{1, b, \dots, b^{m-1}\}$. 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*

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

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

$\overset{\text{Bem. 9}}{\implies}$ $\operatorname{Kern}\phi$ 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 $|<a>| \;\big|\; |G|$, 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.

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

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

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

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

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

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

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

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

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

$$\implies aH \subseteq Ha$$

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. $\square$

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. $\operatorname{Kern} \phi = S^1 \overset{\text{1. Isosatz}}{\Longrightarrow} C^*/S^1 \simeq \mathbb{R}^*_{>0}$

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:

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

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:

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

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

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

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

p und p' sind surjektiv

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

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.

□

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. $\square$

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. $A_3 = \langle h \rangle$

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:

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

□

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 $f_j(X) = B_jX + a_j$.

$$\begin{aligned}&\implies f_j(p) = B_j(\frac{1}{m}(q_1 + \cdots + q_m)) + a_j\\&= \frac{1}{m}(B_jq_1 + \cdots + B_jq_m + ma_j)\\&= \frac{1}{m}((B_jq_1 + a_j) + \cdots + (B_jq_m + a_j))\\&= \frac{1}{m}(f_j(q_1) + \cdots + f_j(q_m))\\&= \frac{1}{m}(f_jf_1(q) + \cdots + f_jf_m(q))\\&\overset{(*)}{=} \frac{1}{m}(q_1 + \cdots + q_m) = p\end{aligned}$$

$(*): \; \{f_1, \ldots, f_m\} = \{f_jf_1, \ldots, f_jf_m\}$ □

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

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

$\implies t_a^{-1}Gt_a \leq O$. □

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 $D = \{$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 $H = \langle y \rangle = \{1, y\}$. 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)

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

$\square$

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. $\square$

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

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

$\square$

[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:

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

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

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).* $\xrightarrow{\text{Klassengleichung}} |G| = 1 + 2 + 3$.

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.

- *$C_p, C_{p^2}, C_{p^3}, \dots$ 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:

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

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 $x \in Z \quad \lightning$.

$\implies$ 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.*

Bemerkung 35. *$\{1\}$ ist nicht einfach.*

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.

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

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

$\operatorname{Kern}\phi = I$ 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 Kern 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 36. *$|gU| = |U|$, 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, $gu \in U\ \forall u \in U$.

Vorlesung 11

Gesehen: Wenn $G \curvearrowright X$, dann operiert G auch auf die Menge der Teilmengen von X. Für $U \subseteq X$ ist der Stabilisator $\mathrm{Stab}(U) = G_U = \{g \in G \mid gU = U\}$

Satz 28. *$G \curvearrowright X$. Sei $U \subseteq X$ und $H \leq G$. Dann ist $H \leq Stab(U) \Leftrightarrow U$ ist die Vereinigung von allen H-Bahnen.*

Beweis: H stabilisiert U

$\Leftrightarrow$ die H-Bahn B_x ist in U enthalten $\forall x \in U$

$\Leftrightarrow U = \bigcup\limits_{x \in U} B_x$. $\square$

$G \curvearrowright \{$Teilmengen von $G\}$ durch Linksmultiplikation.

Satz 29. *Sei $U \subseteq G$. Dann ist $|\,Stab(U)|$ ein Teiler von $|U|$.*

Satz 30. *Sei $H = Stab(U)$. Dann operiert H auf U. $\implies$ U ist eine Vereinigung von H-Bahnen. Diese sind von der Form $H_g, g \in U \implies U$ ist eine Vereinigung von Rechtsnebenklassen von $H \implies |U|$ ist Vielfaches von H.*

$G \curvearrowright \{$Teilmengen von $G\}$ durch Konjugation.

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

Definition 26. *Sei $H \leq G$. Dann ist die Bahn von H unter dieser Operation die Menge der zu H konjugierten Untergruppen. Das heisst*

$$B_H = \{gHg^{-1} \mid g \in G\}$$

Der Stabilisator von H unter dieser Operation heisst ***Normalisator von*** *H.*

$$N(H) = \{g \in G \mid gHg^{-1} = H\}$$

Bemerkung 37.

- $H \leq N(H)$
- $N(H) = G \Leftrightarrow H \trianglelefteq G$ *ist Normalteiler.*

Bahnformel: $|G| = |N(H)| \cdot |\{\text{zu } H \text{ konjugierte Untergruppen}\}|$.

Die Sylow Sätze

Gesehen: Sei G Gruppe, $H \leq G \implies |H| \big| |G|$.

Clicker-Frage: Sei G eine Gruppe und d ein Teiler von G. Folgt daraus dass eine Untergruppe $H \leq G$ existiert, mit $|H| = d$? **Nein.**

Beispiel: $|I|$=60, aber I hat keine Untergruppe von Ordnung 30.

Behauptung 2. *$H \leq G, [G : H] = 2$, dann ist H normal.*

Beweis: Sei $g \in G \backslash H$.

$G = H \cup gH$ und $G = H \cup Hg$ d.h.

$gH = G \backslash H = Hg$

$\implies$ Links- und Rechtsnebenklassen stimmen überein. $\implies H \trianglelefteq G$. □

Sei p prim und G eine endliche Gruppe, s.d. $|G| = n = p^e m$, wobei $e \geq 0, p \nmid m$.

Satz 31 (Sylow I)**.** *Es gibt eine Untergruppe $H \leq G$ sodass $|H| = p^e$.*

Definition 27. *Eine solche Untergruppe H heisst* ***p-Sylowuntergruppe*** *("p-Sylow").*

Korollar 11. *Wenn $p \bigm| |G|$, dann existiert ein $x \in G$ von Ordnung p.*

Beweis: Gemäss Sylow I: $\exists H \leq G$, s.d. $|H| = p^e$

Sei $y \in H \backslash \{1\}$.

Dann hat y Ordnung p^r für $1 \leq r \leq e$. $\implies y^{p^{r-1}}$ hat Ordnung p. □

Satz 32 (Sylow II)**.** *Sei G eine endliche Gruppe.*

(a) Alle p-Sylowuntergruppen in G sind konjugiert zueinander. D.h. falls $H, H' \leq G$ p-Sylow sind, so $\exists g \in G$, s.d. $gHg^{-1} = H'$.

(b) Sei $K \leq G$ eine Untergruppe, sodass $|K| = p^d$, so ist K in einer p-Sylow von G enthalten.

Satz 33 (Sylow III)**.** *Sei s die Anzahl der p-Sylows in G. Dann gilt $s \big| m$ und $s \equiv 1 \mod p$. ($|G| = p^e m$)*

Anwendungen von Sylowsätzen

Satz 34. *Jede Gruppe der Ordnung 15 ist zyklisch.*

Beweis: Sei G eine Gruppe, sodass $|G| = 15 = 5 \cdot 3$.

$\underset{\text{Sylow III}}{\Longrightarrow}$ Die Anzahl der 5-Sylows ist Teiler von 3 und $\equiv 1 \mod 5$.

$\Longrightarrow$ Es gibt nur eine Untergruppe $H \leq G$ mit $|H| = 5$. Insbesondere ist $gHg^{-1} = H \quad \forall g \in G$. D.h. $H \trianglelefteq G$.

Die Anzahl von 3-Sylows ist Teiler von 5 und $\equiv 1 \mod 3$.

$\Longrightarrow$ Es gibt eine eindeutige Untergruppe $K \leq G$ von Ordnung 3.

Insbesondere ist K normal.

$H \cap K = \{1\}$

$HK \leq G$ ist eine Untergruppe. Da $|HK| > 5$, gilt $HK = G$.

$\underset{Satz}{\Longrightarrow}$ $G \simeq H \times K$. Wir haben $H \simeq C_5, K \simeq C_3$ (Gruppen von Ordnung p sind zyklisch).

$\Longrightarrow$ $G \simeq C_5 \times C_3 \simeq C_15$. $\square$

Satz 35. *Sei G eine Gruppe, sodass $|G| = 10$. Dann ist $G \simeq C_5 \times C_2 \simeq C_10$ oder $G \simeq D_5$.*

Beweis: Die Anzahl der 5-Sylows teilt 2 und ist $1 \mod 5$.

$\Longrightarrow$ Es gibt nur eine 5-Sylow $K \leq G$ und diese ist somit normal.

$K \simeq C_5$. Sei $x \in K$ sodass $K = <x>$.

Sei H eine 2-Sylow. Sei $y \in H$, sodass $H = <y>$. Da K normal ist, ist $yxy^{-1} = x^r$ für $1 \leq r \leq 4$ d.h. $yx = x^r y$.

Da $K \cap H = \{1\}$, folgt, dass die $x^i y^j$ alle verschieden sind

$$\begin{aligned}(x^i y^j &= x^{i'} y^{j'} \\ &\Longrightarrow x^{i-i'} = y^{j-j'} \\ &\Longrightarrow i - i' = 0 = j - j')\end{aligned}$$

Das heisst $G = \{x^i y^j \mid 0 \leq i \leq 4, 0 \leq j \leq 1\}$ und die Relationen $x^5 = 1, y^2 = 1, xy = x^r y$ definieren die Gruppenstruktur eindeutig.

Welche Werte kann r annehmen?

Falls $yx = x^r y$:

$\implies x = yyx = yx^r y = x^{r^2} yy = x^{r^2}$

$\implies r^2 \equiv 1 \mod 5$

$\implies r = 2$ und $r = 3$ nicht möglich!

Falls $r = 1$, dann ist $yx = xy$, insbesondere ist $H \trianglelefteq G$ normal.

Da $HK = G$ und $H \cap K = \{1\}$

$\implies G \simeq H \times K \simeq C_2 \times C_5 = C_10$.

Falls $r = 4$, dann ist $yx = x^4 y = x^{-1} y \implies G \simeq D_5$. $\square$

Satz 36. *Sei G eine Gruppe, sodass $|G| = pq$ für p, q prim. Sei $p > q$. Falls $p \not\equiv 1 \mod q$, so ist $G \simeq C_{pq}$.*

Falls $p \equiv 1 \mod q$, so ist $G \simeq C_{pq}$ oder G ist nicht abelsch. (Selbe Beweisidee wie oben).

Lemma 4. *Sei $n = p^e m, p \nmid m, p$ prim, $e \geq 0$. Dann teilt p nicht $N = \binom{n}{p^e}$.*

Beweis:

$$N = \binom{n}{p^e} = \frac{n(n-1)\cdots(n-p^e+1)}{p^e(p^e-1)\cdots 1}$$

Sei $0 \leq k \leq n-1$. Schreibe $k = p^i l, p \nmid l$.

Dann gilt $p^i \mid (n-k)$ und $p^i \big| (p^e - k)$, aber $p^{i+1} \nmid (n-k)$ und $p^{i+1} \nmid (p^e - k)$.

Das heisst, Zähler und Nenner sind gleich oft durch p teilbar.

$\implies p \nmid N$. $\square$

Satz 37 (Wiederholung Sylow I)**.** *Sei G eine Gruppe, sodass $|G| = p^e m$, dann existiert $H \leq G, |H| = p^e$. Beweis von Sylow 1;*

Beweis: Sei X die Menge aller Teilmengen von G mit p^e Elementen.

Betrachte $G \curvearrowright X$ durch Linksmultiplikation.

$|X| = \binom{n}{p^e} =: N$

Wir haben $N = |X| = \sum\limits_{B \text{ Bahnen}} |B|$

Da $p \nmid N$, gibt es ein $U \in X$, sodass $p \nmid |B_U|$.

Bahnformel: $|\operatorname{Stab}(U)| \cdot |B_U| = |G| = p^e m$

$\implies p^e \big| |\operatorname{Stab}(U)|$.

Vorher gesehen: $|\operatorname{Stab}(U)| \big| |U| = p^e$.

$\implies |\operatorname{Stab}(U)| = p^e$

$\implies \operatorname{Stab}(U) \leq G$ ist eine p-Sylow. □

Vorlesung 12

Satz 38 (Erinnerung: Sylow II)**.**

(a) Alle p-Sylows in G sind konjugiert zueinander

(b) Sei $K \leq G$ eine Untergruppe, sodass $|K| = p^d$, so ist K in einer p-Sylow enthalten.

Beweis Sylow II. Sei $H \leq G$ eine p-Sylow. Betrachte $G \curvearrowright X = G/H$ durch Linksmultiplikation.

$$|X| = [G : H] = m$$

Sei $K \leq G, |K| = p^d, d \leq e$.

Behauptung: $\exists a \in G$, s.d. $a^{-1}Ka \subseteq H$. Die Behauptung impliziert (a) und (b): Falls $d = e$, so ist $a^{-1}Ka = H$. Falls $d \leq e$, so ist K in der p-Sylow aHa^{-1} enthalten.

Beweis der Behauptung: Betrachte $K \curvearrowright X = G/H$, d.h. für $k \in K, a \in G$ ist $k(aH) = kaH$. Wir haben:

$$m = |X| = \sum_{\text{K-Bahnen } B} |B|$$

$|B| \big| |K| = p^d$ für alle Bahnen B.

Da $p \nmid m$, folgt, dass eine Bahn B existiert, sodass $|B| = 1$.

Das heisst, es gibt eine Nebenklasse $aH \in G/H$, sodass $kaH = aH, \quad \forall k \in K$.

$\implies a^{-1}kaH = H$

$\implies a^{-1}ka \in H$

und somit $a^{-1}Ka \leq H$. □

Satz 39 (Erinnerung: Sylow III)**.** *Sei s die Anzahl der p-Sylows in G. Dann:*

$$s \big| m \text{ und } s \equiv 1 \mod p$$

Beweis Sylow III. Sei Y die Menge der p-Sylows in G. G operiert auf Y durch Konjugation:

$$H \mapsto gHg^{-1}$$

Gemäss Sylow II gibt es nur eine Bahn.

Bahnformel:

$$\begin{aligned} |G| &= |Y||\operatorname{Stab}(H)| \\ &= |Y||N(H)| \end{aligned}$$

D.h., $|Y| = [G : N(H)]$.

Da $H \leq N(H)$, ist $|H| = p^e$ ein Teiler von $|N(H)| = p^e c$.

$$|G| = p^e m = |Y| \cdot^e c \implies |Y| \big| m$$

Sei H eine p-Sylow. Betrachte $H \curvearrowright Y$ durch Konjugation. Sei $H' \in Y$ sodass H' von H stabilisiert wird. $\implies H \leq N(H')$.

Da $|N(H')| \big| |G|$, ist p^e die höchste Potenz von p, die $|N(H')|$ teilt.

$\implies H$ und H' sind p-Sylows in $N(H')$.

$\implies \exists g \in N(H')$, sodass $H' = gH'g^{-1} = H$.

Das heisst, H ist der einzige Fixpunkt der Operation $H \curvearrowright Y$. Die Längen der anderen Bahnen sind Vielfache von p (da sie $|H| = p^e$ teilen).

$\implies |Y| \equiv 1 \mod p$. □

Satz 40. *Sei G eine endliche abelsche Gruppe. Dann ist G isomorph zu dem Produkt $G_{p_1} \times \cdots \times G_{p_r}$, wobei die G_{p_i} p_i-Gruppen für Primzahlen $p_1, \ldots, p_r$ sind.*

Beweis: Schreibe $|G| = p_1^{r_1} \cdots p_n^{r_n}$ (Primfaktorisierung).

Sei H_i eine p_i-Sylow für $i = 1, \ldots, n$. Alle H_i sind normal. H_1H_2 ist Untergruppe von G und H_1H_2 ist isomorph zu $H_1 \times H_2$, da $H_1 \cap H_2 = \{1\}$.

Per Induktion zeigt man ähnlich, dass $H_1H_2 \cdots H_s$ eine Untergruppe ist und isomorph zu $H_1 \times \cdots \times H_s$:

$H_1 \cdots H_{s-1} \simeq H_1 \times \cdots \times H_{s-1}$

$(H_1 \cdots H_{s-1})H_s$ ist Untergruppe

$H_1 \cdots H_{s-1} \cap H_s = \{1\}$.

$\implies H_1 \times \cdots \times H_n \simeq H_1 \cdots H_n$.

Da $H_1 \times \cdots \times H_n$ genau $|G|$ Elemente enthält, folgt $G = H_1 \cdots H_n \simeq H_1 \times H_1 \times \cdots \times H_n$. □

Definition 28. *Eine Gruppe G heisst* ***endlich erzeugt****, wenn es eine endliche Teilmenge $\{x_1, \ldots, x_n\} \subseteq G$ gibt, sodass $G = <x_1, \ldots, x_n>$*

Satz 41. *Sei G eine endlich erzeugte abelsche Gruppe. Dann ist G isomorph zu $\mathbb{Z}^n \times C_{p_1^{r_1}} \times \cdots \times C_{p_n^{r_n}}$, wobei $p_1, \ldots, p_n$ Primzahlen sind (nicht unbedingt verschieden) und $r_i \geq 0$.*

Beweis: Siehe Algebra II. □

Vorlesung 13

Freie Gruppen

Sei X eine Menge von **Zeichen**.

Beispiel 13. $X = \{a, b, c\}$

Ein **Wort** ist eine endliche Folge von Zeichen.

Beispiel 14. $X = \{a, b\}$

$a, b, aa, bababb$ sind Wörter in X.

Sei W die Menge aller Wörter in X. Wir können Wörter zusammenhängen.

Beispiel 15. *$aa, ba \mapsto aaba$.*

Dies definiert eine assoziative Verknüpfung, somit haben wir eine **Semigruppe** (Menge mit assoziativer Verknüpfung).

$W \times W \to W \quad v, w \mapsto vw.$

Das leere Wort ist das neutrale Element bezüglich dieser Verknüpfung. Wir bezeichnen es mit 1. Somit erhalten wir ein **Monoid** (Semigruppe mit neutralem Element).

Dieses oben definierte Monoid nennt sich das **freie Monoid**.

Um eine Gruppe zu definieren, brauchen wir auch noch Inverse.

Wir fügen zu jedem Zeichen $a \in X$ noch ein Zeichen a^{-1} hinzu. Diese neue Menge nennen wir X'.

Beispiel 16. $X = \{a, b\} \implies X' = \{a, a^{-1}, b, b^{-1}\}$

Sei W' die Menge der Wörter mit Zeichen in X'.

Beispiel 17. $X' = \{a, a^{-1}, b, b^{-1}\}$

$aa^{-1}b \in W',\ b \in W',\ b^{-1}b \in W'$

Falls in einem Wort $w \in W'$ für ein $x \in X$ der Abschnitt $\ldots xx^{-1} \ldots$ oder $\ldots x^{-1}x \ldots$ vorkommt, so kürzen wir die zwei Symbole x, x^{-1} weg und erhalten ein kürzeres Wort.

Definition 29. *Ein Wort ist **reduziert**, wenn man keine solche Kürzung mehr möglich ist.*

Bemerkung 38. *Ein gegebenes Wort $w \in W'$ lässt sich endlich oft kürzen, bis wir ein reduziertes Wort w_0 enthalten. Ein solches w_0 heisst **reduzierte Form** von w.*

Beispiel 18. $babb^{-1}a^{-1}c^{-1}ca$

Mögliche Kürzungen:

- $babb^{-1}a^{-1}c^{-1}ca \to baa^{-1}c^{-1}ca \to bc^{-1}ca \to ba$
- $babb^{-1}a^{-1}c^{-1}ca \to babb^{-1}a^{-1}a \to babb^{-1} \to ba$

Satz 42. *Jedes Wort $w \in W'$ hat genau eine reduzierte Form.*

Beweis: Induktion über die Länge von w.

Base case ist klar für $|w| = 0$.

Falls w reduziert ist, sind wir fertig.

Falls w nicht reduziert ist:

$w = \dots xx^{-1} \dots$ für ein $x \in X'$

Behauptung: Wir erreichen jede reduzierte Form von w, indem wir zuerst $\dots xx^{-1} \dots$ kürzen. Dies impliziert den Satz per Induktion.

Beweis der Behauptung: Sei w_0 eine reduzierte Form von w.

Fall 1: xx^{-1} wird irgendwann einmal weggekürzt. Dann können wir xx^{-1} auch direkt kürzen.

Fall 2: $x^x{-1}$ wird nicht gekürzt. Das Paar $x^x{-1}$ kommt nicht in w_0 vor, d.h. irgendwann ist entweder $\dots x^{-1}xx^{-1} \dots$ oder $\dots xx^{-1}x \dots$.

Diese Vereinfachung hat jedoch denselben Effekt wie wenn man xx^{-1} kürzt $\rightsquigarrow$ Fall 1. $\square$

Für zwei Wörter $w, w' \in W$ definiere $w \sim w'$, falls w und w' dieselbe reduzierte Form haben.

$\rightsquigarrow$ Äquivalenzrelation auf W'.

Satz 43. *Seien $v, v', w, w' \in W'$. Aus $w \sim w'$ und $v \sim v'$ folgt $wv \sim w'v'$.*

Beweis: $wv \underset{\text{vereinfachen}}{\rightsquigarrow} w_0v_0 \rightsquigarrow$ weiter vereinfachen.

Ähnlich $w'v' \underset{\text{vereinfachen}}{\rightsquigarrow} w_0v_0 \rightsquigarrow$ weiter vereinfachen.

$\implies wv$ und $w'v'$ haben dieselbe reduzierte Form. $\square$

Satz 44. *Die Menge F der Äquivalenzklassen von Wörtern in W' bildet mit der von W' induzierten Verknüpfung eine Gruppe.*

Beweis: Die von W' induzierte Verknüpfung ist wohldefiniert gemäss obigem Satz.

Assoziativität ist klar.

Neutrales Element: 1; folgt auch aus der Verknüpfung.

Inverse: Für die Klasse von $w = xy \dots z$ ist die Klasse von $z^{-1} \dots y^{-1}x^{-1}$ ein Inverses. $\square$

Definition 30. *Diese Gruppe F ist die* ***freie Gruppe*** *auf der Menge X.*

Bemerkung 39. *Jedes Element in F entspricht genau einem reduzierten Element. Verknüpfung: hintereinander schreiben, dann reduzieren.*

Beispiel 19. *Sei F die freie Gruppe auf $\{a, b, c\}$.*

$(abc^{-1})(cb) = abc^{-1}cb = abb$

Bemerkung 40. *Wir verwenden Produktschreibweise:*

$$aaab^{-1}b^{-1} = a^3b^{-2}$$

Beispiel 20. *Sei F die freie Gruppe auf $X = \{a\}$. Dann ist $F = \{a^n \mid n \in \mathbb{Z}\} \simeq \mathbb{Z}$*

Sobald $|X| \geq 2$, wird F sehr kompliziert.

Satz 45. *Sei F die freie Gruppe auf X und G eine Gruppe.*

Jede Abbildung $f\colon X \to G$ lässt sich in eindeutiger Weise zu einem Homomorphismus $\phi\colon F \to G$ fortsetzen.

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, hook] \arrow[dr, phantom, "\circlearrowright"] & G \\ F \arrow[ur, "\exists!\phi"'] & \end{tikzcd}$$

Beweis: Sei $w = x_1 \cdots x_n$ ein Wort in W'. Wir definieren $\phi(w) = f(x_1) \cdots f(x_n)$, wobei $f(a^{-1}) = f(a)^{-1}$.

ϕ ist wohldefiniert: Zwei äquivalente Wörter werden auf dasselbe Element in G abgebildet.

ϕ ist offensichtlich ein Homomorphismus und eindeutig. $\square$

Bemerkung 41. *Seien G eine Gruppe, $X \subseteq G$ und F die freie Gruppe auf X. Dann existiert ein Homomorphismus $\phi\colon F \to G$.*

Falls $X \subseteq G$ Erzeugende von G sind, dann ist ϕ surjektiv.

$\underset{\textit{1. Isosatz}}{\Longrightarrow}$ *$G \simeq F/N$, wobei $N = \operatorname{Kern}\phi$.*

*Die Elemente in N heissen **Relationen** zwischen den Erzeugenden.*

D.h., $w \in F$ ist eine Relation $\Leftrightarrow \phi(w) = 1$, d.h. $w = 1$ in G.

Umgekehrt, falls F die freie Gruppe auf X ist und $N \trianglelefteq F$, so ist $G = F/N$ die Gruppe, in der die Relationen $N = 1$ gelten $\forall n \in N$.

Definition 31. *Eine Teilmenge $R \subseteq N$ heisst Menge von **definierenden Relationen** für G, falls N der kleinste Normalteiler ist, der R enthält, d.h.*

$$N = \bigcap_{\substack{H \trianglelefteq G \\ R \subseteq H}} H$$

X und R definieren G. Wir schreiben $G = <X \mid R>$.

$<X \mid R>$ heisst **Präsentation** von G.

Satz 46. *Seien G eine Gruppe und $N \trianglelefteq G$, und $\pi\colon G \to \overline{G} = G/N$ Quotient, $a \mapsto \overline{a} = aN$.*

Sei $\phi\colon G \to G'$ ein Homomorphismus mit $N \subseteq \operatorname{Kern}\phi$. Dann existiert ein eindeutiger Homomorphismus $\overline{\phi}\colon \overline{G} \to G'$, sodass $\overline{\phi} \circ \pi = \phi$.

$$\begin{tikzcd}
G \arrow[rr, "\phi"] \arrow[dr, "\pi"'] & \arrow[d, phantom, "\circlearrowright"] & G' \\
& \overline{G} \arrow[ur, "\exists!\overline{\phi}"'] &
\end{tikzcd}$$

Beweis: Wir definieren $\overline{\phi}(\overline{a}) := \phi(a)$.

Da $\overline{\phi}(\pi(a)) = \phi(a)$ sein soll, gibt es keine andere Wahl.

$\overline{\phi}$ ist wohldefiniert: Seien $a, a' \in G$ s.d. $\overline{(a)} = \overline{a'} \implies \exists n \in N s.d. a' = an$. $\underset{N \in \operatorname{Kern}\phi}{\Longrightarrow} \phi(a') = \phi(a)\phi(a) = \phi(a)$.

$\overline{\phi}$ ist ein Homomorphismus: $\overline{\phi}(\overline{a})\overline{\phi}(\overline{b}) = \phi(a)\phi(b) = \phi(ab) = \overline{\phi}(\overline{ab})$. $\square$

Satz 47. *Diedergruppe $D_n = <x, y \mid x^n, y^2, xyxy>$.*

Beweis: Wir haben gesehen, dass D_n von der Drehung x und der Spiegelung y erzeugt ist und dass gilt: $x^n = 1, y^n = 1, xyxy = 1$.

Sei F die freie Gruppe auf $\{x, y\} \implies \exists$ surjektiver Homomorphismus

$\phi\colon F \to D_n$ s.d. $R = \{x^n, y^n, xyxy\} \subseteq \operatorname{Kern}\phi$.

Sei N der kleinste Normalteiler, der R enthält.

$\implies N \subseteq \operatorname{Kern}\phi$.

$\underset{\text{satz}}{\implies} \exists$ Homomorphismus $\overline{\phi}\colon F/N \to D_n$, s.d. $\overline{\phi} \circ \pi = \phi$,

wobei $\pi\colon F \to F/N$.

Zu zeigen: $\overline{\phi}$ ist ein Isomorphismus.

- $\overline{\phi}$ ist surjektiv, da ϕ surjektiv ist.
- in F/N gilt $\overline{x}^n = 1,\ \overline{y}^2 = 1,\ \overline{xyxy} = 1$

  $\implies$ Wir können jedes Element in F/N auf die Form $\overline{x}^i\overline{y}^j$ bringen, mit $0 \le i \le n-1$ und $0 \le j \le 1$.

  $\implies F/N$ enthält $\le 2n$ Elemente.

  Da $|D_n| = 2n$, folgt, dass $\overline{\phi}$ bijektiv sein muss.

□

Satz 48. *Die Gruppe* $G = \langle x, y | xyx^{-1}y^{-1} \rangle$ *ist abelsch.*

Beweisidee.

- x, y, x^{-1}, y^{-1} kommutieren alle miteinander.
- Alle Wörter kommutieren.

□

Vorlesung 14

Ringe (Kapitel 10 in Artin)

Definition 32. *Ein* ***Ring*** R *ist eine Menge mit zwei Verknüpfungen* $+$ *und* $\cdot$, *Addition und Multiplikation, sodass die folgenden Axiome erfüllt sind:*

(a) $(R, +)$ *ist eine abelsche Gruppe. Bezeichne das neutrale Element mit* 0.

(b) Die Multiplikation ist assoziativ und hat ein neutrales Element $1 \in R$.

(c) Für alle $a, b, c \in R$ *gilt:* $(a+b)c = ac + bc$ *und* $c(a+b) = ca + cb$ *(Distributivgesetz).*

Beispiele

- Die ganzen Zahlen $\mathbb{Z}$
- Der Nullring $R = \{0\}$
- $\mathbb{Z}\left[\frac{1}{2}\right] = \left\{\frac{a}{2^k} \mid a, k \in \mathbb{Z}\right\}$
- Die Gaussschen Zahlen: $\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\} \subseteq \mathbb{C}$
- $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$
- $\mathrm{Mat}_{n\times n}$, der Ring der $(n \times n)$-Matrizen über einem Körper K. (Hier ist die Multiplikation nicht kommutativ.)

Bemerkung 42. *Ein **kommutativer Ring** ist ein Ring, in dem die Multiplikation kommutativ ist. In dieser Vorlesung: Ring = kommutativer Ring.*

Bemerkung 43. *In manchen Quellen ist die Existenz eines neutralen Elements nicht Teil der Definition eines Rings.*

Satz 49. *Sei R ein Ring. Dann gilt $0 \cdot a = 0 \quad \forall a \in R$.*

Beweis: Sei $x \in R$. Dann ist $xa = (0 + x)a = 0a + xa \implies 0a = 0$. □

Daraus folgt direkt:

Korollar 12. *Sei R ein Ring. Falls $1 = 0$, so ist R der Nullring.*

Bemerkung 44. *$(-1)a = -a$ für alle $a \in R$.*

Beweis: $a + (-1)a = (1 - 1)a = 0a = 0 \implies (-1)a = -a$ □

Definition 33. *Ein Ring R ist ein **Körper**, falls R nicht der Nullring ist und jedes Element in $R\setminus\{0\}$ ein multiplikatives Inverses hat.*

Definition 34. *Seien R, R' Ringe. Ein **Homomorphismus** $\phi\colon R \to R'$ ist eine Abbildung, s.d. $\forall a, b \in R$:*

(1) $\phi(a + b) = \phi(a) + \phi(b)$

(2) $\phi(ab) = \phi(a)\phi(b)$

(3) $\phi(1_R) = 1_{R'}$

*Falls ϕ ausserdem bijektiv ist, so ist ϕ ein **Isomorphismus**.*

Bemerkung 45. *Ein Ringhomomorphismus ist immer auch ein Gruppenhomomorphismus bezüglich der additiven Gruppe. $\implies \phi(0_R) = 0_{R'}$.*

Beispiele

- $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ ist ein Ringhomomorphismus.
- Sei R der Nullring. Es gibt keinen Homomorphismus $\phi\colon R \to R'$, wenn R' nicht auch der Nullring ist.

Definition 35. *Sei $\phi\colon R \to R'$ ein Ringhomomorphismus. Der **Kern** von ϕ ist* $\operatorname{Kern}\phi = \{a \in R \mid \phi(a) = 0\}$

Bemerkung 46. *Ein Ringhomomorphismus $\phi\colon R \to R'$ ist injektiv $\Leftrightarrow \operatorname{Kern}\phi = 0$, da ϕ ein Homomorphismus von den additiven Gruppen ist.*

Definition 36. *Sei R ein Ring. Ein **Unterring** $S \subseteq R$ ist eine Teilmenge, s.d.*

(1) S ist eine Untergruppe bezüglich Addition

(2) S ist abgeschlossen bezüglich Multiplikation

(3) $1 \in S$

Bemerkung 47.

- *Falls $R \neq 0$, so ist $\operatorname{Kern}\phi$ <u>kein</u> Unterring (da $1 \notin \operatorname{Kern}\phi$).*
- *Falls $a \in \operatorname{Kern}\phi$ und $r \in R$, so ist auch $ra \in \operatorname{Kern}\phi$.*

Definition 37. *Ein **Ideal** $I \subseteq R$ ist eine Teilmenge s.d.*

(i) $I \subseteq R$ ist eine additive Untergruppe

(ii) Ist $a \in I$, dann ist für alle $r \in R$ auch $ra \in I$.

Bemerkung 48.

- $\operatorname{Kern}\phi \subseteq R$ *ist ein Ideal*
- *$I \subseteq R$ ist ein Ideal genau dann, wenn $I \neq \emptyset$ und für alle $a_1, \ldots, a_n \in I$ und $r_1, \ldots, r_n \in R$ (und alle n) gilt, dass $r_1a_1 + \cdots + r_na_n \in I$.*

Beweis: Kleine Übung. □

Vorlesung 15

Definition 38. *Sei R ein Ring. Ein **Unterring** $S \subseteq R$ ist eine Teilmenge, s.d. $S \subseteq R$ ist eine Teilmenge, sodass*

(1) S ist Untergruppe bezüglich Addition

(2) S ist abgeschlossen bezüglich Multiplikation

(3) $1 \in S$

Definition 39. *Sei R ein Ring. Ein **Ideal** $I \subseteq R$ ist eine Teilmenge, s.d.*

(a) *I ist eine Untergruppe bezüglich Addition.*

(b) *Ist $n \in R$ und $a \in I$, so ist $ra \in I$.*

Bemerkung 49. *Sei $\phi \colon R \to R'$ ein Homomorphismus.* $\implies$ Bild $\phi \subseteq R'$ *ist ein Unterring.*

Beweis: Bild ϕ ist eine Untergruppe, da ϕ auch Gruppenhomomorphismus ist.

$a = \phi(r), b = \phi(s)$ für $r, s \in R$

$\implies ab = \phi(r)\phi(s) = \phi(rs)$, d.h. $ab \in$ Bild ϕ.

$\implies$ abgeschlossen bez. Multiplikation.

$1_{R'} \in$ Bild ϕ da $\phi(1_R) = \phi(1_{R'})$. □

Beispiel

- Für $n \in \mathbb{Z}$ ist $n\mathbb{Z}$ ein Ideal.
- Allgemein, für $a \in R$ ist $aR = Ra = \{ra \mid r \in R\} = (a)$ ein Ideal.

Definition 40. *Ein Ideal von der Form (a) für ein $a \in R$ heisst **Hauptideal**.*

Definition 41. *Seien $a_1, \ldots, a_n \in R$. Das Ideal $(a_1, \ldots, a_n) = \left\{ \sum_{i=1}^{n} r_i a_i \mid r_i \in R \right\}$ heisst das **Ideal erzeugt von** $a_1, \ldots, a_n$.*

Definition 42. *Sei R ein Ring. Ein $a \in R$ ist eine **Einheit**, falls es ein $b \in R$ gibt, s.d. $ab = 1$.*

Ticker Frage: Sei R ein Ring und $a \in R$ eine Einheit. Dann ist $(a) = R$. (wahr, da $1 = ba \in (a) \implies r \cdot 1 = r \in (a) \quad \forall r \in R$).

Satz 50. *Jedes Ideal in $\mathbb{Z}$ ist ein Hauptideal.*

Beweis: Jede Untergruppe von $\mathbb{Z}^+$ ist von der Form $n\mathbb{Z}$ für ein $n \in \mathbb{Z}$. Dies sind alles Ideale. □

Satz 51. (a) *Sei K ein Körper. Dann sind 0 und (1) die einzigen Ideale.*

(b) *Hat ein Ring R genau zwei Ideale, so ist R ein Körper.*

Beweis: (a) Sei $I \subseteq K$ ein Ideal. Falls $I \neq (0)$, so enthält I ein Element $a \neq 0$. Da K ein Körper ist, ist a eine Einheit.

$\implies (a) = (1) = K$.

(b) $R \neq 0$, da R zwei Ideale enthält, d.h. $1 \neq 0$. Sei $0 \neq a \in R$, dann ist $(a) \neq (0)$.

$\implies (a) = (1) = R$

$\implies \exists b \in R$ s.d. $ba = 1$

$\implies b = a^{-1}$. D.h. R ist ein Körper.

$\square$

Korollar 13. *Seien K ein Körper und $R \neq \{0\}$ ein Ring. Jeder Homomorphismus $\phi\colon K \to R$ ist injektiv.*

Beweis: $\operatorname{Kern} \phi \subseteq K$ ist ein Ideal.

Falls $\operatorname{Kern} \phi = (1)$, so ist $R = 0$. Ansonsten ist $\operatorname{Kern}(\phi) = (0)$.

$\implies \phi$ ist injektiv. $\square$

Definition 43. *Sei S ein Ring, $R \subseteq S$ ein Unterring und $\alpha \in S$. Wir bezeichnen mit $R[\alpha] \subseteq S$ den kleinsten Unterring, der R und α enthält.*

Bemerkung 50.

$$R[\alpha] = \{s \in S \mid \exists n \text{ und } r_0, \dots r_n \in R \text{ s.d. } s = r_0 + r_1\alpha + \dots + r_n\alpha^n\} =: R'$$

Beweis: R' ist Unterring und $R \subseteq R'$, $\alpha \in R' \implies R[\alpha] \subseteq R'$.

Offensichtlich ist auch $R[\alpha \supseteq R'$. $\square$

Beispiele

- $\mathbb{Z}[i] = \{a + bi \mid a, b, \in \mathbb{Z}\} \subseteq \mathbb{C}$
- $\mathbb{Q}[\sqrt{2}] \subseteq \mathbb{R}$

Polynomringe

Sei R ein Ring und x eine Variable. Der **Polynomring** $R[x]$ ist der Ring der Polynome

$$R[x] = \left\{ \sum_{i=0}^{n} a_i x^i \mid n \geq 0, a_i \in R \right\}$$

mit der üblichen Addition und Multiplikation.

Bemerkung 51. *$R[x]$ ist im Allgemeinen nicht dasselbe wie der Ring der polynomialen Abbildungen $R \to R$.*

Beispiel 21. *Wenn R endlich ist, so gibt es nur endlich viele Abbildungen $R \to R$ und somit nur endlich viele polynomiale Abbildungen. Aber der Ring der Polynome $R[x]$ ist unendlich.*

Bemerkung 52. *Die Inklusionsabbildung $\iota R \hookrightarrow R[x] \quad a \mapsto a + 0x + \cdots$ ist ein Ringhomomorphismus. Wir können R somit als Unterring von $R[x]$ anschauen.*

Definition 44. *Seien R ein Ring und $x_1, \ldots, x_n$ Variablen. Der **Polynomring** $R[x_1, \ldots, x_n]$ in n Variablen ist der Ring der Polynome*

$$\left\{ \sum_{i_1,\ldots,i_n} a_{i_1\cdots i_n} x_1^{i_1} \cdots x_n^{i_n} \;\middle|\; \substack{a_{i_1\cdots i_n} \in R, (i_1,\ldots,i_n) \in \mathbb{Z}^n_{\geq 0}, \\ \text{nur endlich viele der } a_{i_1\cdots i_n} \text{ sind nicht } 0} \right\}$$

mit der üblichen Addition und Multiplikation.

*Elemente von der Form $x_1^{i_1} \cdots x_n^{i_n}$ heissen **Monome**.*

Bemerkung 53. *Oft schreibt man $i = (i_1, \ldots, i_n)$ und dann $a_i x^i = a_{i_1\cdots i_n} x_1^{i_1} \cdots x_n^{i_n}$ (Multiindex Schreibweise).*

In dieser Schreibweise gilt, für $i = (i_1, \ldots, i_n), j = (j_1, \ldots, j_n): \quad x^i x^j = x^{i+j}$.

Beobachtung 1. *Ein $a \in R$ induziert einen Homomorphismus $R[x] \to R \quad p(x) \mapsto p(a)$.*

Satz 52 (Einsetzungsprinzip)**.** *Sei $\phi\colon R \to R'$ ein Ringhomomorphismus zu gegebenen Elementen $\alpha_1, \ldots, \alpha_n \in R'$, gibt es einen eindeutig bestimmten Homomorphismus $\Phi\colon R[x_1, \ldots, x_n] \to R'$, so dass die Einschränkung von Φ auf die konstanten Polynome mit ϕ übereinstimmt und sodass $\Phi(x_1) = \alpha_i$ für $i = 1, \ldots, n$.*

$$\begin{tikzcd}
R \arrow[rr, "\phi"] \arrow[dr, hook, "i"'] & & R' \\
& R[x] \arrow[ur, "\Phi"'] \arrow[u, phantom, "\circlearrowright"] &
\end{tikzcd}$$

Beweis: Multindex-Schreibweise

$$\begin{aligned} x &= (x_1, \ldots, x_n) \\ \alpha &= (\alpha_1, \ldots, \alpha_n) \\ i &= (i_1, \ldots, i_n) \end{aligned}$$

Für $r \in R$, schreiben wir $r' := \phi(r)$.

Falls Φ existiert, so muss gelten

$$\begin{aligned}\Phi\left(\sum nx^i\right) &= \sum \phi(r_i)\alpha^i \\ &= \sum r_i'\alpha^i\end{aligned}$$

(da Φ ein Homomorphismus ist). D.h. Φ ist eindeutig.

Es genügt zu zeigen: Die Abbildung $\Phi\colon R[x] \to R \quad \sum r_i x^i \mapsto \sum r_i'\alpha^i$ ist ein Homomorphismus.

Wir haben:

$$\begin{aligned}\Phi\left(\sum r_i x^i + \sum s_i x^i\right) &= \Phi\left(\sum (r_i + s_i)x^i\right) \\ &= \sum (r_i + s_i)\alpha^i \\ &= \sum (r_i' + s_i')a^i \\ &= \sum r_i'\alpha^i + \sum s_i'\alpha^i \\ &= \Phi\left(\sum r_i\alpha^i\right) + \Phi\left(\sum s_i\alpha^i\right)\end{aligned}$$

$$\begin{aligned}\Phi\left(\left(\sum r_i x^i\right)\left(\sum s_j x^j\right)\right) &= \Phi\left(\sum r_i s_j x^{i+j}\right) \\ &= \sum (r_i s_j)'\alpha^{i+j} \\ &= \sum r_i' s_j' \alpha^{i+j} \\ &= \left(\sum r_i'\alpha^i\right)\left(\sum s_j'\alpha^j\right) \\ &= \Phi\left(\sum r_i\alpha^i\right)\Phi\left(\sum s_j\alpha^j\right)\end{aligned}$$

und $\Phi(1) = 1$ (per Definition). □

Bemerkung 54. *Sei $\psi\colon R \to R'$ ein Homomorphismus $\rightsquigarrow$ Homomorphismus*

$$\begin{tikzcd} R \arrow[r] \arrow[rr, bend right, "\phi"'] & R' \arrow[r, hook] & R'[x] \end{tikzcd}$$

Gemäss Satz können wir ϕ eindeutig zu einem Homomorphismus $\Phi\colon R[x] \to R'[x]$ fortsetzen, sodass x auf x abgebildet wird.

Φ bildet ein Polynom $a_0 + a_1 x + \cdots a_n x^n$ auf das Polynom $\phi(a_0) + \phi(a_1)x + \cdots + \phi(a_n)x^n$ ab.

Beispiel 22. *$\psi\colon \mathbb{Z} \to \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ Reduktion modulo p.*

$\rightsquigarrow \Phi\colon \mathbb{Z}[x] \to \mathbb{F}_p[x]$ $f(x) = a_0 + \cdots + a_n x^n \mapsto \overline{a_0} + \cdots + \overline{a_n} x^n$

$\overline{f}(x)$ ist die Restklasse von $f(x)$ modulo p.

(Bemerkung: $\operatorname{Kern}\Phi = (p)$*).*

$$R[x][y] \underbrace{\simeq}_{\textit{wollen wir zeigen}} R[x,y]$$

Beispiel 23.

$$x^2y^2 + 4x^3 - 3x^2y - 4y^2 + 2 = (x^2-4)y^2 - (3x^2)y + (4x^3+2)$$

Satz 53. *Seien $x = (x_1, \cdots, x_n), y = (y_1, \ldots, y_m)$ zwei Mengen von Variablen. Dann gibt es einen eindeutigen Isomorphismus $\Phi\colon R[x,y] \to R[x][y]$ s.d. Φ auf R die Identität ist und Φ die Variablen auf sich selbst abbildet.*

Beweis: Es gibt einen eindeutigen Homomorphismus $\Phi\colon R[x,y] \to R[x][y]$ s.d. Φ auf R die Identität ist und Φ die Variablen auf sich selbst schickt.

Zu zeigen: Φ ist ein Isomorphismus.

Betrachten wir die Inklusion $\psi\colon R[x] \hookrightarrow R[x,y]$

$\rightsquigarrow$ ψ lässt sich eindeutig fortsetzen zu einem Homomorphismus

$\Psi\colon R[x][y] \to R[x,y]$ so dass die y_i's auf sich selbst abgebildet werden.

$\Psi \circ \Phi\colon R[x,y] \to R[x,y]$ ist die Identität auf R und schickt die Variablen auf sich selbst.

$\underset{\text{Einsetzungsprinzip}}{\Longrightarrow}$ $\Psi \circ \Phi = \mathrm{id}_{R[x,y]}$, Ähnlich: $\Phi \circ \Psi = \mathrm{id}_{R[x,y]}$ $\square$