# Algebra I – Prof. Christian Urech

Mitschrift: Franz Nowak

Herbstsemester 2025

## Vorlesung 1

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

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

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

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

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

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

**Bemerkung 1.** *Wenn $G$ assoziativ ist, dann ist $g_1g_2\cdots g_n$ eindeutig definiert (für $g_1,g_2,\ldots,g_n \in G$).*

**Satz 1.** *(a) Das neutrale Element ist eindeutig.*

*(b) Das Inverse von jedem Element ist eindeutig.*

*Beweis:* (a) Seien $e,e' \in G$ neutrale Elemente. Dann ist $e = ee' = e'$.

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

□

**Satz 2.** *Seien $G$ eine Gruppe und $a,b,c \in G$, sodass $ab = ac$. Dann ist $b = c$.*

*Beweis:*

$$ab = ac \implies \underbrace{a^{-1}a}_{e} b = \underbrace{a^{-1}a}_{e} c \implies b = c$$

□

**Beispiele**

- Ganze Zahlen mit Addition, $(\mathbb{Z}, +)$ oder $\mathbb{Z}^+$
- Reelle Zahlen mit Addition, $(\mathbb{R}, +)$ oder $\mathbb{R}^+$
- Körper $K$ mit Addition, $(K, +)$ oder $K^+$. (Bemerkung: Keine Gruppe mit Multiplikation, wenn 0 enthalten ist.)
- Vektorraum $V$ mit Addition, $(V, +)$ oder $V^+$.
- Allgemeine lineare Gruppe, $GL_n(K)$
- Spezielle lineare Gruppe, $SL_n(K) := \{A \in GL_n(K) \mid \det A = 1\}$
- Orthogonale Gruppe, $O_n$
- Unitäre Gruppe, $U_n$

**Permutationsgruppen**

Sei $\mathrm{Sym}(M)$ die Menge der Bijektionen von einer Menge $M$ zu sich selbst, zusammen mit der Verknüpfung von Abbildungen. Die **symmetrische Gruppe** $S_n := \mathrm{Sym}(\{1, 2, \ldots, n\})$ ist eine Gruppe mit $n!$ Elementen.

**Bemerkung 2.** *Jedes Element in $S_n$ ist ein Produkt von Transpositionen.*

**Erinnerung:** Eine **Transposition** ist eine Permutation, die genau zwei Elemente vertauscht und die übrigen gleich lässt.

**Beispiel 1.** *$S_3$, die Gruppe der Permutationen von $\{1, 2, 3\}$. Seien $\sigma, \tau \in S_3$,*

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

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

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

*D.h. $S_3$ ist nicht abelsch.*

## Untergruppen

**Definition 2.** *Sei $G$ eine Gruppe. Eine **Untergruppe** $H \leq G$ ist eine Teilmenge $H \subseteq G$ sodass*

*(a)* $\forall a, b \in H, ab \in H$

*(b)* $1_G \in H$

*(c)* $\forall a \in H, a^{-1} \in H$

**Bemerkung 3.** *Jede Untergruppe ist eine Gruppe* $(H, *_H)$. $*_G$ *induziert* $*_H$.

**Bemerkung 4.** $H \subseteq G$ *mit* $H \neq \{\emptyset\}$ *ist eine Untergruppe von* $G$ *genau wenn* $\forall a, b \in H,\ ab^{-1} \in H$.

*Beweis:* "$\Rightarrow$": klar.

"$\Leftarrow$": Bedingung: Seien $a, b \in H$.

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

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

(c) $\implies 1_G a^{-1} \in H$ d.h. $a^{-1} \in H$

□

**Bemerkung 5.** *Jede Gruppe* $G$ *hat als Untergruppen immer* $\{1\}$ *(die triviale Untergruppe) und* $G$ *selbst. Andere Untergruppen heissen* ***echte*** *Untergruppen.*

**Beispiele**

- $SL_n(K) \leq GL_n(K)$
- $n\mathbb{Z} \leq \mathbb{Z} \quad \forall n \in \mathbb{Z}$
- Sei $S^1 := \{c \in \mathbb{C}^* \mid |C| = 1\}$. $S^1 \leq \mathbb{C}^*$. $(\mathbb{C}^* := (\mathbb{C}\backslash\{0\}, \cdot)$
- $B_n(K) := \{A \in GL_n(K) \mid A$obere Dreiecksmatrix$\}$. $B_n \leq GL_n(K)$.
- $O_n \leq GL_n(\mathbb{R})$
- Die alternierende Gruppe $A_n \leq S_n$ ist die Untergruppe aller Permutationen, die das Produkt einer geraden Anzahl von Transpositionen sind.

**Bemerkung 6.** *Seien* $G$ *eine Gruppe und* $a \in G$. *Dann ist*

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

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

**Bemerkung 7.** $<a>$ *ist abelsch:* $a^m a^n = a^{m+n} = a^{n+m} = a^n a^m$

**Lemma 1.** *Sei* $X \subseteq \mathbb{Z}$ *die Menge der Zahlen* $n$, *sodass* $a^n = 1$. *Dann ist* $X = m\mathbb{Z}$ *für ein* $m \in \mathbb{Z}$.

*Beweis:* $X$ ist eine Untergruppe von $\mathbb{Z}$:

(a) Seien $m, n \in X$, dann ist $a^{m+n} = a^m a^n = 1_G \implies m + n \in X$

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

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

Gemäss Übung ist $X$ von der Form $m\mathbb{Z}$ für ein $m \in \mathbb{Z}$. $\square$

Falls $m \neq 0$:

Für $n \in \mathbb{Z}$ schreibe $n = km + r$ für ein $k \in \mathbb{Z}$ s.d. $0 \leq r < m$. Dann ist $a^n = a^{km+r} = a^{km}a^r = a^r$. $\implies$ $<a> = \{1, a, \ldots, a^{m-1}\}$ und all diese Elemente sind verschieden. (Falls $a^r = a^{r'} \implies a^{r-r'} = 1 \implies r - r' \in m\mathbb{Z} \implies r = r'$ $0 \leq r, r' < m$)

Falls $m = 0$:

Dann ist $<a> = \{\ldots, a^{-2}, a^{-1}, 1, a, a^2, \ldots\}$ und alle Partitionen sind verschieden.

# Vorlesung 2

**Definition 3.** *Die **Ordnung** $|G|$ einer Gruppe $G$ ist die Anzahl der Elemente in $G$ (kann $\infty$ sein). Die **Ordnung des Elements** $a \in G$ ist $|<a>|$, wobei $<a> = \{1, a, \ldots, a^{m-1}\}$ mit $m > 0$ die kleinste Zahl s.d. $a^m = 1$.*

**Beispiele**

- $A = \begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \in GL_2(\mathbb{R})$ hat Ordnung 6.
- $B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \in GL_2(\mathbb{R})$ hat Ordnung $\infty$.

## Homomorphismen

**Definition 4.** *Seien $G, G'$ zwei Gruppen. Ein **Homomorphismus** ist eine Abbildung $\phi\colon G \to G'$ s.d. $\phi(ab) = \phi(a)\phi(b)$ $\forall a, b \in G$.*

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

**Beispiele**

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

**Satz 3.**

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

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

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

(2) zu zeigen: $\phi^{-1}$ ist ein Homomorphismus.

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

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

□

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

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

Falls $|G| = |G'|$ endlich ist, so ist $G = \{1, a, \ldots, a^{m-1}\}$, $G' = \{1, b, \ldots, b^{m-1}\}$. Somit ist $\phi$ wohldefiniert, bijektiv und ein Homomorphismus.

Falls $|G| = |G'| = \infty$, so ist $\phi$ 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 $f$). $\phi$ ist ein Automorphismus.*

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

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

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

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

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

**Beispiele**

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

**Bemerkung 9.** *Seien $\phi\colon G \to G'$ ein Homomorphismus und $a \in \operatorname{Kern}\phi$ und $b \in G$. Dann ist*

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

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

$\overset{\text{Bem. 9}}{\implies}$ $\operatorname{Kern}\phi$ ist immer ein Normalteiler.

# Vorlesung 3

**Erinnerung:** Eine Untergruppe $N \leq G$ ist ein Normalteiler, falls:

$$\forall a \in N, \forall b \in G : bab^{-1} \in N$$

. Clicker-Frage zu Normalteilern $\trianglelefteq$:

1. $B_n(K) \leq GL_n(K)$ ist kein Normalteiler.
2. $Z^+ \trianglelefteq R^+$ ist Normalteiler (weil $R^+$ abelsch)
3. $SL_n(K) \trianglelefteq GL_n(K)$, weil $\det(ABA^{-1}) = \det(A)\det(B)\det(A)^{-1} = \det(B)$, oder bemerke, dass $SL_n(K) = \operatorname{Kern}\det$
4. $A_n \trianglelefteq S_n$ weil $A_n = \operatorname{Kern}\operatorname{sign}$.

## Partitionen

Sei $\phi\colon G \to G'$ ein Homomorphismus. Für jedes Element $h \in H$ betrachte die **Faser** $\phi^{-1}(h) = \{g \in G \mid \phi(g) = h\}$ (Urbild von G in H). Die Fasern bilden eine Partition von G.

**Beispiel 3.** *Sei $\phi\colon \mathbb{C}^* \to \mathbb{R}^*_{>0}, \qquad \phi(z) \mapsto |z|. \qquad$ 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:* "⇒": Falls $\phi(a) = \phi(b)$, dann it $U(a)^{-1}\phi(b) = \phi(a^{-1}b) = 1$, d.h. $\exists n \in N$, s.d. $a^{-1}b = n \implies b = an$.

"⇐" Falls $b = an$ für $n \in N$, dann ist $\phi(b) = \phi(a)\phi(n) = \phi(a)$. □

Aus dem Satz folgt, dass die Fasern von $\phi$ alle von der folgenden Form sind:

$$aN = \{g \in G \mid g = an \text{ für ein } n \in N\}$$

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

*Beweis:* "⇒" klar.

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

## Nebenklassen

**Erinnerung:** Sei $X$ eine Menge. Eine **Äquivalenzrelation** auf $X$ ist eine binäre Relation $\sim$ so dass:

i) (Transitivität) Falls $a \sim b$ und $b \sim c$, dann ist $a \sim c$.

ii) (Symmetrie) Falls $a \sim b$, so ist $b \sim a$.

iii) (Reflexivität) $a \sim a$ für alle $a \in X$.

**Gesehen:** Jede Äquivalenzrelation definiert eine Partition von $X$. Diese besteht aus den **Äquivalenzklassen**, d.h. Teilmengen von der Form $[a] := \{b \in X \mid b \sim a\}$.

Sei $\overline{X}$ die Menge der Äquivalenzklassen. Dann erhalten wir eine surjektive Abbildung $\pi\colon X \to \overline{X}$, $\quad \pi(a) := [a]$. Dann ist $\pi^{-1}([a]) = \{b \in X \mid b \sim a\}$.

**Gesehen:** "Rechnen modulo $m$". $\mathbb{Z}$ mit Äquivalenzrelation $\equiv$, wobei $a \equiv b$ falls $a - b \in m\mathbb{Z}$.

Menge der Äquivalenzklassen: $\mathbb{Z}/m\mathbb{Z}$. $\quad \mathbb{Z}/m\mathbb{Z} = \{[0], [1], \ldots, [m-1]\}$.

Ausserdem können wir die Klassen in $\mathbb{Z}/m\mathbb{Z}$ miteinander addieren, so dass $[a + b] = [a] + [b]$.

$\mathbb{Z}/m\mathbb{Z}$ mit Addition ist somit eine Gruppe, und die Quotientenabbildung $\pi\colon \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, $\quad \pi(n) := [n]$ ist ein Homomorphismus.

**Definition 9.** *Sei $H \leq G$ eine Untergruppe. Eine **Linksnebenklasse** von $H$ ist eine Teilmenge von der Form $aH = \{ah \mid h \in H\}$ für ein $a \in G$.*

**Beispiel 4.** *$m\mathbb{Z}^+ \leq \mathbb{Z}^+$. Dann sind die Linksnebenklassen $m\mathbb{Z}$ die Teilmengen von der Form $0 + m\mathbb{Z}, 1 + m\mathbb{Z}, \ldots, (m-1) + m\mathbb{Z}$.*

Wir schreiben $a \equiv b$, falls ein $h \in H$ existiert, so dass $b = ah$, d.h. falls $b \in aH$.

**Satz 6.** *Die Relation "$\equiv$" ist eine Äquivalenzrelation.*

*Beweis:* 1. Falls $a \equiv b$ und $b \equiv a \implies \exists h, h' \in H$, so dass $b = ah$ und $c = bh' \implies c = a\underbrace{hh'}_{\in H} \implies c \equiv a$.

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

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

$\phi\colon X \to Y$ Abbildung $\phi^{-1}(y) = \{x \in X \mid \phi(x) = y\}$ für $y \in Y$. □

**Korollar 2.** *Die Linksnebenklassen bilden eine Partition von $G$.*

*Beweis:* $aH = bH \Leftrightarrow a \equiv b$. □

**Definition 10.** *Die Anzahl der Linksnebenklassen von $H$ in $G$ ist der sogenannte **Index von** $H$ **in** $G$. Wir schreiben $[G : H]$ für den Index. ($[G : H]$ kann $\infty$ 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 $\phi\colon H \to aH, \qquad \phi(h) = ah.$

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

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

Daraus folgt direkt:

**Korollar 3** (Satz von Lagrange)**.** *Seien $G$ eine Gruppe und $H \leq G$ eine Untergruppe. Dann ist $|H|$ ein Teiler von $|G|$.*

**Bemerkung 10.** *Falls $a \in G$, dann folgt mit Lagrange, dass $|<a>| \mid |G|$, d.h. $Ord(a)$ teilt die Ordnung von $G$.*

**Korollar 4.** *Sei $G$ eine Gruppe, s.d. $|G|$ prim ist. Sei $a \in G, a \neq 1$, dann ist $G = <a>$.*

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

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

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

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

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

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

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

**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, sodass $b = ha$.

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

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

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

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

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

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

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

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

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

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

# Vorlesung 4

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

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

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

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

## Faktorgruppen

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

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

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

$\rightsquigarrow$ Assoziativität der Verknüpfung auf X.

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

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

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

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

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

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

□

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

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

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

*Beweis:* In Vorlesung 3 gesehen:

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

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

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

□

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

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

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

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

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

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

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

*Beweis:*
1. $\overline{\phi}$ ist wohldefiniert: $\phi(an) = \phi(a)\phi(n) = \phi(a)$, d.h. $\overline{\phi}(aN)$ hängt nicht von der Wahl des Repräsentanten ab.
2. $\overline{\phi}$ ist ein Homomorphismus:
$$\begin{aligned}\overline{\phi}((aN)(bN)) &= \overline{\phi}(abN)\\ &= \phi(ab) = \phi(a)\phi(b)\\ &= \overline{\phi}(aN)\overline{\phi}(bN)\end{aligned}$$
3. $\overline{\phi}$ ist bijektiv: $\overline{\phi}$ ist surjektiv, da $\phi$ 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 bestehend aus den Elementen mit Betrag 1. Dann ist der Quotient $\mathbb{C}^*/S^1$ isomorph zu $\mathbb{R}^*_{>0}$. (Wahr)

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

**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:

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

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

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

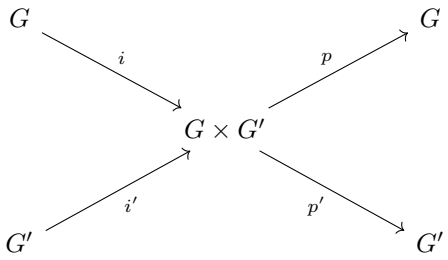
**Erinnerung:** $G, G'$ Gruppen $\rightsquigarrow G \times G'$ ist Gruppe mit Verknüpfung $(a, a')(b, b') = (ab, a'b')$.

**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:




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

**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*

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

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 $\pi$ 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. $h_1 k_1 = h_2 k_2$.

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

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

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

$$\Longrightarrow KH \subseteq HK$$

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

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

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

(ii) $1 \in HK$

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

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

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

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

$$\implies hk = kh$$

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

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

□

**Beispiele**

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

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

*Beweis:* Sei $G$ eine Gruppe mit $|G| = G$. 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 $g \in G$

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

$\pi \colon G \to G/<g>$ 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 hat $(gh)$ Ordnung 6. Das haben wir aber ausgeschlossen. Also ist $hg = gh^2$.

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

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

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

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

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

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

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

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

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

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

Wir haben also insbesondere Homomorphismus $\psi\colon \mathrm{Isom}(R^n) \to O, \psi(t_a d_B) = d_B$.

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

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

# Vorlesung 6

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

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

$\mathcal{T}_n \trianglelefteq \mathrm{Isom}(\mathbb{R}^n)$ 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 $f \in Isom(\mathbb{R}^2)$, $f = t_a d_B$.*

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

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

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

**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 $O' = t_p O t_p^{-1} \leq Isom(\mathbb{R}^n)$*

*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 $\theta$ 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 $\theta$ 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. $\overset{1.Fall}{\implies}$ $\operatorname{Kern}\phi$ ist zyklisch erzeugt von Drehung $\implies G = \operatorname{Kern}\phi + S\operatorname{Kern}\phi$ 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.

$D_n \subseteq \operatorname{Isom}(\mathbb{R}^2)$ bestehend aus allen $g \in \operatorname{Isom}(R^2)$ 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 $\Delta, \Delta'$ sind **kongruent**, falls es ein $g \in$ Isom($\mathbb{R}^2$) gibt, so dass $g\Delta = \Delta'$. Die Bahn $B_\Delta$ ist die Menge aller zu $\Delta$ 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 $\Delta$ ein gleichseitiges Dreieck. Dann ist der Stabilisator von $\Delta$ 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:*
- $\phi$ ist wohldefiniert. Seien $a, b \in G$ s.d. $aH = bH \Leftrightarrow b = ah$ für ein $h \in H \implies bx = a\underbrace{hx}_{x} = ax$.
- $\phi$ ist surjektiv: klar, da $B_x$ genau aus den Elementen der Form $ax$ besteht, $a \in G$.
- $\phi$ 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 $\phi$.

□

**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)

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

□

**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. □

**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 $|B| = [H : H \cap K] \implies [H : H \cap K] \leq |X| = [G : K]$. □

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

$\phi$ 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

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

$\square$

[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:

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

$\implies$ 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 $\mathrm{Bild}\,\phi \leq \mathrm{Sym}(G) \simeq S_n$. □

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

**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 $p^e$.

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

$\Longrightarrow$ es gibt $x \in G\backslash\{1\}$ sodass $x \in Z$. □

**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 $i$. □

**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 $x \in Z \quad \lightning$.

$\Longrightarrow$ $G$ ist abelsch. □

**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 $p^2$. $\Longrightarrow$ $G$ 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. $\implies$ $H_1H_2 \leq G$.

Da $H_1 \lneq H_1H_2$ ist, ist $|H_1H_2| = p^2 \implies H_1H_2 = G$. 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 $\pi$ 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 $N = \bigcup_{x_i \in N} K(x_i)$. $|N|$ teilt 60.

Es folgt:

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

□

**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 $\phi$ 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. □

**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 $\text{Stab}(U) = G_U = \{g \in G \mid gU = U\}$

**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 $\forall x \in U$

$\Leftrightarrow U = \bigcup_{x \in U} B_x$. □

$G \curvearrowright \{\text{Teilmengen von } G\}$ 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 $H$.*

$G \curvearrowright \{\text{Teilmengen von } G\}$ 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 $p \mid |G|$, 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).

$\Longrightarrow$ $G \simeq C_5 \times C_3 \simeq C_1 5$. □

**Satz 35.** *Sei* $G$ *eine Gruppe, sodass* $|G| = 10$*. Dann ist* $G \simeq C_5 \times C_2 \simeq C_1 0$ *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 $H \cap K = \{1\}$

$\implies G \simeq H \times K \simeq C_2 \times C_5 = C_1 0.$

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

**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.

$\implies p \nmid N$. □

**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 $N = |X| = \sum_{B \text{ Bahnen}} |B|$

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. $H_1 H_2$ ist Untergruppe von $G$ und $H_1 H_2$ ist isomorph zu $H_1 \times H_2$, da $H_1 \cap H_2 = \{1\}$.

Per Induktion zeigt man ähnlich, dass $H_1 H_2 \cdots H_s$ 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. □

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. □

**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. □

**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:*

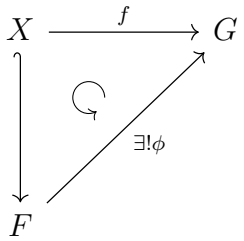
$$aaab^{-1}b^{-1} = a^3b^{-2}$$

**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.*




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

$\phi$ ist wohldefiniert: Zwei äquivalente Wörter werden auf dasselbe Element in $G$ abgebildet.

$\phi$ ist offensichtlich ein Homomorphismus und eindeutig. □

**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 $\phi$ surjektiv.*

$\underset{1.\ Isosatz}{\Longrightarrow} G \simeq F/N$, *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.*

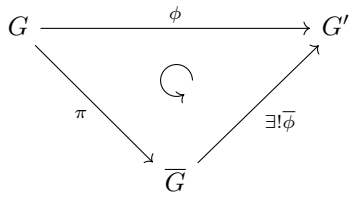
$$N = \bigcap_{\substack{H \trianglelefteq G \\ R \subseteq H}} H$$

$X$ 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 $\overline{\phi} \circ \pi = \phi$.*




*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: $\overline{\phi}(\overline{a})\overline{\phi}(\overline{b}) = \phi(a)\phi(b) = \phi(ab) = \overline{\phi}(\overline{ab})$. □

**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 $\phi$ 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 $G = <x, y | xyx^{-1}y^{-1}>$ 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 $R\backslash\{0\}$ 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 $\phi$ ausserdem bijektiv ist, so ist $\phi$ 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 $\phi$ 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 $\phi$ 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* $\operatorname{Kern}\phi$ *kein 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.* $\implies$ $\operatorname{Bild}\phi \subseteq R'$ *ist ein Unterring.*

*Beweis:* $\operatorname{Bild}\phi$ ist eine Untergruppe, da $\phi$ auch Gruppenhomomorphismus ist.

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

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

$\implies$ abgeschlossen bez. Multiplikation.

$1_{R'} \in \operatorname{Bild}\phi$ 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.

□

**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. □

**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 $\alpha$ enthält.*

**Bemerkung 50.**

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

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

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

**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*

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

*mit der üblichen Addition und Multiplikation.*

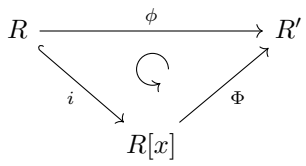
*Elemente von der Form $x_1^{i_1} \cdots x_n^{i_n}$ heissen **Monome**.*

**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 $\Phi$ auf die konstanten Polynome mit $\phi$ übereinstimmt und sodass $\Phi(x_1) = \alpha_i$ für $i = 1, \ldots, n$.*




*Beweis:* Multindex-Schreibweise

$$x = (x_1, \ldots, x_n)$$
$$\alpha = (\alpha_1, \ldots, \alpha_n)$$
$$i = (i_1, \ldots, i_n)$$

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

Falls $\Phi$ 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 $\Phi$ ein Homomorphismus ist). D.h. $\Phi$ 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.

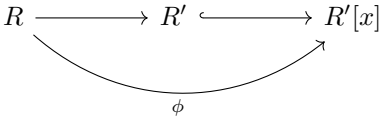
Wir haben:

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

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

und $\Phi(1) = 1$ (per Definition). □

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




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

*$\Phi$ bildet ein Polynom $a_0 + a_1x + \cdots a_nx^n$ 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:* $\operatorname{Kern}\Phi = (p)$*).*

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

**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.* $\Phi$ *auf* $R$ *die Identität ist und* $\Phi$ *die Variablen auf sich selbst abbildet.*

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

**Zu zeigen:** $\Phi$ ist ein Isomorphismus.

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

$\rightsquigarrow \psi$ 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: $\Phi \circ \Psi = \mathrm{id}_{R[x,y]}$ □

# Vorlesung 16

Sei $R$ ein Ring. Es gibt einen eindeutigen Homomorphismus $\phi\colon \mathbb{Z} \to R$ gegeben durch

$\phi(n) = \underbrace{1_R + 1_R + \cdot + 1_R}_{\text{n-mal}}$ falls $n \geq 0$

$\phi(-n) = \underbrace{-(1_R + 1_R + \cdot + 1_R)}_{\text{n-mal}}$

Falls $\psi\colon \mathbb{Z} \to \mathbb{R}$ ein Homomorphismus ist, so ist $\psi(1) = 1_R$

$\Longrightarrow \psi = \phi$, d.h. $\phi$ ist eindeutig.

**Zu zeigen:** $\phi$ ist ein Homomorphismus.

$\phi(m+n) = \phi(m) + \phi(n)$

$\phi(mn) = \underbrace{1_R + 1_R + \cdot + 1_R}_{\text{mn-mal}} = \underbrace{1_R + 1_R + \cdot + 1_R}_{\text{m-mal}} \underbrace{1_R + 1_R + \cdot + 1_R}_{\text{n-mal}} = \phi(m)\phi(n)$

**Definition 45.** $\operatorname{Kern}\phi \subseteq \mathbb{Z}$ *ist Ideal* $\implies \operatorname{Kern}\phi = n\mathbb{Z}$ *für ein* $n \geq 0$. *Dieses* $n$ *ist die* ***Charakteristik*** *von* $R$.

**Gestern:** $R$ Ring $\rightsquigarrow R[x]$

$f \in R[x]$

$f = a_n x^n + \cdots + a_1 x + a_0, \quad a_n \neq 0$

$\deg(f) := n$ heisst der **Grad** von $f$.

$a_n$ ist der **Leitkoeffizient**.

Ist $a_n = 1$, so heisst $f$ **normiert**.

**Beispiel 24.** $f = 2x^3 + x^2 - 1 \in \mathbb{Z}[x]$ *hat Grad 3 und Leitkoeffizient 2.* $f$ *ist nicht normiert.*

**Satz 54.** *Seien* $R$ *ein Ring und* $f, g, \in R[x]$, *s.d. der Leitkoeffizient von* $f$ *eine Einheit ist. Dann gibt es Polynome* $q, r \in R[x]$ *s.d.* $g = fq + r$ *wobei* $\deg(r) < \deg(f)$.

*Beweis:* Induktion über $\deg(g)$.

Falls $\deg(g) < \deg(f)$, dann ist $g = 0f + r$.

Falls $\deg(g) \geq \deg(f) = m$:

Wir schreiben:

$$\begin{aligned} g &= a_0 + a_1 x + \cdots + a_n x^n && a_n \neq 0 \\ f &= b_0 + b_1 x + \cdots + b_m x^m && \substack{b_m \neq 0 \\ b_m \text{ Einheit}} \end{aligned}$$

Sei $g_1 = g - b_m^{-1} a_n x^{n-m} f$

$= a_0 + \cdots + \cancel{a_n x^n} - b_m^{-1} a_n b_0 - \cdots - \cancel{b_m^{-1} a_n b_m x^n}$

d.h. $\deg(g_1) < \deg(g)$

Induktion: $\exists q_1, r_1 \in R[x]$ s.d. $g_1 = fq_1 + r_1 \quad \deg(r_1) < \deg(q_1)$

$g_1 = f(\underbrace{b_m^{-1} a_n x^{n-m} + q_1}_{:=q}) + \underbrace{r_1}_{:=r}$ □

**Korollar 14.** *Sei $g \in R[x]$ und sei $\alpha \in \mathbb{R}$ s.d. $g(\alpha) = 0$. Dann gilt $g = (x-\alpha)q$ für ein $q \in R[x]$.*

*Beweis:* Wir schreiben $g = (x-\alpha)q + r$

$\deg(r) < \deg(x-\alpha) = 1$

$\implies r \in R$

$\implies r = 0$ □

**Bemerkung 55.** *Sei $K$ ein Körper. Jedes $f \in K[x]\backslash\{0\}$ hat eine Einheit als Leitkoeffizient.*

**Satz 55.** *Sei $K$ ein Körper. Jedes Ideal in $K[x]$ ist ein Hauptideal.*

*Beweis:* Sei $I \subseteq K[x]$ ein Ideal.

Falls $I = (0)$ sind wir fertig.

Ansonsten: Sei $f \in I\backslash\{0\}$ vom kleinsten Grad.

Behauptung: $I = (f)$.

Beweis: Sei $g \in I$. Wir schreiben $g = fq + r, \deg(r) < \deg(f)$.

$\implies r = g - fq \in I$

Da aber $\deg(g) < \deg(f)$, folgt $r = 0$.

$\implies g \in (f)$. □

## Restklassenringe

Sei $R$ ein Ring und $I \subseteq R$ ein Ideal.

$\rightsquigarrow I$ ist eine additive Untergruppe mit Nebenklassen $r + I \quad r \in R$.

Die Menge der Nebenklassen $R/I$ bildet eine Gruppe.

$\pi\colon R \to R/I$ ist ein Gruppenhomomorphismus.

**Satz 56.** *(a) Es gibt eine eindeutige Ringstruktur auf $\overline{R} = R/I$ so dass*

$\pi\colon R \to \overline{R}, \quad r \mapsto r + I$ *ein Ringhomomorphismus ist.*

*(b)* $\operatorname{Kern}\pi = I$

*Beweis:* Für $(r+I), (s+I) \in \overline{R}$ definieren wir $(r+I)(s+I) := (rs+I)$

Diese Multiplikation ist wohldefiniert:

Seien u und v jeweils Repräsentanten von $s+I$ und $r+I$.

$\implies$ es gibt $a, b \in I$, s.d. $u = s + a, v = r + b$.

$\implies vu = (r+b)(s+a) = rs + \underbrace{(ra+bs+ba)}_{\in I}$

$\implies vu + I = rs + I$

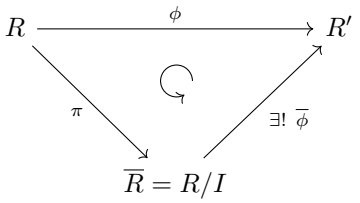
Man überprüfe direkt, dass $\overline{R}$ mit dieser Multiplikation alle Ringaxiome erfüllt und dass $\pi$ ein Homomorphismus mit Kern $I$ ist (kleine Übung).

$R/I$ heisst **Restklassenring** von $R$ modulo $I$ oder auch **Faktorring**. □

# Vorlesung 17

**Gesehen:** Sei $R$ ein Ring, $I \subseteq R$ ein Ideal. $\rightsquigarrow \overline{R} = R/I$ hat eindeutige Ringstruktur, s.d. $\pi\colon R \to \overline{R} \quad r \mapsto r + I$ ein Homomorphismus ist.

**Satz 57** (Abbildungseigenschaft)**.** *Sei $\phi\colon R \to R'$ ein Ringhomomorphismus und $I \subseteq R$ ein Ideal, s.d. $I \subseteq \operatorname{Kern}\phi$. Dann existiert ein eindeutiger Ringhomomorphismus $\overline{\phi}\colon \overline{R} = R/I \to R'$ mit $\overline{\phi} \circ \pi = \phi$*




*Beweis:* Aus der Abbildungseigenschaft für Gruppen folgt, dass ein eindeutiger Gruppenhomomorphismus $\overline{\phi}\colon \overline{R} \to R'$ existiert, s.d. $\phi = \overline{\phi} \circ \pi$, gegeben durch $\overline{\phi}(\overline{a}) := \phi(a)$, $\overline{a} = a + I$. Man überprüfe direkt, dass $\overline{\phi}$ auch ein Ringhomomorphismus ist. □

**Beispiel 25.** *$\phi\colon \mathbb{Z} \hookrightarrow \mathbb{Q}$, $\phi(n\mathbb{Z}) \subseteq \mathbb{Q}$ ist kein Ideal, falls $n \neq 0$.*

**Behauptung 3** (Clicker-Frage)**.** *Sei $\phi\colon R \to R'$ ein surjektiver Homomorphismus mit $I \subseteq R$ Ideal $\implies \phi(I) \subseteq R'$ ist Ideal.*

*Beweis:* $\phi(I) \subseteq R'$ ist eine additive Untergruppe (da es das Bild einer Untergruppe unter $\phi$ ist).

Sei $r' \in R'$ und $a' \in \phi(I)$

$\implies \exists r \in R$ und $a \in I$ s.d. $\phi(r) = r'$ und $\phi(a) = a'$

$\implies r'a' = \phi(r)\phi(a) = \phi(ra) \in \phi(I)$ □

**Behauptung 4** (Clicker-Frage)**.** *Seien $\phi\colon R \to R'$ ein Homomorphismus und $J \subseteq R'$ ein Ideal. Dann gilt: $\phi^{-1}(J) \subseteq R$ ist ein Ideal.*

*Beweis:* Seien $a, b \in \phi^{-1}(J)$

$\implies \phi(a+b) = \phi(a) + \phi(b) \in J$

$\implies a + b \in \phi^{-1}(J), \quad 0 \in \phi^{-1}(J)$

Sei $r \in R$

$\implies \phi(ra) = \phi(r)\phi(a) \in J$

$\implies ra \in \phi^{-1}(J).$ □

**Satz 58** (Entsprechungssatz)**.** *Sei $R$ ein Ring, $I \subseteq R$ ein Ideal, $\pi\colon R \to R/I = \overline{R}$ Quotient.*

*Dann gilt:*

*(a) Die Abbildung $\Phi\colon \{$Ideale $J \subseteq R \mid I \subseteq J\} \to \{$Ideale in $R\}$*

*$J \mapsto \pi(J)$ ist eine Bijektion $\pi^{-1}(H) \leftarrow H$.*

*(b) Falls $J \subseteq R$ ein Ideal ist mit $I \subseteq J$, so gilt $R/J \simeq \overline{R}/\pi(J)$*

*Beweis:* (a) $\pi(J) \subseteq R$ ist ein Ideal, da $\pi$ surjektiv ist. Ist $H \subseteq \overline{R}$ ein Ideal, so ist $\pi^{-1}(H) \subseteq R$ ein Ideal, das $I$ enthält (da $\pi^{-1}(0) = I$). D.h., beide Abbildungen sind wohldefiniert.

**Z.z:**

- $\pi^{-1}(\pi(J)) = J$ und
- $\pi(\pi^{-1}(H)) = H$

für alle $I \subseteq R$ und $H \subseteq \overline{R}$.

Wir haben $\pi(\pi^{-1}(H)) = H$, da $\pi$ surjektiv ist.

Ausserdem gilt $\pi^{-1}(\pi(J)) \supseteq J$.

Sei $x \in \pi^{-1}(\pi(J))$, d.h. $\pi(x) \in \pi(J)$

$\implies \exists y \in J$ s.d. $\pi(x) = \pi(y)$.

$\implies \pi(x - y) = 0$

$\implies x - y \in \operatorname{Kern} \pi = I$.

Da $y \in J$ und $x - y \in I \subseteq J$, folgt $x = (x - y) + y \in J$

$\implies \pi^{-1}(\pi(J)) = J$

(b) Sei $\phi\colon \overline{R} \to \overline{R}/\pi(J)$ Quotient.

Man betrachte $R \xrightarrow{\pi} \overline{R} \xrightarrow{\phi} \overline{R}/\pi(J)$.

Dann ist $\operatorname{Kern} \pi \circ \phi = \pi^{-1}(\pi(J)) \overset{(a)}{=} J$

$\implies \overline{R}/\pi(J) \simeq R/J.$

□

Sei $R$ ein Ring und $a \in R$. Wir können $R/(a)$ interpretieren als den Ring, in welchem zusätzlich die Relation $a = 0$ gilt.

**Beispiel 26.** *$R = \mathbb{Z}$ und ausserdem soll gelten $3 \cdot 4 = 1 \Leftrightarrow 11 = 0$.*

$\rightsquigarrow \mathbb{Z}/(11) = \mathbb{Z}/11\mathbb{Z}$.

**Beispiel 27.** *Sei $R = \mathbb{Z}[i]$ der Ring der Gaussschen Zahlen. Sei $\overline{R}$ der Ring, den man durch Einführung der Relation $1+3i = 0$ erhält, d.h. $\overline{R} = \mathbb{Z}[i]/(1+3i)$.*

*Wir haben $-i(1 + 3i) \in (1 + 3i)$,*

*d.h. in $\overline{R}$ gilt $\overline{-i}(\overline{1} + \overline{3i}) = 0$*

$\implies \overline{-i} + \overline{3} = 0$

*d.h. in $\overline{R}$ gilt $\overline{i} = \overline{3}$*

$\implies \overline{1} + \overline{3i} = \overline{1} + \overline{9} = \overline{10} = 0$

**Behauptung 5.** $\overline{R} := \mathbb{Z}[i]/(1 + 3i) \simeq \mathbb{Z}/10\mathbb{Z}$

*Beweis:* Man betrachte den Homomorphismus $\phi\colon \mathbb{Z} \to \overline{R}$ (es gibt genau einen).

Jedes Element in $\overline{R}$ ist von der Form $\overline{a} + \overline{bi} = \overline{a} + \overline{b}\overline{3}$ für $a, b \in \mathbb{Z}$

$\implies \phi$ ist surjetktiv.

Da $\overline{10} = 0$ gilt in $\overline{R}$, folgt $10\mathbb{Z} \subseteq \operatorname{Kern}\phi$.

Sei $n \in \operatorname{Kern}\phi$. Dann ist $n \in (1 + 3i) \subseteq \mathbb{Z}[i]$,

d.h. $\exists a, b \in \mathbb{Z}$ sodass $n = (a + bi)(1 + 3i) = (a - 3b) + \underbrace{(3a + b)}_{=0} i$

$\implies b = -3a$

$\implies n = a(1 + 3i)(1 + 3i) = 10a \implies n \in 10\mathbb{Z}$

$\implies \operatorname{Kern}\phi = 10\mathbb{Z}$

$\implies \overline{R} \simeq \mathbb{Z}/\operatorname{Kern}\phi = \mathbb{Z}/10\mathbb{Z}$ □

## Adjunktion von Elementen

Hinzufügen von Elementen zu einem Ring, die bestimmte Relationen erfüllen.

**Beispiel 28.** *$\pi\colon \mathbb{R}[x] \to \mathbb{C}$ s.d. $\pi/\mathbb{R}\colon \mathbb{R} \hookrightarrow \mathbb{C}$ und $\pi(x) = i$.*

*Dann ist* $\operatorname{Kern}\pi = (x^2 + 1)$.

*(<u>Beweis</u>* $(x^2 + 1) \subseteq \operatorname{Kern}\pi$*:*

*Falls* $f \in \mathbb{R}[x]$ *s.d.* $f(i) = 0 \implies (x-i) \big| f$ *aber auch* $f(-i) = 0 \implies (x+i) \big| f$ $\implies (x^2+1) \big| f \implies f \in (x^2+1)$*.)*

$\implies \mathbb{C} \simeq \mathbb{R}[x]/(x^2+1)$

**Allgemein:** Sei $S$ ein Ring, $R \subseteq S$ Unterring, $\alpha \in S$.

Man betrachte $\pi \colon R[x] \to R[\alpha]$ sodass $\pi/R$ bildet $R$ auf $R$ ab und $\pi(x) = \alpha$.

Dann ist $R[\alpha] \simeq R[x]/\operatorname{Kern} \pi$.

Sei $R$ ein Ring und $f \in R[x]$. $f = c_n x^n + \cdots + c_0$.

Wir bezeichnen mit $\alpha$ die Restklasse von $x$ modulo $(f)$. Dann erfüllt $\alpha$ in $R[x]/(f)$ die Relation

$$\overline{c}_n \alpha^n + \overline{c}_{n-1} \alpha^{n-1} + \cdots + \overline{c}_0 = 0$$

wobei $\overline{c}_i$ die Restklasse von $c_i$ modulo $(f)$ ist.

**Definition 46.** *Oft bezeichnet man den Ring* $R[x]/(f)$ *durch* $R[\alpha]$ *und man nennt ihn den Ring, den man durch* ***Adjunktion*** *von* $\alpha$ *zu* $R$ *erhält.*

**Satz 59.** *Seien* $R$ *ein Ring und* $f \in R[x]$ *ein normiertes Polynom, s.d.* $\deg f =: n > 0$*. Dann ist die Abbildung*

$\Phi \colon R^n \to R[\alpha] = R[x]/(f)$

$(r_0, \ldots, r_{n-1}) \mapsto r_0 + r_1 \alpha + \cdots + r_{n-1} \alpha^{n-1}$

*eine Bijektion.*

*Beweis:* Jedes Element in $R[\alpha]$ ist von der Form $g(\alpha)$ für ein $g(x) \in R[x]$.

Division mit Rest:

$g(x) = f(x)q(x) + r(x)$ mit $\deg r(x) < \deg f(x)$.

Da $f(\alpha) = 0$, folgt $g(\alpha) = r(\alpha) \implies \Phi$ surjektiv.

Um zu zeigen, dass $\Phi$ injektiv ist, zeigen wir

$r_0 + r_1 \alpha + \cdots + r_{n-1} \alpha^{n-1} \neq 0$ für alle $r_0, \ldots, r_{n-1} \in R$, nicht alle null.

Dazu zeigen wir, dass $(f) \backslash \{0\}$ keine Elemente von Grad $< n$ enthält.

Sei $g \in (f) \backslash \{0\}$. Dann ist $g = hf$ für ein $h \in R[x]$

$h = b_0 + \cdots + b_m x^m, b_m \neq 0$

$\implies hf = b_m x^{m+n} + \cdots$

$\implies \deg g = \deg(hf) \geq n.$ □

**Beispiel 29.** $\mathbb{Z}[\alpha] = \mathbb{Z}[x]/(x^3 + 3x + 1)$

$\underset{Satz}{\Longrightarrow}$ *Jedes Element in* $\mathbb{Z}[\alpha]$ *ist von der Form* $r_0 + r_1\alpha + r_2\alpha^2, \quad r_i \in \mathbb{Z}$.

*Wir haben z.B.*

$$(2 + \alpha - \alpha^2) + (1 + \alpha) = 3 + 2\alpha - \alpha^2$$

$$\begin{aligned}(2 + \alpha - \alpha^2)(1 + \alpha) &= 2 + 3\alpha - \alpha^3 \\ &= \underbrace{(1 + 3\alpha + \alpha^3)(-1)}_{=0} + (3 + 6\alpha) \\ &= 3 + 6\alpha\end{aligned}$$

Wir nutzen meist normierte Polynome, um leicht verständliche Ringe zu erhalten. Hier ein Beispiel mit einem nicht normierten Polynom:

**Beispiel 30.** *Für* $a \in R$ *betrachten wir* $R[x]/(ax - 1) = R[\alpha]$

*Dann ist* $a\alpha = 1$, *d.h.* $a$ *ist invertierbar in* $R[\alpha]$.

*Sei* $\beta \in R[\alpha]$. *Wir schreiben*

$$\beta = r_0 + r_1\alpha + \cdots + r_m\alpha^m$$

*für ein* $m \geq 0$. *Dann ist* $\beta = \alpha^m(r_0a^m + r_1a^{m-1} + \cdots + r_m)$.

*Das heisst, Elemente in* $R[\alpha]$ *sind von der Form* $\alpha^k r$ *für* $r \in R, k \geq 0$.

**Beispiel 31** (Spezialfall)**.** $R = K[t]$. *Wir betrachten* $' = K[t, x]/(xt - 1)$.

*Dann ist* $R'$ *der Ring der* ***Laurentpolynome****, d.h. Polynome in* $t$ *und* $t^{-1}$.

$$f(t) = \sum_{i=-n}^{n} a_i t^i = t^{-n} \left( \sum_{i=-m}^{n} a_i t^{i+n} \right)$$

*Wir bezeichnen oft* $R' = K[t, t^{-1}]$.

# Vorlesung 18

**Gestern:** Sei $R$ ein Ring.

$R[\alpha] = R[x]/(f)$ mit $f \in R[x]$. $\alpha$ ist die Restklasse von $x$.

Dies nennen wir die Adjunktion von $\alpha$ zu $R$, s.d. $\alpha$ die Relation $f(\alpha) = 0$ erfüllt.

**Beispiel 32.** $f = x^2$

$\Longrightarrow$ $R[\alpha] = R + R\alpha$ *und es gilt* $\alpha^2 = 0$.

Der Homomorphismus $\phi\colon R \to R[\alpha]$ ist nicht immer injektiv.

Falls $f$ normiert ist, so ist $\phi$ inkektiv (folgt aus dem Satz von gestern).

Im Allgemeinen ist $\operatorname{Kern}\phi = R \cap (f)$.

**Beispiel 33.** $R[x]/(x \cdot 0 - 1) = 0$

## Integritätsbereiche & Quotientenkörper

Sei $R$ ein Ring.

**Definition 47.** *Ein $a \in R\backslash\{0\}$ heisst **Nullteiler**, falls ein $b \in R\backslash\{0\}$ existiert, s.d. $ab = 0$.*

**Beispiel 34.** *In $\mathbb{Z}/10\mathbb{Z}$ gilt $\overline{5} \cdot \overline{2} = \overline{0}$.*

**Definition 48.** *Ein **Integritätsbereich** (IB) ist ein Ring $R$, der nicht der Nullring ist und der keine Nullteiler enthält.*

D.h. in einem IB gilt $1 \neq 0$ und aus $ab = 0$ folgt immer $a = 0$ oder $b = 0$.

**Beispiel 35.** *Jeder Unterring von einem Körper ist ein IB.*

**Bemerkung 56.** *Sei $R$ ein IB. Falls $ab = ac$ für ein $a \neq 0$, so folgt $b = c$.*

*Beweis:* $ab = ac \implies a(b-c) = 0 \implies (b-c) = 0 \implies (b = c)$ □

**Satz 60.** *Sei $R$ ein IB, dann ist auch $R[x]$ ein IB.*

*Beweis:* Seien $f, g \in R[x]\backslash\{0\}$. Wir schreiben

$$f = a_0 + \cdots + a_n x^n \qquad a_n \neq 0$$
$$g = b_0 + \cdots + b_m x^m \qquad b_m \neq 0$$

$$\implies fg = \underbrace{a_n b_n}_{\neq 0 \text{da } R \text{ IB}} x^{m+n} + \cdots$$

$$\implies fg \neq 0$$ □

**Satz 61.** *Sei $R$ ein IB mit endlich vielen Elementen, dann ist $R$ ein Körper.*

*Beweis:* Sei $a \in R\backslash\{0\}$.

Man betrachte: $m_a\colon R\backslash\{0\} \to R\backslash\{0\}$

$b \mapsto ab$

Falls $ab = ac$, so ist $b = c$, d.h. $m_a$ ist injektiv.

$\underset{R \text{ endlich}}{\implies}$ $m_a$ ist surjektiv.

$\implies \exists b \in R$ s.d. $m_a(b) = ab = 1$

$\Longrightarrow$ $a$ ist eine Einheit. $\square$

**Satz 62.** *Sei $R$ ein IB. Dann gibt es einen Körper $K$ und einen injektiven Ringhomomorphismus $i\colon R \hookrightarrow K$.*

**Beispiel 36.** $\mathbb{Z} \hookrightarrow \mathbb{Q}$

*Beweis/Konstruktion.* Ein **Bruch** ist ein Symbol $\frac{a}{b}$, wobei $a, b \in R$ und $b \neq 0$.

Wir definieren $\frac{a_1}{b_1} \approx \frac{a_2}{b_2}$, falls $a_1 b_2 = a_2 b_2$.

Dies ist eine Äquivalenzrelation.

Reflexivität und Symmetrie sind klar.

Transitivität:

Falls $\frac{a_1}{b_1} \approx \frac{a_2}{b_2} \approx \frac{a_3}{b_3}$

$\Longrightarrow$ $a_1 b_2 = a_2 b_1$ und $a_2 b_3 = b_2 a_3$

$\Longrightarrow$ $a_1 b_2 b_3 = a_2 b_1 b_3 = a_3 b_2 b_1$

$\underset{b_2 \neq 0}{\Longrightarrow}$ $a_1 b_3 = a_3 b_1$

$\Longrightarrow$ $\frac{a_1}{b_1} \approx \frac{a_3}{b_3}$.

Der **Quotientenkörper** $K$ von $R$ ist die Menge der Äquivalenzklassen von Brüchen. Wir schreiben $\frac{a_1}{b_1} = \frac{a_2}{b_2}$, falls $\frac{a_1}{b_1} \approx \frac{a_2}{b_2}$.

Wir definieren Addition und Multiplikation auf $K$.

$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$

$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$

**Zu überprüfen:**

- Addition und Multiplikation sind wohldefiniert.
- Alle Körperaxiome sind erfüllt.

$\rightsquigarrow$ kleine Übung.

Wir haben ausserdem

$i\colon R \to K$

$a \mapsto \frac{a}{1}$

Dies ist ein Ringhomomorphismus (klar)

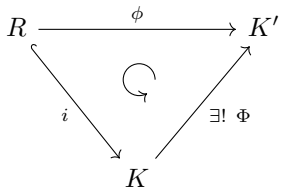
und inketiv: $\frac{a}{1} = \frac{b}{1} \Leftrightarrow a \cdot 1 = b \cdot 1$. $\square$

**Beispiel 37.** *Sei $K$ ein Körper. Der Quotientenkörper $K(x)$ von $K[x]$ heisst* ***Körper der rationalen Funktionen*** *in $x$ über $K$.*

$K(x) = \left\{ \ddot{A}quivalenzklassen\ \frac{f}{g},\ wobei\ f, g \in K[x], g \neq 0 \right\}$

# Vorlesung 19

**Satz 63.** *Sei $R$ ein IB mit Quotientenkörper $K$. Sei $K'$ ein Körper und $\phi\colon R \to K'$ ein injektiver Homomorphismus. Dann gibt es einen eindeutigen Homomorphismus $\Phi\colon K \to K'$ s.d. $\phi = \Phi \circ i$.*




*Beweis:* Wir definieren $\Phi(\frac{a}{b}) := \phi(a)\phi(b)^{-1}$

$\Phi$ ist eindeutig.

$\Phi$ ist wohldefiniert:

Falls $\frac{a_1}{b_1} \approx \frac{a_2}{b_2} \implies a_1 b_2 = b_1 a_2$

$$\begin{aligned} \implies \phi(a_2)\phi(b_1) &= \phi(a_1)\phi(b_2) \\ \implies \Phi\left(\frac{a_2}{b_2}\right) &= \phi(a_2)\phi(b_2)^{-1} \\ &= \phi(a_1)\phi(b_1)^{-1} \\ &= \Phi\left(\frac{a_1}{b_1}\right) \end{aligned}$$

Man überprüft direkt, dass das ein Homomorphismus ist. □

## Maximale Ideale

**Definition 49.** *Sei $R$ ein Ring. Ein Ideal $I \subseteq R$ ist* ***maximal****, falls $I \neq R$ und falls $I$ in keinem anderen Ideal ausser $I$ und $R$ enthalten ist.*

**Beispiel 38.** *Sei $K$ ein Körper. Dann ist $(0) \subseteq K$ maximal.*

**Beispiel 39.** *Die maximalen Ideale in $\mathbb{Z}$ sind die Ideale von der Form $p\mathbb{Z}$ für $p$ prim.*

*Beweis:* Alle Ideale in $\mathbb{Z}$ sind von der Form $n\mathbb{Z}$.

Wir haben $n\mathbb{Z} \subseteq m\mathbb{Z} \Leftrightarrow m \big| n$.

D.h. falls $p\mathbb{Z} \subseteq n\mathbb{Z}$, so gilt $n \big| p \implies n = p$ oder $n = 1$. □

**Satz 64.** *Ein Ideal $I \subseteq R$ ist maximal $\Leftrightarrow$ $R/I$ ist ein Körper.*

*Beweis:* $R/I$ ist ein Körper $\Leftrightarrow$ $R/I$ hat genau zwei Ideale: (0) und $R/I$.

Entsprechungssatz:

$\{$ Ideale $I \subseteq R$ s,d $I \subseteq J\} \overset{1:1}{\leftrightarrow} \{$ Ideale in $R/I\}$

d.h. $R/I$ hat genau zwei Ideale $\Leftrightarrow$ I ist maximal. □

**Beispiel 40.** *$\mathbb{Z}/n\mathbb{Z}$ ist ein Körper $\Leftrightarrow$ $n$ ist prim.*

**Satz 65.** *Die maximalen Ideale in $\mathbb{C}[x]$ sind die Hauptideale von der Form $(x-a), a \in \mathbb{C}$.*

**Bemerkung 57.** *$(x-a)$ ist genau der Kern des Einsetzungshomomorphismus $e_a \colon \mathbb{C}[x] \to \mathbb{C} \quad f \mapsto f(a)$*

*D.h. es gibt eine Bijektion*

$$\begin{aligned} \mathbb{C} &\xrightarrow{\sim} \{\textit{maximale Ideale in } \mathbb{C}[x]\} \\ a &\mapsto \operatorname{Kern} e_a \end{aligned}$$

*Beweis:* Sei $I \subseteq \mathbb{C}[x]$ maximal. Gesehen: $I = (f)$, wobei $f \in I$ von minimalem Grad in $(f)$ ist. Da $(0) \neq I \neq \mathbb{C}[x]$, ist $f$ nicht konstant.

$\implies \exists a \in \mathbb{C}$ s.d. $f(a) = 0$

$\implies x - a \big| f$

$\implies f \in (x-a)$

$\implies I \subseteq (x-a)$

$\underset{I \text{ maximal}}{\implies} I = (x-a)$

Umgekehrt:

$\mathbb{C}[x]/(x-a) = \mathbb{C}[x]/\operatorname{Kern} e_a \simeq \mathbb{C} \implies (x-a)$ ist maximal (da $\mathbb{C}$ ein Körper ist). □

**Beispiel 41.** *$(x^2+1) \subseteq \mathbb{R}[x]$ ist maximal, da $\mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}$*

**Beispiel 42.** *Sei $(a_1, \ldots, a_n) \in \mathbb{C}^n$, dann ist das Ideal $(x_1 - a_1, \ldots, x_n - a_n) \subseteq \mathbb{C}[x_1, \ldots, x_n]$ maximal.*

*Beweis:* Übung. □

**Satz 66** (Hilbert Nullstellenstatz)**.** *Jedes maximale Ideal in* $\mathbb{C}[x_1, \ldots, x_n]$ *ist von dieser Form.*

*Beweis:* Siehe Artin. □

Das ist der Beginn der Algebraischen Geometrie.

Geometrie von $\mathbb{C}^n \leftrightarrow$ maximale Ideale in $\mathbb{C}[x_1, \ldots, x_n]$

**Satz 67.** *Sei* $R$ *ein Ring. Jedes Ideal* $I \subseteq R, I \neq (1)$ *ist in einem maximalen Ideal enthalten.*

*Beweis:* Siehe Übungen. Benötigt Lemma von Zorn / Auswahlaxiom. □

**Definition 50.** *Ein Ideal* $I \subseteq R$ *heisst* ***Primideal****, falls* $I \neq (1)$ *und falls für alle* $a, b \in R$ *gilt: falls* $ab \in I$*, so ist* $a \in I$ *oder* $b \in I$*.*

**Übung:** $I \subseteq$ ist Primideal $\Leftrightarrow R/I$ ist Integritätsbereich.

## Faktorzerlegung

### Ganze Zahlen

Gesehen: Jedes Ideal in $\mathbb{Z}$ ist von der Form $n\mathbb{Z}$ für $n \in \mathbb{Z}_{\geq 0}$.

Wir haben:

$$\begin{aligned} a\mathbb{Z} + b\mathbb{Z} &= \{ar + bs \mid r, s \in \mathbb{Z}\} \\ &= d\mathbb{Z} \text{ für ein } d \in \mathbb{Z}_{\geq 0} \end{aligned}$$

$d$ heisste der **grösste gemeinsame Teiler** von $a$ und $b$. Wir schreiben $d = \mathrm{ggT}(a, b)$.

**Satz 68.** $a, b \in \mathbb{Z}_{\geq 0}, d = \mathrm{ggT}(a, b)$*. Dann gilt:*

*(a)* $\exists r, s \in \mathbb{Z}$ *s.d.* $d = ar + bs$

*(b)* $d \mid a$ *und* $d \mid b$

*(c) Sei* $e \in \mathbb{Z}$ *sodass* $e \mid a$ *und* $b \mid a$*, dann gilt* $e \mid d$*.*

*Beweis:* (a) Klar, da $d \in a\mathbb{Z} + b\mathbb{Z}$

(b) folgt, da $a, b \in d\mathbb{Z}$

(c) $e \mid a$ und $e \mid b$

$\implies a, b \in e\mathbb{Z}$

$\implies ar + bs \in e\mathbb{Z}$ für alle $r, s \in \mathbb{Z}$

$\implies d \in e\mathbb{Z}$.

□

**Lemma 5.** *Seien $p \in \mathbb{Z}$ eine Primzahl und $a, b \in \mathbb{Z}$. Falls $p \mid ab$, dann gilt entweder $p \mid a$ oder $p \mid b$.*

*Beweis:* Man nehme an $p \mid ab$, aber $p \nmid a$.

$\implies \text{ggT}(p, a) = 1$

$\implies \exists r, s \in \mathbb{Z}$ s.d. $rp + sa = 1$

$\implies \underbrace{rpb + sab}_{\text{durch } p \text{ teilbar}} = b$

$\implies p \mid b.$ □

**Satz 69.** *Sei $a \in \mathbb{Z}, a \neq 0$. Dann gibt es ein $k \geq 0$ und Primzahlen $p_1, \ldots, p_k > 0$ s.d. $a = cp_1 \cdots p_k$ mit $c = \pm 1$.*

*Diese Faktorisierung ist eindeutig (bis auf die Reihenfolge der Primfaktoren).*

*Beweis:* Induktion über $a$.

Anfang: $a = 1$ stimmt (keine Primfaktoren).

Induktionsschritt:

Falls $a$ prim ist, sind wir fertig.

Sonst $a = bb'$ für $b, b' < a$.

$\underset{\text{IH}}{\implies} b$ und $b'$ haben Primfaktorisierung.

$\implies a$ hat eine solche Faktorisierung.

Eindeutigkeit: Man nehme an $\pm p_1 \cdots p_n = \pm q_1 \cdots q_m$ zwei solche Faktorisierungen.

Vorzeichen stimmen überein.

Wir haben $p_1 \mid q_1 \cdots q_m$

$\underset{p_1 \text{ prim}}{\implies} p_1 \mid q_i$ für ein $i$. oBdA $i = 1$.

$\implies p_1 = q_1 \implies p_2 \cdots p_n = q_2 \cdots q_m$ durch Induktion über $n$. □

Kleine Übung: Analoge Resultate gelten für $K[x]$ wenn $K$ ein Körper ist.

## Faktorielle Ringe

**Definition 51.** *Seien $R$ ein IB und $a, b \in R$.*

- *$a$ **teilt** $b$, falls $b = aq$ für ein $q \in R$. Wir schreiben $a \mid b$.*
- *$a$ ist ein **echter Teiler** von $b$, falls $b = aq$, sodass weder $a$ noch $q$ eine Einheit sind.*
- *$a$ und $b$ sind **assoziiert**, falls $a \mid b$ und $b \mid a$.*
- *$a$ ist **irreduzibel**, falls $a$ keine Einheit ist, $a \neq 0$ und falls $a$ keine echten Teiler hat.*
- *$p \in R$ ist ein **Primelement**, falls $p$ keine Einheit ist, $p \neq 0$, und falls $p \mid ab$, so gilt $p \mid a$ oder $p \mid b$.*

**Bemerkung 58.** *$a$ und $b$ sind assoziiert $\Leftrightarrow b = ua$ für eine Einheit $u$.*

*Beweis:* " $\Longrightarrow$ "

$a = qb$ und $b = q'a$

$\Longrightarrow a = qq'a$

$\Longrightarrow 1 = qq'$, d.h. $q$ ist eine Einheit.

" $\Longleftarrow$ " klar. □

**Bemerkung 59.**

- *$a$ teilt $b \Leftrightarrow (a) \supseteq (b)$*
- *$a$ ist ein echter Teiler von $b \Leftrightarrow (b) \subsetneq (a) \subsetneq (1)$*
- *$a$ und $a'$ sind assoziiert $\Leftrightarrow (a) = (a')$*
- *$a$ ist irreduzibel $\Leftrightarrow (a) = (0), (a) \subsetneq (1)$ und es gibt kein Hauptideal $(c)$, sodass $(a) \subsetneq (c) \subsetneq (1)$.*
- *$p \neq 0$ ist prim $\Leftrightarrow$ aus $ab \in (p)$ folgt $a \in (p)$ oder $b \in (p)$.*

  *$\Leftrightarrow (p)$ ist Primideal.*

**Bemerkung 60.** *Falls $p \in R$ prim ist, so ist $p$ auch irreduzibel.*

*Beweis:* Falls $p = ab \Longrightarrow p \mid a$ oder $p \mid b$.

oBdA $p \mid b$.

$\Longrightarrow b = rp$ für $r \in R$

$\Longrightarrow p = arp$

$\Longrightarrow 1 = ar$

$\Longrightarrow a$ ist Einheit, d.h. $p$ hat keine echten Teiler. □

# Vorlesung 20

Sei $R$ ein Integritätsbereich.

(1) Können wir jedes $a \in R$ als Produkt von irreduziblen Elementen schreiben?

(2) Falls ja, ist diese Zerlegung eindeutig?

Wir müssen annehmen, dass $a \neq 0$ und $a$ keine Einheit ist.

Idee zu (1): $a \in R, a \neq 0, a$ keine Einheit. Falls $a$ irreduzibel ist, sind wir fertig.

Ansonsten ist $a = a_1 b_1, a_1, b_1$ keine Einheit.

Wir wiederholen diesen Prozess nun mit $a_1$ und $b_1$.

Endet dieser Prozess für alle $a \in R, a \neq 0, a$ keine Einheit, so sagen wir, dass in $R$ **Faktorisierung** endet.

**Satz 70.** *Sei $R$ ein Integritätsbereich. Die folgenden Bedingungen sind äquivalent:*

*(a) Faktorisierung endet in $R$*

*(b) $R$ enthält keine unendliche aufsteigende Kette von Hauptidealen: $(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots$*

*Beweis:* Man nehme an, $R$ hat eine solche Kette $(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots$

Dann ist $(a_n) \subsetneq (1) \forall n$, d.h. $a_n$ ist ein echter Teiler von $a_{n-1}$, d.h. $a_{n-1} = a_n b_n$, $a_n, b_n$ keine Einheiten.

$\implies a_1 = a_2 b_2 = a_3 b_3 b_2 = a_4 b_4 b_3 b_2$

$\implies$ Faktorisierung endet nicht in $R$.

Umgekehrt liefert eine solche unendliche Folge von Zerlegungen $a_1 = a_2 b_2 = a_3 b_3 b_2 = \cdots$ eine unendliche Folge von Hauptidealen. Dann haben wir eine unendliche Kette $(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \cdots$ □

**Beispiel 43.** *Man nehme den Polynomring $K[x_1]$ und anjungiere alle $2^k$-ten Wurzeln von $x_1$ zu $K[x_1]$:*

$K[x_1, x_2, x_3, \ldots]/(\{x_k^{2^k} - x_1 \mid k \geq 2\})$

*In R:*

$$x_1 = x_2^2 = x_3^4 = x_4^8 = \cdots$$

*das heisst*

$$(x_1) \subsetneq (x_2) \subsetneq (x_3) \subsetneq \cdots$$

$\rightsquigarrow$ *In der Praxis treten solche Ringe selten auf.*

Falls eine Faktorisierung in irreduzible Elemente existiert, so ist diese nicht immer eindeutig.

**Beispiel 44.** $\mathbb{Z}[\sqrt{-5}] \subseteq \mathbb{C}$

$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$

*Man kann zeigen:* $2, 3, 1 + \sqrt{-5}, 1 - \sqrt{-5}$ *sind alle irreduzibel in* $\mathbb{Z}[\sqrt{-5}]$.

**Definition 52.** *Sei $R$ ein IB. $R$ heisst **faktoriell**, wenn Folgendes erfüllt ist:*

*(i) Faktorisierung endet*

*(ii) Die Faktorisierung in irreduzible Faktoren ist eindeutig im folgenden Sinn:*

*Falls $a \neq 0, a$ keine Einheit, geschrieben werden kann als*

$$a = p_1 \cdots p_m = q_1 \cdots q_n$$

*für irreduzible $p_i$ und $q_i$ ist $m = n$ und — nach Umordnung der Faktoren — ist $p_i$ assoziiert zu $q_i$ für $i = 1, \cdots, n$.*

**Satz 71.** *Sei $R$ ein IB, in dem Faktorisierung endet. Dann ist $R$ faktoriell $\Leftrightarrow$ jedes irreduzible Element ist prim.*

*Beweis:* " $\Longleftarrow$ " Man nehme an, jedes irreduzible Element ist auch prim. Sei $a \in R$ und seien

$$a = p_1 \cdots p_m = q_1 \cdots q_n$$

zwei Zerlegungen in irreduzible Elemente.

Falls $n = 1$,so ist auch $m = 1$ und $p_1 = q_1$ (da $p_1$ irreduzibel).

Falls $n > 1$: $p_1$ ist prim, d.h. $p_1 \big| q_i$ für ein $i$. OBdA $i = 1$.

Da $q_1$ irreduzibel ist, folgt, dass $p_1$ und $q_1$ assoziiert sind.

$\underset{\text{kürzen}}{\rightsquigarrow} p_2 \cdots p_n = q_2 \cdots q_m$.

Behauptung folgt per Induktion über $n$.

" $\Longrightarrow$ " Man nehme an, es gibt ein $p \in R$, das irreduzibel aber nicht prim ist.

$\Longrightarrow \exists a, b \in R$, s.d. $p \big| ab$ aber $p \nmid a$ und $p \nmid b$.

Das heisst, $pc = ab$ für ein $c \in R$. Faktorisiere $a, b, c$ in irreduzible Faktoren $c = c_1 \cdots c_r$, $a = a_1 \cdots a_m$, $b = b_1 \cdots b_n$.

$\rightsquigarrow pc_1 \cdots c_r = a_1 \cdots a_m b_1 \cdots b_n$ sind zwei verschiedene Faktorisierungen $\Longrightarrow R$ ist nicht faktoriell. $\square$

# Vorlesung 21

### Letzte Woche

Sei $R$ ein Integritätsbereich

- $r \in R$ ist **irreduzibel**, falls $r$ keine echten Teiler hat, d.h. falls $r = ab \implies$ $a$ oder $b$ ist eine Einheit
- $r \in R$ ist **prim**, falls aus $r \mid ab$ folgt, dass $r \mid a$ oder $r \mid b$.

prim $\implies$ irreduzibel, aber im Allgemeinen irreduzibel $\not\impliedby$ prim.

**Beispiel 45.** $\mathbb{Z}[\sqrt{-5}], 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$

$\rightsquigarrow$ *2 ist irreduzibel aber nicht prim, da* $2 \nmid (1+\sqrt{-5}), 2 \nmid (1-\sqrt{-5})$

Ein IB $R$ ist **faktoriell**, falls jedes $r \in R$ *eindeutig* als Produkt von irreduziblen Elementen geschrieben werden kann. In faktoriellen Ringen:

prim $\Leftrightarrow$ irreduzibel.

**Clicker-Frage:** Sei $R$ ein Integritätsbereich und seien $a, b \in R$, so dass $a \mid b$. Falls $c$ assoziiert ist zu $a$, so gilt $c \mid b$.

*Beweis:* $c$ ist assoziiert zu $a$: Falls $a \mid c$ und $c \mid a$, $\Leftrightarrow a = uc$ für $u \in R$ Einheit.

Dann haben wir $a \mid b \Leftrightarrow b = aq = cuq \implies c \mid b$. □

**Satz 72.** *Sei $R$ faktoriell und seien $a, b \in R$. Seien $a = p_1 \cdots p_r$ und $b = q_1 \cdots q_s$ Primfaktorzerlegungen.*

*Dann gilt $a \mid b \Leftrightarrow s \geq r$ und (nach Umordnung) $p_i$ ist assoziiert zu $q_i$ für $i = 1, \ldots, r$.*

*Beweis:* " $\implies$ "

Falls $a \mid b$, so folgt $p_1 \mid b$.

$\implies p_1 \mid q_i$ für ein $i$. OBdA $i = 1$.

$\implies p_1$ und $q_1$ sind assoziiert.

$\implies$ wir haben $p_1 p_2 \cdots p_r c = q_1 q_2 \cdots q_s$ für ein $c \in R$.

$\implies p_2 \cdots p_r c = q_2' \cdots q_s$ für $q_2'$ assoziiert zu $q_2$.

$\implies p_2 \cdots p_r \mid q_2 \cdots q_s$

$\rightsquigarrow$ per Induktion $s \geq r$ und $p_i$ ist assoziiert zu $q_i$ für $i = 1, \ldots, r$.

" $\impliedby$ " ist klar. □

**Korollar 15.** *Sei $R$ faktoriell und seien $a, b \in R$, nicht beide null. Dann gibt es ein $d \in R$ s.d.*

*(i) $d \mid a$ und $d \mid b$*

*(ii) $\forall e \in R$, s.d. $e \mid a$ und $e \mid b \implies e \mid d$*

*Ein solches $d$ heisst* ***grösster gemeinsamer Teiler*** *(ggT) von $a$ und $b$.*

*Beweis:* Übung. □

**Bemerkung 61.** *Zwei verschiedene ggT sind assoziiert.*

**Bemerkung 62.** *Im Allgemeinen ist ein ggT von $a$ und $b$ nicht von der Form $ar + bs$ für $r, s \in R$.*

**Definition 53.** *Ein IB, in dem jedes Ideal ein Hauptideal ist, heisst* ***Hauptidealring****.*

**Satz 73.** *Seien $R$ ein Hauptidealring und $a, b \in R$, nicht beide null. Dann ist $d \in R$, sodass $(d) = (a) + (b)$ ein ggT von $a$ und $b$ ist. Ausserdem existieren $r, s \in R$ s.d. $d = ar + bs$.*

*Beweis:* Da $a, b \in (d)$, folgt $d \mid a$ und $d \mid b$.

Falls $e \mid a$ und $e \mid b$, so ist $a \in (e)$ und $b \in (e)$

$\implies (d) = (a) + (b) \subseteq (e)$

$\implies e \mid d$.

Da $d \in (a) + (b)$, existieren $r, s \in R$ s.d. $d = ar + bs$. □

**Korollar 16.** *Sei $R$ ein Hauptidealring. Dann*

*(a) Ein $r \in R$ ist irreduzibel $\Leftrightarrow$ $r$ ist prim*

*(b) Die maximalen in $R$ sind genau die Hauptideale, die von einem irreduziblen Element erzeugt werden.*

*Beweis:*

(a) gesehen: Primelemente sind irreduzibel. Sei $r \in R$ irreduzibel und man nehme an, dass $r \mid ab$ und $r \nmid a$.

**z.z:** $r \mid b$.

Sei $d$ ein ggT von $a$ und $r$.

$r$ ist irreduzibel $\implies$ $d$ ist Einheit oder $d$ ist assoziiert zu $r$. Da $r \nmid a$ ist $d$ nicht assoziiert zu $r$, d.h. $d$ ist eine Einheit.

$\implies (a) + (r) = (d) = (1)$.

$\implies \exists s, t \in R$ s.d. $1 = sr + ta$

$\implies b = \underbrace{srb + tab}_{\text{durch } r \text{ teilbar}}$

$\implies r \mid b$

(b) Sei $q \in R$ irreduzibel.

$\Longrightarrow$ alle Teiler von $q$ sind assoziiert zu $q$ oder Einheiten.

Falls $(q) \subseteq (p)$, so ist $(q) = (p)$ oder $(p) = (1)$.

$\Longrightarrow$ $(q)$ ist maximal.

Falls $q \in R$ nicht irreduzibel ist: Sei $a$ ein echter Teiler von $q$.

$\Longrightarrow$ $(q) \subsetneq (a) \subsetneq (1)$, d.h. $(q)$ ist nicht maximal. □

**Satz 74.** *Ein Hauptidealring $R$ ist faktoriell.*

*Beweis:* Gesehen: Jedes irreduzible Element in $R$ ist prim.

**z.Z:** Faktorisierung endet in R.

Man nehme an, es gibt eine unendliche aufsteigende Kette von Hauptidealen

$(a_1) \subsetneq (a_2) \subsetneq \cdots$

**Behauptung:** $\bigcup_{i=1}^{\infty}(a_i) = I \subseteq R$ ist ein Ideal. *Beweis:* Seien $a, b \in I, r \in R$. Dann sind $a, b \in (a_n)$ für ein $n \implies a + b \in (an) \subseteq I$ und $ra \in (a_n) \subseteq I$.

R ist Hauptidealring, d.h. $I = (1)$ für ein $b \in R$. Da $b \in I$, folgt, dass $b \in (a_n)$ für ein $n \implies (b) \subseteq (a_n)$.

Aber auch $(a_n) \subsetneq (a_{n+1})$ (Widerspruch). □

**Bemerkung 63.** *Gesehen: $K$ Körper $\implies$ $K[x]$ ist ein Hauptidealring.*

*Die Einheiten sind genau die Elemente in $K^*$.*

*Jedes Polynom in $K[x]\backslash\{0\}$ ist assoziiert zu einem eindeutigen normierten Polynom.*

**Satz 75.** *Seien $f, g \in K[x]$. Dann:*

*(a) Es existiert ein eindeutiger normierter ggT $d \in K[x]$ und $r, s \in K[x]$ s.d. $rf + sg = d$.*

*(b) Falls $f$ und $g$ keinen nicht-konstanten gemeinsamen Faktor haben, so existieren $r, s \in K[x]$ s.d. $rf + sg = 1$.*

*(c) Jedes irreduzible $p \in K[x]$ ist auch prim.*

*(d) Sei $f \in K[x]$ normiert, dann ist $f = p_1 \cdots p_k$, $p_i \in K[x]$ normiert. Diese Faktorisierung ist eindeutig bis auf eine Permutation der $p_i$.*

*Beweis:* Kleine Übung (folgt aus all den Resultaten von heute). □

**Gesehen:** Sei $R$ ein Ring, $\alpha \in R, f \in R[x]$. Dann ist $f(\alpha) = 0 \Leftrightarrow (x-\alpha)\big|f$.

**Beispiel 46.** *Sei* $f \in \mathbb{C}[x], \deg f \geq 2$. *Dann* $\exists \alpha \in \mathbb{C}$ *s.d.* $f(\alpha) = 0$.

$\implies (x-\alpha)\big|f$, *d.h.* $f$ *ist nicht irreduzibel.*

*Die einzigen irreduziblen Elemente in* $\mathbb{C}[x]$ *sind also* $(x-a), \quad a \in \mathbb{C}$.

$\implies$ *Jedes normierte* $f \in \mathbb{C}[x]$ *hat eine eindeutige Faktorisierung* $f = (x-\alpha_1)\cdots(x-\alpha_n) \quad \alpha_i \in \mathbb{C}$

**Satz 76.** *Sei* $K$ *ein Körper. Ein Polynom* $f \in K[x]$ *mit* $\deg(f) = n$ *hat höchstens* $n$ *Nullstellen.*

*Beweis:* Ein $\alpha \in K$ ist eine Nullstelle von $f \Leftrightarrow (x-\alpha)\big|f$.

Ist dies der Fall, so ist $f(x) = (x-\alpha)q(x), \quad \deg(q) < \deg(f)$.

Falls $\beta \in K$ s.d. $f(\beta) = 0$, so ist $(\beta-\alpha)q(\beta) = 0 \implies \alpha = \beta$ oder $\beta$ ist Nullstelle von $q$.

Gemäss Induktion hat $q$ höchstens $n-1$ Nullstellen. □

Um zu zeigen, dass $\mathbb{Z}$ und $K[x]$ Hauptidealringe sind, verwenden wir Division mit Rest.

$a = bq + r$

**Definition 54.** *Sei* $R$ *ein IB. Eine* ***Grössenfunktion*** *ist eine Funktion* $\sigma\colon R\backslash\{0\} \to \mathbb{Z}_{\geq 0}$.

**Definition 55.** $R$ *ist ein* ***euklidischer Ring****, falls es eine Grössenfunktion* $\sigma\colon R\backslash\{0\} \to \mathbb{Z}_{\geq 0}$ *gibt, so dass ein Divisionsalgorithmus existiert:*

*Für alle* $a, b \in R, b \neq 0$ *gibt es* $q, r \in R$ *mit* $a = bq + r$ *sodass entweder* $r = 0$ *ist oder* $\sigma(r) < \sigma(b)$.

# Vorlesung 22

Letztes Mal: Euklidische Ringe.

**Beispiel 47.**

- $\mathbb{Z}$ *mit Grössenfunktion* $|\cdot|$
- $K[x]$ *mit Grössenfunktion* deg

**Satz 77.** *Der Ring der Gaussschen Zahlen* $\mathbb{Z}[i]$ *ist euklidisch mit Grössenfunktion* $\sigma(x+iy) = x^2 + y^2$.

*Beweis:* Seien $a = m_1 + in_1$ und $b = m_2 + in_2$, $a, b \in \mathbb{Z}[i]$ und $b \neq 0$. Dann ist

$$\frac{a}{b} = \frac{a\bar{b}}{|b|^2} = \frac{m_1m_2 + n_1n_2}{m_2^2 + n_2^2} + i\frac{n_1m_2 - m_1n_2}{m_2^2 + n_2^2}$$

$$= \underbrace{q_1 + iq_2}_{=:q\in\mathbb{Z}[i]} + (r_1 + ir_2)$$

s.d. $r_1, r_2 \in \mathbb{Q} \cap \left(-\frac{1}{2}, \frac{1}{2}\right]$

$$\implies a = bq + \underbrace{b(r_1 + ir_2)}_{=:r}$$

$$r = a - bq \in \mathbb{Z}[i]$$

$$|r|^2 = |b|^2(r_1^2 + r_2^2) \leq |b|^2(\frac{1}{4} + \frac{1}{4}) = \frac{1}{2}|b|^2 \leq |b|^2$$

$\implies a = bq + r$ s.d. $|r|^2 < |b|^2$ □

**Satz 78.** *Ein euklidischer Ring $R$ ist ein Hauptidealring.*

*Beweis:* $R$ ist IB.

Sei $I \subseteq R$ ein Ideal.

(0) ist Hauptideal. Wir nehmen an, $I \neq (0)$.

Sei $b \in I$, s.d. $\sigma(b)$ minimal ist ($\sigma$ die Grössenfunktion auf $R$).

**z.Z:** $(b) = I$.

Sei $a \in I$.

Teilen mit Rest: $a = bq + r$, s.d. $\sigma(r) < \sigma(b)$ oder $r = 0$.

$r = a - bq \in I$.

$\sigma(r) < \sigma(b)$ nicht möglich, da $\sigma(b)$ minimial.

$\implies r = 0 \implies a = bq \implies a \in (b) \implies I = (b)$ □

**Korollar 17.** *Die Ringe $\mathbb{Z}$, $K[x]$ (für $K$ Körper) und $\mathbb{Z}[i]$ sind Hauptidealringe.*

**Übersicht über bisher gesehene Ringe**

euklidische Ringe $\subseteq$ Hauptidealringe $\subseteq$ faktorielle Ringe $\subseteq$ Integritätsbereiche

## Das Gausssche Lemma

Sei $R$ ein faktorieller Ring.

**Ziel:** Studieren der Faktorisierung in $R[x]$.

In diesem Abschnitt: $R = \mathbb{Z}$. Aber der allgemeine Fall ist sehr ähnlich.

Wir verstehen die Faktorisierung in $\mathbb{Z}$ und in $\mathbb{Q}[x]$.

**Beispiel 48.** $f(x) = 6x^3 + 9x^2 + 9x + 3$

$\underbrace{=}_{in\ \mathbb{Z}[x]}\ 3(2x+1)(x^2+x+1)$

$\underbrace{=}_{in\ \mathbb{Q}[x]}\ \frac{3}{2}(x+\frac{1}{2})(x^2+x+1)$

# Vorlesung 23

**Ziel:** Faktorisierung in $\mathbb{Z}[x]$.

$\mathbb{Z}[x] \subseteq \mathbb{Q}[x]$

**Definition 56.** *Ein Polynom $f(x) \in \mathbb{Z}[x], \quad f(x) = a_n x^n + \cdots + a_0$ ist **primitiv**, falls der ggT aller Koeffizienten 1 ist und $a_n > 0$.*

**Lemma 6.** *Jedes Polynom $f(x) \in \mathbb{Q}[x]\backslash\{0\}$ lässt sich eindeutig schreiben als $f(x) = cf_0(x)$ für ein $c \in \mathbb{Q}$ und ein $f_0(x) \in \mathbb{Z}[x]$ primitiv.*

**Definition 57.** *Die Zahl $x \in \mathbb{Q}$ heisst der **Inhalt** von $f$.*

*Beweis:*

**Existenz:** Multipliziere $f$ mit $n \in \mathbb{Z}$ sodass $nf \in \mathbb{Z}[x]$.

Sei $m \in \mathbb{Z}$ der ggT aller Koeffizienten von $f_1$ mit geeignetem Vorzeichen, s.d. $f_1 = mf_0, f_0 \in \mathbb{Z}[x]$ primitiv.

$\implies f = \frac{m}{n} f_0$

**Eindeutigkeit:** Seien $cf_0(x) = dg_0(x), \quad c, d \in \mathbb{Q}, f_0, g_0 \in \mathbb{Z}[x]$ primitiv. Nach Multiplikation mit ganzer Zahl können wir annehmen, dass $c, d \in \mathbb{Z}$ Sei $f_0(x) = a_n x^n + \cdots + a_0, g_0(x) = b_n x^n + \cdots + b_0$

$\implies ca_i = db_i$

Da $f_0$ und $g_0$ primitiv sind, ist der ggT von $\{ca_0, \ldots, ca_n\}c$ und der ggT von $\{db_0, \ldots, db_n\}$ ist $d$

$\implies c = \pm d$ und somit $f_0 = \pm g_0$.

Aber $f_0$ und $g_0$ haben positive Leitkoeffizienten.

$\implies f_0 = g_0$ und $c = d$. □

**Gesehen:** Es gibt einen Ringhomomorphismus $\mathbb{Z}[x] \to \mathbb{F}_p[x]$

$f(x) = a_n x^n + \cdots + a_0 \mapsto \overline{a_n} x^n + \cdots + \overline{a_0} = \overline{f}(x)$

**Bemerkung 64.** *Falls $f(x) \in \mathbb{Z}[x]$ primitiv ist, so ist $\overline{f}(x) \in \mathbb{F}_p[x]$ nicht null, da mindestens einer der Koeffizienten von $f(x)$ nicht durch $p$ teilbar ist.*

**Satz 79** (Gauss-Lemma)**.** *Seien $f, g \in \mathbb{Z}[x]$ primitiv. Dann ist auch $h := fg$ primitiv.*

*Beweis:* Die Leitkoeffizienten von $f$ und $g$ sind positiv $\implies$ Leitkoeffizient von $h = fg$ ist positiv.

**z.z:** Es gibt keine Primzahl $p$, die alle Koeffizienten von $h$ teilt.

Sei $p$ eine Primzahl. Man betrachte den Homomorphismus $\mathbb{Z}[x] \to \mathbb{F}_p[x]$

Da $f$ und $g$ primitiv sind, ist $\overline{f} \neq 0$ und $\overline{g} \neq 0$.

$\underset{\mathbb{F}_p[x] \text{ ist IB}}{\implies} \overline{h} = \overline{f}\,\overline{g} \neq 0$

$\implies$ $p$ teilt nicht alle Koeffizienten von $h$. □

**Satz 80.** *(a) Seien $f, g \in \mathbb{Q}[x]$ und $f_0, g_0 \in Z[x]$ primitiv s.d. $f = cf_0, g = dg_0$. Falls $f$ ein Teiler von $g$ in $\mathbb{Q}[x]$ ist, so ist $f_0$ ein Teiler von $g_0$ in $\mathbb{Z}[x]$.*

*(b) Sei $f \in \mathbb{Z}[x]$ primitiv und $g \in \mathbb{Z}[x]$ beliebig. Falls $g = fq$ für $q \in \mathbb{Q}[x]$, dann ist $q \in \mathbb{Z}[x]$*

*(c) Seien $f, g \in \mathbb{Z}[x]$. Falls $f$ und $g$ einen gemeinsamen nicht konstanten Teiler $h$ in $Q[x]$ haben, so haben sie auch in $\mathbb{Z}[x]$ einen gemeinsamen nicht konstanten Teiler.*

*Beweis:*

**(b)** Wir schreiben $q = cq_0$ mit $c \in \mathbb{Q}, q_0 \in \mathbb{Z}[x]$ primitiv. $\underset{\text{Gauss}}{\implies} fq_0$ ist primitiv.

Wir haben $g = cfq_0$, daher muss gelten, dass $c \in \mathbb{Z}$ und somit $q \in \mathbb{Z}[x]$.

**a** Falls $f$ Teiler von $g$ in $\mathbb{Q}[x]$ ist, so ist auch $f_0$ ein Teiler von $g_0$ in $\mathbb{Q}[x]$.

$\underset{(b)}{\implies}$ $f_0$ ist ein Teiler von $g_0$ in $\mathbb{Z}[x]$.

**(c)**: Wir schreiben $h = ch_0, c \in \mathbb{Q}, h_0 \in \mathbb{Z}[x]$ primitiv.

$f = ch_0 f_1$ und $g = ch_0 g_1$ für $f_1, g_1 \in \mathbb{Q}[x]$.

$\underset{(b)}{\implies}$ $h_0$ teilt $f$ und $h_0$ teilt $g$ in $\mathbb{Z}[x]$. □

**Korollar 18.** *Sei $f \in \mathbb{Z}[x]$ nicht konstant. Falls $f$ in $\mathbb{Z}[x]$ irreduzibel ist, so ist, $f$ auch in $\mathbb{Q}[x]$ irreduzibel.*

*Beweis:* $f$ hat keine echten Teiler in $\mathbb{Q}[x]$

$\underset{\text{Satz}}{\Longrightarrow}$ $f$ hat keine echten Teiler in $\mathbb{Z}[x]$. □

**Satz 81.** *Sei $f(x) \in \mathbb{Z}[x]$ mit positivem Leitkoeffizienten. Das Polynom $f$ ist genau dann irreduzibel in $\mathbb{Z}[x]$, wenn entweder*

*(i) $f$ ist eine Primzahl.*

*(ii) $f$ ist primitiv und in $\mathbb{Q}[x]$ irreduzibel.*

*Beweis:* " $\Longrightarrow$ " Sei $f$ irreduzibel. Wir schreiben $f = cf_0$ für $f_0$ primitiv.

Da $f$ irreduzibel ist, muss $c$ oder $f_0$ eine Einheit sein.

D.h. entweder $c = 1$ oer $f_0 = 1$.

Falls $f_0 = 1$, dann ist $f$ konstant und somit eine Primzahl.

Falls $c = 1$, so ist $f = f_0$ primitiv und somit irreduzibel in $\mathbb{Q}[x]$ gemäss Korollar.

" $\Longleftarrow$ " klar. □

**Satz 82.** *Jedes irreduzible Element in $\mathbb{Z}[x]$ ist ein Primelement.*

*Beweis:* Sei $f$ irreduzibel und seien $g, h \in \mathbb{Z}[x]$ sodass $f \big| gh$.

**z.z:** $f \big| g$ oder $f \big| h$.

1. Fall: $f = p$ ist eine Primzahl. Wir schreiben $g = cg_0$ und $h = dh_0$. $g_0, h_0$ primitiv, $c, d \in \mathbb{Z}$.

$\underset{\text{Gauss}}{\Longrightarrow}$ $h_0 g_0$ primitiv.

$\Longrightarrow$ es gibt einen Koeffizienten $a$ von $g_0 h_0$, der nicht durch $p$ teilbar ist.

Da aber $p \big| gh$ und $gh = cdg_0 h_0$

$\Longrightarrow$ $p \big| cda$

$\Longrightarrow$ $p \big| c$ oder $p \big| d$

$\Longrightarrow$ $p \big| g$ oder $p \big| h$.

2. Fall: $f$ ist primitiv und irreduzibel in $\mathbb{Q}[x]$.

$\underset{\mathbb{Q}[x]\text{ist faktoriell}}{\Longrightarrow}$ $f$ ist prim in $\mathbb{Q}[x]$.

$\Longrightarrow$ $f$ ist Teiler von $g$ oder von $h$ in $\mathbb{Q}[x]$

$\underset{\text{Satz}}{\Longrightarrow}$ $f$ ist Teiler von $g$ oder $h$ in $\mathbb{Z}[x]$. □

**Satz 83.** *$\mathbb{Z}[x]$ ist faktoriell. Insbesondere lässt sich jedes $f(x) \in \mathbb{Z}[x]$ eindeutig (bis auf Permutation der Faktoren) schreiben als $f(x) = \pm p_1 \cdots p_m q_1(x) \cdots q_n(x)$ wobei $p_i$ positive Primzahlen sind und $q_i$ irreduzible primitive Polynome.*

*Beweis:* Es reicht zu zeigen, dass Faktorisierung in $\mathbb{Z}[x]$ endet, da irreduzible Elemente prim sind.

Sei $(p_1) \subsetneq (p_2) \subsetneq \cdots$ eine aufsteigende Kette von Hauptidealen, d.h. $p_{i+1}$ ist echter Teiler von $p_i, i = 1, 2, \cdots$

$\implies \deg P_{P_{i+1}} \leq \deg p_i$

$\implies \deg p_n = \deg p_{n+k}$ für $n$ gross genug und für alle $k \geq 0$ schreibe $p_n = c_n p_{n,0}$

$p_{n+k} = c_{n+k} p_{n+k,0}$

$p_{n,0}, p_{n+k,0}$ primitiv.

Da $p_{n+k} | p_k$ gilt $p_{0,n+k} = p_{0,n}$ und somit $c_{n+k} | c_n$ in $\mathbb{Z}$.

Da $c_n$ nur endlich viele Teile hat, erhalten wir $(p_{n+k}) = (p_{n+k+1}) = \cdots$ für $k$ gross genug.

$\implies$ es gibt keine solchen Ketten. □

**Satz 84.** *Sei $R$ ein faktorieller Ring mit Quotientenkörper $K$. Dann gilt:*

*(a) Seien $f, g \in R[x]$ nicht konstant. Falls $f$ und $g$ in $K[x]$ einen nicht-konstanten gemeinsamen Teiler haben, so haben sie auch in $R[x]$ einen nicht-konstanten gemeinsamen Teiler.*

*(b) Sei $f \in R[x]$ nicht konstant. Falls $f$ in $R[x]$ irreduzibel ist, so ist es auch in $K[x]$ irreduzibel.*

*(c) $R[x]$ ist faktoriell.*

*Beweis:* Beweise analog zum Fall $R = \mathbb{Z}$. ($\rightsquigarrow$ etwas komplizierter wegen Einheiten). □

**Korollar 19.** *Die Polynomringe $\mathbb{Z}[x_1, \ldots, x_n] K[x_1, \ldots, x_n]$, für $K$ Körper, sind faktoriell.*

*Beweis:* Falls $R$ faktoriell ist, so erhalten wir induktiv, dass auch $R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$ faktoriell ist. □

# Vorlesung 24

## Kriterien für Irreduzbilität

Wie zeigt man, dass $f \in \mathbb{Q}[x]$ irreduzibel ist?

**Satz 85.** *Sei $f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Sei $p$ eine Primzahl, sodass $p \nmid a_n$.*

*Ist die Restklasse $\overline{f} \mod p$ irreduzibel in $\mathbb{F}_p[x]$, so ist $f$ irreduzibel in $Q[x]$.*

*Beweis:* Man nehme an $f = gh$, für $g, h \in \mathbb{Q}[x]$ echte Faktoren, d.h. insbesondere $\deg g, \deg h < \deg f$.

Gemäss Satz von gestern können wir annehmen, dass $g, h \in \mathbb{Z}[x]$.

Reduktion $\mod p$.

$\overline{f} = \overline{g}\overline{h}$ in $\mathbb{F}_p[x]$

Da $p \nmid a_n$, ist $\deg \overline{f} = n$.

Ausserdem haben wir $\deg \overline{g} < n, \deg \overline{h} < n$.

aber $\deg(\overline{g}\overline{h}) = n$

$\implies \deg \overline{g} > 0, \deg \overline{h} > 0$

$\implies \overline{g}$ ist ein echter Teiler von $\overline{f}$.

$\implies \overline{f}$ ist nicht irreeduzibel. □

**Bemerkung 65.** *Man kann so nicht zeigen, dass ein Polynom reduzibel ist. Es gibt Polynome $f \in \mathbb{Z}[x]$, sodass $f$ irreduzibel ist, aber die Restklasse $\overline{f} \mod p$ ist nicht irreduzibel für alle Primzahlen $p$ (z.B. $f(x) = x^4 - 10x^2 + 1$).*

**Sieb des Eratosthenes**

Das Sieb des Eratosthenes um Primzahlen zu finden.

**2 3** ~~4~~ **5** ~~6~~ **7** ~~8~~ ~~9~~ ~~10~~ **11** ~~12~~ **13** ~~14~~ ~~15~~ ~~16~~ **17** ~~18~~ **19**

Diese Methode funktioniert auch für $\mathbb{F}_p[x]$.

Wir schreiben alle Polynome Grad für Grad nebeneinander und streichen die Vielfachen weg.

$\mathbb{F}_2[x]$:

Grad 1:

$x, x+1$

Grad 2:

$x^2, x^2+x, x^2+x+1, x^2+1$

Grad 3:

$x^3, x^3+x^2, x^3+x^2+x, x^3+x^2+x+1, \ldots$

Nach dem Sieb bleiben $x, x+1, x^2+x+1, \ldots$

**Beispiel 49.** *$x^2 + x + 1$ ist irreduzibel in $\mathbb{F}_2[x]$*

$\underset{Satz}{\Longrightarrow}$ *$3x^2 + x + 7 \in \mathbb{Z}[x]$ ist auch irreduzibel.*

**Satz 86** (Eisenstein Kriterium)**.** *Sei $p$ eine Primzahl.*

*$f(x) = a_n x^n + \cdots + a_0 \in \mathbb{Z}[x]$ sodass*

*(i)* $p \nmid a_n$

*(ii)* $p \mid a_i$ *für* $i = 0, \ldots, n-1$

*(iii)* $p^2 \nmid a_0$

*Dann ist $f$ irreduzibel in $\mathbb{Q}[x]$.*

**Beispiel 50.** *$x^4 + 50x^2 + 30x + 20$ ist irreduzibel in $\mathbb{Q}[x]$ (und auch $\mathbb{Z}[x]$, da es primitiv ist.)*

*Beweis:* Sei $\overline{f}$ die Restklasse von $f \mod p$.

$\Longrightarrow$ $\overline{f} = \overline{a_n} x^n, \overline{a_n} \neq 0$.

Wir nehmen an, $f \in \mathbb{Q}[x]$ ist reduzibel, d.h. $f = gh$, mit $g, h$ echten Teilern.

Wir können annehmen $g, h \in \mathbb{Z}[x]$.

$\Longrightarrow$ $\overline{g}$ und $\overline{h}$ teilen $\overline{a_n} x^n$

$\Longrightarrow$ $\overline{g}$ und $\overline{h}$ sind Monome.

$\Longrightarrow$ alle Koeffizienten von $g$ und $h$ ausser dem Leitkoeffizienten sind durch $p$ teilbar.

Sei $b_0$ der konstante Koeffizient von $g$ und $c_0$ der konstante Koeffizient von $h$.

$\Longrightarrow$ der konstante Koeffizient von $f$ ist $a_0 = b_0 c_0$.

Da $p \mid b_0$ und $p \mid c_0$, folgt $p^2 \mid a_0$ (widerspruch zu (iii)).

$\Longrightarrow$ $f$ ist irreduzibel. □

**Definition 58.** *Sei $p$ eine Primzahl.*

*Betrachte* $x^p - 1 = (x-1) \underbrace{(x^{p-1} + x^{p-2} + \cdots + x + 1)}_{f(x)}$.

*$f(x)$ heisst* ***Kreisteilungspolynom****.*

**Korollar 20.** *Sei $p$ eine Primzahl. $f(x) = x^{p-1} + x^{p-2} + \cdots + x + 1$ ist irreduzibel in $\mathbb{Q}[x]$.*

*Beweis:* $(x-1) f(x) = x^p - 1$.

Substituiere $x = y + 1$

$\implies yf(y+1) = (y+1)^p - 1 = y^p + \binom{p}{1} y^{p-1} + \binom{p}{2} y^{p-2} + \cdots + \binom{p}{p-1} y$

Wir haben $\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{i!}$

$i < p \implies p \nmid i!$

$\implies p \mid \binom{p}{i}$ für $i = 1, \ldots, p-1$.

Aber $\binom{p}{p-1} = p$, d.h. $p^2 \nmid \binom{p}{p-1}$

$\implies f(y+1)$ erfüllt das Einsenstein-Kriterium.

$f(y+1)$ ist irreduzibel.

$f(y)$ ist irreduzibel. $\square$