

# Algebra I – Prof. Christian Urech

Mitschrift: Franz Nowak

Herbstsemester 2025

## Vorlesung 1

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

- (1) (Assoziativität)  $\forall g, h, k \in G: (g * h) * k = g * (h * k)$
- (2) (Neutrales Element)  $\exists e \in G: g * e = e * g = g \quad \forall g \in G$
- (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  $g_1 g_2 \cdots g_n$  eindeutig definiert (für  $g_1, g_2, \dots, g_n \in G$ ).

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

(b) Das Inverse von jedem Element ist eindeutig.

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

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

□

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

*Beweis:*

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

□

## Beispiele

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

## Permutationsgruppen

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

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

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

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

$$\sigma: \begin{cases} 1 \rightarrow 2 \\ 2 \rightarrow 1 \\ 3 \rightarrow 3 \end{cases} \quad \tau: \begin{cases} 1 \rightarrow 2 \\ 2 \rightarrow 3 \\ 3 \rightarrow 1 \end{cases}$$

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

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

D.h.  $S_3$  ist nicht abelsch.

## Untergruppen

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

- $\forall a, b \in H, ab \in H$
- $1_G \in H$
- $\forall a \in H, a^{-1} \in H$

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

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

$$\langle a \rangle := \{\dots, a^{-2}, a^{-1}, a^0, a, a^2, \dots\}$$

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

**Bemerkung 7.**  $\langle a \rangle$  ist abelsch:  $a^m a^n = a^{m+n} = a^{n+m} = a^n a^m$

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

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

- (a) Seien  $m, n \in X$ , dann ist  $a^{m+n} = a^m a^n = 1_G \implies m + n \in X$
- (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  $a^n = a^{km+r} = a^{km}a^r = a^r$ .  $\Rightarrow \langle a \rangle = \{1, a, \dots, a^{m-1}\}$  und all diese Elemente sind verschieden. (Falls  $a^r = a^{r'}$   $\Rightarrow a^{r-r'} = 1 \Rightarrow r - r' \in m\mathbb{Z} \Rightarrow r = r' \quad 0 \leq r, r' < m$ )

Falls  $m = 0$ :

Dann ist  $\langle a \rangle = \{\dots, a^{-2}, a^{-1}, 1, a, a^2, \dots\}$  und alle Partitionen sind verschieden.

## Vorlesung 2

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

### Beispiele

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

### Homomorphismen

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

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

### Beispiele

- $\det: GL_n(K) \rightarrow K^*$
- signum - sign:  $S_n \rightarrow \mathbb{Z}/2\mathbb{Z}$ ,  

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

### Satz 3.

- (1) Falls  $\phi: G \rightarrow G'$  und  $\psi: G' \rightarrow G''$  Homomorphismen sind, so auch  $\psi \circ \phi: G \rightarrow G''$ .

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

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

(2) zu zeigen:  $\phi^{-1}$  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  $G = \langle a \rangle, G' = \langle b \rangle$  und  $\phi: G \rightarrow G', \phi(a^n) \mapsto b^n$ .

Falls  $|G| = |G'|$  endlich ist, so ist  $G = \{1, a, \dots, a^{m-1}\}, G' = \{1, b, \dots, b^{m-1}\}$ . Somit ist  $\phi$  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  $\phi: G \rightarrow G'$  ein Homomorphismus. Dann sind  $\phi(1_G) = 1_{G'}$  und  $\phi(a^{-1}) = \phi(a)^{-1} \forall a \in G$

*Beweis:*

$$\begin{aligned} 1_G &= 1_G 1_G \\ &\implies \phi(1_G) = \phi(1_G 1_G) = \phi(1_G)\phi(1_G) \\ &\stackrel{\text{kürzen}}{\implies} 1_{G'} = \phi(1_G) \end{aligned}$$

Ausserdem:

$$\begin{aligned} \phi(a^{-1}\phi(a)) &= \phi(a^{-1}a) = \phi(1_G) = 1_{G'} \\ &\implies \phi(a^{-1}) = \phi(a)^{-1} \end{aligned}$$

□

**Definition 6.** Ein Automorphismus ist ein Isomorphismus  $\phi: G \rightarrow G$  von einer Gruppe  $G$  zu sich selbst.

**Beispiel 2.** Für  $f \in G$  definiere  $\phi: G \rightarrow G, \phi(g) := f g f^{-1}$  ( $f g f^{-1}$  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  $\phi: G \rightarrow G'$  definiere:

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

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

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

### Beispiele

- $\det: GL_n(K) \rightarrow K^*$ , Kern  $\det = SL_n(K)$
- $\text{sign}: S_N \rightarrow C_2$ , Kern  $\text{sign} = A_n$

**Bemerkung 9.** Seien  $\phi: G \rightarrow G'$  ein Homomorphismus und  $a \in \text{Kern } \phi$  und  $b \in G$ . Dann ist

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

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

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

### Partitionen

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

**Beispiel 3.** Sei  $\phi: \mathbb{C}^* \rightarrow \mathbb{R}_{>0}^*$ ,  $\phi(z) \mapsto |z|$ . Allgemein:  $\phi^{-1} = \text{Kern } \phi$ .

**Satz 5.** Sei  $U: G \rightarrow G'$  ein Homomorphismus mit Kern  $N$ . Für  $a, b \in G$  gilt  $\phi(a) = \phi(b) \Leftrightarrow \exists n' \in N \text{ s.d. } b = an$ , d.h.  $a^{-1}b \in N$ .

*Beweis:* “ $\Rightarrow$ ”: Falls  $\phi(a) = \phi(b)$ , dann ist  $U(a)^{-1}\phi(b) = \phi(a^{-1}b) = 1$ , d.h.  $\exists n \in N$ , s.d.  $a^{-1}b = n \implies b = an$ .

“ $\Leftarrow$ ” Falls  $b = an$  für  $n \in N$ , dann ist  $\phi(b) = \phi(a)\phi(n) = \phi(a)$ .  $\square$

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

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

**Korollar 1.** Ein Homomorphismus  $\phi: G \rightarrow G'$  ist injektiv  $\Leftrightarrow \text{Kern } \phi = \{1\}$ .

*Beweis:* “ $\Rightarrow$ ” klar.

“ $\Leftarrow$ ” Man nehme an, dass der Kern  $\phi = \{1\}$ .  $\phi(a) = \phi(b) \Leftrightarrow a^{-1}b \in \text{Kern } \phi$ , d.h.  $a^{-1} + b = 1 \implies a = b$ .  $\square$

## Nebenklassen

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

- i) (Transitivität) Falls  $a \sim b$  und  $b \sim c$ , dann ist  $a \sim c$ .
- ii) (Symmetrie) Falls  $a \sim b$ , so ist  $b \sim a$ .
- iii) (Reflexivität)  $a \sim a$  für alle  $a \in X$ .

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

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

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

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

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

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

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

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

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

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

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

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

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

$\phi: X \rightarrow Y$  Abbildung  $\phi^{-1}(y) = \{x \in X \mid \phi(x) = y\}$  für  $y \in Y$ .  $\square$

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

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

**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.**  $m \geq 1$ ,  $[\mathbb{Z} : m\mathbb{Z}] = m$ .

**Satz 7.** Sei  $G$  eine endliche Gruppe und  $H \leq G$ . Dann ist  $|G| = |H|[G : H]$ .

*Beweis:* Die Abbildung  $\phi: H \rightarrow aH$ ,  $\phi(h) = ah$ .

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

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

Daraus folgt direkt:

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

**Bemerkung 10.** Falls  $a \in G$ , dann folgt mit Lagrange, dass  $|\langle a \rangle| \mid |G|$ , d.h.  $\text{Ord}(a)$  teilt die Ordnung von  $G$ .

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

*Beweis:*  $\text{ord } a \mid p$ , da  $\text{ord } a > 1$  ist,  $\text{ord } a = p$ , d.h.  $|\langle a \rangle| = p \implies \langle a \rangle = G$ .  $\square$

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

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

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

$$\begin{aligned} \implies |\text{Bild } \phi| &= [G : \text{Kern } \phi] \\ \implies |G| &= |\text{Kern } \phi| \cdot [G : \text{Kern } \phi] \\ &= |\text{Kern } \phi| \cdot |\text{Bild } \phi| \end{aligned}$$

□

**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  $a \in G$ .

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

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

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

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

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

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

## Vorlesung 4

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

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

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

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

## Faktorgruppen

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

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

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

$\rightsquigarrow$  Assoziativität der Verknüpfung auf  $X$ .

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

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

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

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

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

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

□

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

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

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

*Beweis:* In Vorlesung 3 gesehen:

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

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

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

□

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

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

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

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

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

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

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

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

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

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

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

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

## Vorlesung 5

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

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

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

Begründung:

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

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  $\langle S \rangle := \bigcap_{\substack{H \leq G \\ s.d. S \subseteq H}} H$  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.  $\text{ggT}(m, n) = 1$  dann ist  $C_{mn} \simeq C_m \times C_n$

Wir haben vier Homomorphismen:

$$\begin{array}{ccccc} G & & & & G \\ & \searrow i & & \nearrow p & \\ & & G \times G' & & \\ & \swarrow i' & & \searrow p' & \\ G' & & & & G' \end{array}$$

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

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

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

$p$  und  $p'$  sind surjektiv

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

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

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

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

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

**Satz 11.** (a) Ist  $H \cap K = \{1\}$ , so ist  $\pi$  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  $\pi: H \times K \rightarrow G$  ein Isomorphismus.

*Beweis:* (a) Seien  $(h_1, k_1), (h_2, k_2) \in H \times K$  s.d.  $h_1k_1 = h_2k_2$ .

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

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

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

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

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

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

(ii)  $1 \in HK$

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

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

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

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

$$\implies hk = kh$$

$$\implies \pi(h_1, k_1)\pi(h_2, k_2) = h_1k_1h_2k_2 = h_1h_2k_1k_2 = \pi((h_1, k_1)(h_2, k_2))$$

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

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

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

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

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

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

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

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

Wir haben  $hg = gh$  oder  $hg = gh^2$ . Falls  $hg = gh$ , so 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  $g^i h^j$  bringen, wobei  $0 \leq i \leq 1, 0 \leq j \leq 2$ .

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

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

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

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

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

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

## Symmetrie

Isometrien von  $\mathbb{R}^n$

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

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

Zwei wichtige Untergruppen:

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

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

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

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

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

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

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

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

## Vorlesung 6

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

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

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

## Orientierung

Falls  $n = 2$ :

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

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

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

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

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

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

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

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

Beweis:

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

□

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

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

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

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

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

$$(*) : \{f_1, \dots, f_m\} = \{f_jf_1, \dots, f_jf_m\}$$

□

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

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

$$\implies t_a^{-1}Gt_a \leq O.$$

□

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

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

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

*Beweis:* **1. Fall:** Alle Elemente in  $G$  sind in  $\text{SO}(2)$ , 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:  $\langle d_\theta \rangle = G$ .

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

$$\begin{aligned} d + B = d_\alpha d_{-n\theta} &= d_\alpha (d_\theta^{-1})^n \in G \\ &\implies \beta = 0 \\ &\implies d_\alpha (d_\theta^{-1})^n = 1 \\ &\implies d_\alpha = (d_\theta)^n \in \langle d_\theta \rangle \end{aligned}$$

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

## Vorlesung 7

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

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

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

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

Sei  $y$  eine Spiegelung  $\implies \text{ord } y = 2$ . 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.

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

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

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

so dass

- (a)  $1x = x \quad \forall x \in X$
- (b)  $(gg')x = g(g'(g'x)) \quad \forall g, g' \in G, x \in X$

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

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

$$m_g: X \rightarrow X \quad m_g(x) = gx$$

$m_g$  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  $\mathbb{R}^2$ . (Hat nur einen Orbit)

- Sei  $D = \{\text{Dreiecke in } \mathbb{R}^2\}$  Isom( $\mathbb{R}^2$ ) operiert auf  $D$ .
- Zwei Dreiecke  $\Delta, \Delta'$  sind **kongruent**, falls es ein  $g \in \text{Isom}(\mathbb{R}^2)$  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.

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

**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.** •  $\text{Isom}(\mathbb{R}^2) \curvearrowright \mathbb{R}^2$  Der Stabilisator von  $O$  ist die Untergruppe  $O \leq \text{Isom}(\mathbb{R}^2)$ .  $O \simeq O(2)$ .

•  $\text{Isom}(\mathbb{R}^2) \curvearrowright D$ . 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  $H = \langle y \rangle = \{1, y\}$ . Nebenklassen:

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

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

$$m_x: \begin{cases} K_1 \mapsto K_2 \\ K_2 \mapsto K_3 \\ K_3 \mapsto K_1 \end{cases} \quad m_y: \begin{cases} K_1 \mapsto K_1 \\ K_2 \mapsto K_3 \\ K_3 \mapsto K_2 \end{cases}$$

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

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

$$\phi: G/H \rightarrow B_x \quad aH \mapsto ax$$

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 injektiv: 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

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

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

*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  $B_1, \dots, B_k$  die Bahnen. Dann ist

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

### Beispiel: Dodekaeder

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

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

$$\implies |G_S| = 5.$$

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

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

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

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

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

## Vorlesung 8

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

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

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

$\phi$  ist tatsächlich ein Homomorphismus:

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

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

$$\text{d.h. } \phi(gh) = \phi(g)\phi(h).$$

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

Mit dieser Beobachtung zeigt man:

**Satz 18.** Es gibt eine Bijektion

$$\{\text{Operationen } G \curvearrowright X\} \leftrightarrow \{\text{Homomorphismen } G \rightarrow \text{Sym}(X)\}$$

$$G \curvearrowright X \mapsto \phi: G \rightarrow \text{Sym}(X) \quad g \mapsto m_g$$

**Definition 21.** Eine Operation  $G \curvearrowright X$  heisst **treu**, falls der entsprechende Homomorphismus  $\phi: G \rightarrow \text{Sym}(X)$  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  $\phi: G \rightarrow S_3$ . 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  $\Rightarrow |G| \geq 6$ .  $\Rightarrow \phi$  ist ein Isomorphismus.  $\square$

**Satz 20.** Für  $g \in S_3$  sei  $k_g: S_3 \rightarrow S_3$   $k_g(a) = gag^{-1}$  ist ein Automorphismus von  $S_3$ . Dann ist  $f: S^3 \rightarrow \text{Aut}(S_3)$   $f(g) = k_g$  ein Isomorphismus.<sup>1</sup>

*Beweis:* •  $f$  ist Homomorphismus:

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

D.h.  $k_{gh} = k_gk_h$ .  $\Rightarrow f(gh) = f(g)f(h)$ .

- $f$  ist injektiv: Falls  $gag^{-1} = a \quad \forall a \in S_3$  so ist  $g = 1$  (kleine Übung).
- $f$  ist surjektiv: Beobachtung:  $\text{Aut}(S_3)$  operiert auf die Menge der Elemente von Ordnung 2  $\{y, xy, x^2y\}$ :

$$y: \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 1 \\ 3 \mapsto 3 \end{cases} \quad x: \begin{cases} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 1 \end{cases}$$

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

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

$$\begin{aligned} &\Rightarrow |\text{Aut}(S_3)| \leq 6 \\ &\Rightarrow |\text{Aut}(S_3)| = 6 \\ &\Rightarrow S_3 \rightarrow \text{Aut}(S_3) \text{ ist bijektiv, d.h. ein Isomorphismus.} \end{aligned}$$

$\square$

---

<sup>1</sup>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:

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

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

$$G \rightarrow \text{Sym}(G) \quad g \mapsto m_g$$

⇒ 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

$$\phi: G \rightarrow \text{Sym}(G) \simeq S_n \quad g \mapsto m_g$$

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

$G$  operiert auch auf sich selbst durch Konjugation:

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

Sei  $x \in G$ .

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

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

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

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

**Bemerkung 28.**

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

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

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

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

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

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

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

**Bemerkung 30.**

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

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

**Beispiel 10.**

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

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

*Beweis:* Klassengleichung:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**2. Fall:** Alle Elemente in  $G \setminus \{1\}$  haben Ordnung  $p$ . Sei  $x \in G \setminus \{1\}$  und  $H_1 = \langle x \rangle$ . Sei  $y \in G \setminus H$ , und  $H_2 = \langle y \rangle$ . Dann ist  $H_1 \cap H_2 \leq H_2$  und somit  $H_1 \cap H_2 = \{1\}$ .

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

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

$$G \simeq H_1 \times H_2$$

□

## Ikosaedergruppe

Erinnerung:  $I \leq SO(3)$  die Untergruppe der Drehungen, die das Dodekaeder  $D \subseteq \mathbb{R}^3$  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  $\phi: G \rightarrow G'$  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 Würfekante. Die Wahl von einer solchen Kante definiert die Einbettung.

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

$\rightsquigarrow \phi: I \rightarrow S_5$ .

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

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

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

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

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

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

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

**Korollar 10.**  $A + 5$  ist einfach.<sup>2</sup>

## Operationen auf Teilmengen

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

$G \times \mathcal{P}(X) \rightarrow \mathcal{P}(X)$  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  $H \leq \text{Stab}(U) \Leftrightarrow U$  ist die Vereinigung von allen  $H$ -Bahnen.

*Beweis:*  $H$  stabilisiert  $U$

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

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

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

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

**Satz 30.** Sei  $H = \text{Stab}(U)$ . 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.

---

<sup>2</sup>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,  $H \leq G \implies |H||G|$ .

**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  $g \in G \setminus H$ .

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

$$gH = G \setminus H = Hg$$

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

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  $y \in H \setminus \{1\}$ .

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

**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  $s|m$  und  $s \equiv 1 \pmod{p}$ . ( $|G| = p^e m$ )

### Anwendungen von Sylowsätzen

**Satz 34.** Jede Gruppe der Ordnung 15 istzyklisch.

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

$\implies$  Die Anzahl der 5-Sylows ist Teiler von 3 und  $\equiv 1 \pmod{5}$ .  
Sylow III

$\implies$  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  $\equiv 1 \pmod{3}$ .

$\implies$  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  $HK = G$ .

$\implies$   $G \simeq H \times K$ . Wir haben  $H \simeq C_5, K \simeq C_3$  (Gruppen von Ordnung  $p$  sind zyklisch).  
*Satz*

$\implies G \simeq C_5 \times C_3 \simeq C_{15}$ . □

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

*Beweis:* Die Anzahl der 5-Sylows teilt 2 und ist  $1 \pmod{5}$ .

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

$K \simeq C_5$ . Sei  $x \in K$  sodass  $K = \langle x \rangle$ .

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

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

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

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  $yx = x^r y$ :

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

$$\implies r^2 \equiv 1 \pmod{5}$$

$$\implies r = 2 \text{ und } r = 3 \text{ nicht möglich!}$$

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

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

$$\implies G \simeq H \times K \simeq C_2 \times C_5 = C_{10}.$$

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

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

Falls  $p \equiv 1 \pmod{q}$ , 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  $p^i \mid (p^e - k)$ , 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.

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

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

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

Betrachte  $G \curvearrowright X$  durch Linksmultiplikation.

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

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

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

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

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

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

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

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

## 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:

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

$$|B| \cdot |K| = p^d \text{ für alle Bahnen } B.$$

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

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

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

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

und somit  $a^{-1}Ka \leq H$ .  $\square$

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

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

*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:

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

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

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

$$|G| = p^e m = |Y| \cdot {}^e c \implies |Y| \mid m$$

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  $|N(H')| \mid |G|$ , 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).

$\implies |Y| \equiv 1 \pmod{p}$ . □

**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  $p_1, \dots, p_r$  sind.

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

Sei  $H_i$  eine  $p_i$ -Sylow für  $i = 1, \dots, n$ . 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  $\{x_1, \dots, x_n\} \subseteq G$  gibt, sodass  $G = \langle x_1, \dots, x_n \rangle$

**Satz 41.** Sei  $G$  eine endlich erzeugte abelsche Gruppe. Dann ist  $G$  isomorph zu  $\mathbb{Z}^n \times C_{p_1^{r_1}} \times \dots \times C_{p_n^{r_n}}$ , wobei  $p_1, \dots, p_n$  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).

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

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  $\dots xx^{-1} \dots$  oder  $\dots x^{-1}x \dots$  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:

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

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

*Beweis:* Induktion über die Länge von  $w$ .

Base case ist klar für  $|w| = 0$ .

Falls  $w$  reduziert ist, sind wir fertig.

Falls  $w$  nicht reduziert ist:

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

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

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

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

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

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

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

$\rightsquigarrow$  Äquivalenzrelation auf  $W'$ .

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

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

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

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

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

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

Assoziativität ist klar.

Neutrales Element: 1; folgt auch aus der Verknüpfung.

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

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

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

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

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

**Bemerkung 40.** Wir verwenden Produktschreibweise:

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

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

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

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

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

$$\begin{array}{ccc} X & \xrightarrow{f} & G \\ \downarrow & \swarrow \exists! \phi & \\ F & & \end{array}$$

*Beweis:* Sei  $w = x_1 \dots x_n$  ein Wort in  $W'$ . Wir definieren  $\phi(w) = f(x_1) \dots f(x_n)$ , 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.  $\square$

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

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

$\xrightarrow[1. \text{ Isosatz}]{} G \simeq F/N$ , wobei  $N = \text{Kern } \phi$ .

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  $G = \langle X \mid R \rangle$ .

$\langle X \mid R \rangle$  heisst **Präsentation** von  $G$ .

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

Sei  $\phi: G \rightarrow G'$  ein Homomorphismus mit  $N \subseteq \text{Kern } \phi$ . Dann existiert ein eindeutiger Homomorphismus  $\bar{\phi}: \overline{G} \rightarrow G'$ , sodass  $\bar{\phi} \circ \pi = \phi$ .

$$\begin{array}{ccc} G & \xrightarrow{\phi} & G' \\ \pi \searrow & \swarrow \text{Q} & \\ & \overline{G} & \end{array}$$

$$\exists! \bar{\phi}$$

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

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

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

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

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

*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

$$\phi: F \rightarrow D_n \text{ s.d. } R = \{x^n, y^n, xyxy\} \subseteq \text{Kern } \phi.$$

Sei  $N$  der kleinste Normalteiler, der  $R$  enthält.

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

$$\underset{\text{satz}}{\implies} \exists \text{ Homomorphismus } \bar{\phi}: F/N \rightarrow D_n, \text{ s.d. } \bar{\phi} \circ \pi = \phi,$$

wobei  $\pi: F \rightarrow F/N$ .

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

- $\bar{\phi}$  ist surjektiv, da  $\phi$  surjektiv ist.

- in  $F/N$  gilt  $\bar{x}^n = 1, \bar{y}^2 = 1, \bar{xyxy} = 1$

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

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

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

□

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

*Beweisidee.*

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

□

## Vorlesung 14

### Ringe (Kapitel 10 in Artin)

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

- (a)  $(R, +)$  ist eine abelsche Gruppe. Bezeichne das neutrale Element mit  $0$ .
- (b) Die Multiplikation ist assoziativ und hat ein neutrales Element  $1 \in R$ .
- (c) Für alle  $a, b, c \in R$  gilt:  $(a + b)c = ac + bc$  und  $c(a + b) = ca + cb$  (Distributivgesetz).

## Beispiele

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

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

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

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

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

Daraus folgt direkt:

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

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

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

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

**Definition 34.** Seien  $R, R'$  Ringe. Ein **Homomorphismus**  $\phi: R \rightarrow R'$  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

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

**Definition 35.** Sei  $\phi: R \rightarrow R'$  ein Ringhomomorphismus. Der **Kern** von  $\phi$  ist  $\text{Kern } \phi = \{a \in R \mid \phi(a) = 0\}$

**Bemerkung 46.** Ein Ringhomomorphismus  $\phi: R \rightarrow R'$  ist injektiv  $\Leftrightarrow \text{Kern } \phi = 0$ , 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  $\text{Kern } \phi$  kein Unterring (da  $1 \notin \text{Kern } \phi$ ).
- Falls  $a \in \text{Kern } \phi$  und  $r \in R$ , so ist auch  $ra \in \text{Kern } \phi$ .

**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.**

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

*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  $\phi: R \rightarrow R'$  ein Homomorphismus.  $\implies \text{Bild } \phi \subseteq R'$  ist ein Unterring.

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

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

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

$\implies$  abgeschlossen bez. Multiplikation.

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

□

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

**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  $(a) \neq (0)$ .

$$\begin{aligned} \Rightarrow (a) &= (1) = R \\ \Rightarrow \exists b \in R \text{ s.d. } ba &= 1 \\ \Rightarrow b &= a^{-1}. \text{ D.h. } R \text{ ist ein Körper.} \end{aligned}$$

□

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

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

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

$\Rightarrow \phi$  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.**

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

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

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  $R \rightarrow R$ .

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

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

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

$$\left\{ \sum_{i_1, \dots, i_n} a_{i_1 \dots i_n} x_1^{i_1} \cdots x_n^{i_n} \mid \begin{array}{l} a_{i_1 \dots i_n} \in R, (i_1, \dots, i_n) \in \mathbb{Z}_{\geq 0}^n, \\ \text{nur endlich viele der } a_{i_1 \dots i_n} \text{ sind nicht 0} \end{array} \right\}$$

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  $i = (i_1, \dots, i_n)$  und dann  $a_i x^i = a_{i_1 \dots i_n} x_1^{i_1} \cdots x_n^{i_n}$  (Multiindex Schreibweise).

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

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

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

$$\begin{array}{ccc} R & \xrightarrow{\phi} & R' \\ & \searrow i & \swarrow \Phi \\ & \mathcal{Q} & \\ & \downarrow & \\ R[x] & & \end{array}$$

*Beweis:* Multindex-Schreibweise

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

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  $\Phi: R[x] \rightarrow R \quad \sum r_i x^i \mapsto \sum r'_i \alpha^i$  ist ein Homomorphismus.

Wir haben:

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

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

und  $\Phi(1) = 1$  (per Definition).  $\square$

**Bemerkung 54.** Sei  $\psi: R \rightarrow R'$  ein Homomorphismus  $\rightsquigarrow$  Homomorphismus

$$R \xrightarrow{\quad} R' \xleftarrow{\quad} R'[x]$$

$\phi$

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

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

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

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

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

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

$$R[x][y] \underset{\substack{\simeq \\ \text{wollen wir zeigen}}}{\sim} R[x, y]$$

**Beispiel 23.**

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

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

*Beweis:* Es gibt einen eindeutigen Homomorphismus  $\Phi: R[x, y] \rightarrow R[x][y]$  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  $\psi: R[x] \hookrightarrow R[x, y]$

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

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

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

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

□

## Vorlesung 16

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

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

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

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

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

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

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

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

**Definition 45.**  $\text{Kern } \phi \subseteq \mathbb{Z}$  ist Ideal  $\implies \text{Kern } \phi = n\mathbb{Z}$  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:

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

$$\begin{aligned} \text{Sei } g_1 &= g - b_m^{-1} a_n x^{n-m} f \\ &= a_0 + \cdots + a_{n-m} x^{n-m} - b_m^{-1} a_n b_0 - \cdots - \cancel{b_m^{-1} a_n b_m x^n} \end{aligned}$$

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

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

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

□

**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  $f \in K[x] \setminus \{0\}$  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  $f \in I \setminus \{0\}$  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.

$\pi: R \rightarrow R/I$  ist ein Gruppenhomomorphismus.

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

$$\pi: R \rightarrow \overline{R}, \quad r \mapsto r + I \text{ ein Ringhomomorphismus ist.}$$

(b)  $\text{Kern } \pi = I$

*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  $r + I$ .

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

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

$$\implies vu + I = rs + I$$

Man überprüfe direkt, dass  $\bar{R}$  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**.  $\square$

## Vorlesung 17

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

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

$$\begin{array}{ccc} R & \xrightarrow{\phi} & R' \\ & \searrow \pi & \swarrow \exists! \bar{\phi} \\ & \bar{R} = R/I & \end{array}$$

(Quiver diagram)

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

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

**Behauptung 3** (Clicker-Frage). *Sei  $\phi: R \rightarrow R'$  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  $a' \in \phi(I)$

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

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

$\square$

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

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

$$\begin{aligned} &\implies \phi(a+b) = \phi(a) + \phi(b) \in J \\ &\implies a+b \in \phi^{-1}(J), \quad 0 \in \phi^{-1}(J) \end{aligned}$$

Sei  $r \in R$

$$\begin{aligned} &\implies \phi(ra) = \phi(r)\phi(a) \in J \\ &\implies ra \in \phi^{-1}(J). \end{aligned}$$

□

**Satz 58** (Entsprechungssatz). *Sei  $R$  ein Ring,  $I \subseteq R$  ein Ideal,  $\pi: R \rightarrow R/I = \bar{R}$  Quotient.*

Dann gilt:

(a) Die Abbildung  $\Phi: \{\text{Ideale } J \subseteq R \mid I \subseteq J\} \rightarrow \{\text{Ideale in } R\}$

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

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

*Beweis:* (a)  $\pi(J) \subseteq R$  ist ein Ideal, da  $\pi$  surjektiv ist. Ist  $H \subseteq \bar{R}$  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  $H \subseteq \bar{R}$ .

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.  $\pi(x) \in \pi(J)$

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

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

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

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  $\phi: \bar{R} \rightarrow \bar{R}/\pi(J)$  Quotient.

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

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

$$\implies R/\pi(J) \simeq R/J.$$

□

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  $\bar{R}$  der Ring, den man durch Einführung der Relation  $1+3i = 0$  erhält, d.h.  $\bar{R} = \mathbb{Z}[i]/(1+3i)$ .

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

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

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

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

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

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

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

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

$\implies \phi$  ist surjektiv.

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

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

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

$$\implies b = -3a$$

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

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

$$\implies \bar{R} \simeq \mathbb{Z}/\text{Kern } \phi = \mathbb{Z}/10\mathbb{Z}$$

□

## Adjunktion von Elementen

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

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

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

(Beweis  $(x^2 + 1) \subseteq \text{Kern } \pi$ :

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

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

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

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

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

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

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

wobei  $\bar{c}_i$  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

$$\Phi: R^n \rightarrow R[\alpha] = R[x]/(f)$$

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

eine Bijektion.

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

Division mit Rest:

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

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

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

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

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

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

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

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

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

□

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

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

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  $R' = K[t, x]/(xt - 1)$ .

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.**  $f = x^2$

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

Der Homomorphismus  $\phi: R \rightarrow R[\alpha]$  ist nicht immer injektiv.

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

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

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

## Integritätsbereiche & Quotientenkörper

Sei  $R$  ein Ring.

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

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

**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  $f, g \in R[x] \setminus \{0\}$ . Wir schreiben

$$\begin{aligned} f &= a_0 + \cdots + a_n x^n & a_n \neq 0 \\ g &= b_0 + \cdots + b_m x^m & b_m \neq 0 \\ \implies fg &= \underbrace{a_n b_n}_{\neq 0 \text{ da } R \text{ IB}} x^{m+n} + \cdots \\ \implies fg &\neq 0 \end{aligned}$$
□

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

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

Man betrachte:  $m_a: R \setminus \{0\} \rightarrow R \setminus \{0\}$

$b \mapsto ab$

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

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

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

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

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

**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  $a_1 b_2 = a_2 b_1$ .

Dies ist eine Äquivalenzrelation.

Reflexivität und Symmetrie sind klar.

Transitivität:

$$\begin{aligned} &\text{Falls } \frac{a_1}{b_1} \approx \frac{a_2}{b_2} \approx \frac{a_3}{b_3} \\ &\implies a_1 b_2 = a_2 b_1 \text{ und } a_2 b_3 = a_3 b_2 \\ &\implies a_1 b_2 b_3 = a_2 b_1 b_3 = a_3 b_2 b_1 \\ &\stackrel{b_2 \neq 0}{\implies} a_1 b_3 = a_3 b_1 \\ &\implies \frac{a_1}{b_1} \approx \frac{a_3}{b_3}. \end{aligned}$$

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  $K$ .

$$\begin{aligned} \frac{a}{b} \cdot \frac{c}{d} &= \frac{ac}{bd} \\ \frac{a}{b} + \frac{c}{d} &= \frac{ad+bc}{bd} \end{aligned}$$

**Zu überprüfen:**

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

$\rightsquigarrow$  kleine Übung.

Wir haben ausserdem

$$i: R \rightarrow K$$

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

Dies ist ein Ringhomomorphismus (klar)

$$\text{und injektiv: } \frac{a}{1} = \frac{b}{1} \Leftrightarrow a \cdot 1 = b \cdot 1. \quad \square$$

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

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

## Vorlesung 19

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

$$\begin{array}{ccc} R & \xrightarrow{\phi} & K' \\ & \searrow i & \nearrow \exists! \Phi \\ & K & \end{array}$$

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

$\Phi$  ist eindeutig.

$\Phi$  ist wohldefiniert:

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

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

Man überprüft direkt, dass das ein Homomorphismus ist.  $\square$

## 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  $n\mathbb{Z} \subseteq m\mathbb{Z} \Leftrightarrow m|n$ .

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

**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:

$$\{ \text{Ideale } I \subseteq R \text{ s.d. } I \subseteq J \} \xrightarrow{1:1} \{ \text{Ideale in } R/I \}$$

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

**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  $e_a: \mathbb{C}[x] \rightarrow \mathbb{C} \quad f \mapsto f(a)$

D.h. es gibt eine Bijektion

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

*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.

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

$$\implies x - a | f$$

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

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

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

Umgekehrt:

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

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

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

*Beweis:* Übung.  $\square$

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

*Beweis:* Siehe Artin. □

Das ist der Beginn der Algebraischen Geometrie.

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

**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:**  $I \subseteq R$  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:

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

$d$  heisse der **größte gemeinsame Teiler** von  $a$  und  $b$ . Wir schreiben  $d = \text{ggT}(a, b)$ .

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

- (a)  $\exists r, s \in \mathbb{Z}$  s.d.  $d = ar + bs$
- (b)  $d|a$  und  $d|b$
- (c) Sei  $e \in \mathbb{Z}$  sodass  $e|a$  und  $e|b$ , dann gilt  $e|d$ .

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

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

(c)  $e|a$  und  $e|b$

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

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

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

□

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

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

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

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

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

$$\implies p|b.$$

□

**Satz 69.** Sei  $a \in \mathbb{Z}, a \neq 0$ . Dann gibt es ein  $k \geq 0$  und Primzahlen  $p_1, \dots, p_k > 0$  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  $b, b' < a$ .

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

$\implies a$  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  $p_1|q_1 \cdots q_m$

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

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

□

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  $a|b$ .
- $a$  ist ein echter Teiler von  $b$ , falls  $b = aq$ , sodass weder  $a$  noch  $q$  eine Einheit sind.
- $a$  und  $b$  sind assoziiert, falls  $a|b$  und  $b|a$ .
- $a$  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  $p|ab$ , so gilt  $p|a$  oder  $p|b$ .

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

Beweis: “ $\Rightarrow$ ”

$$a = qb \text{ und } b = q'a$$

$$\Rightarrow a = qq'a$$

$$\Rightarrow 1 = qq', \text{ d.h. } q \text{ ist eine Einheit.}$$

“ $\Leftarrow$ ” klar.  $\square$

**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  $p = ab \Rightarrow p|a$  oder  $p|b$ .

oBdA  $p|b$ .

$$\Rightarrow b = rp \text{ für } r \in R$$

$$\Rightarrow p = arp$$

$$\Rightarrow 1 = ar$$

$$\Rightarrow a \text{ ist Einheit, d.h. } p \text{ hat keine echten Teiler.} \quad \square$$

## 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:  $(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \dots$

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

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  $a_1 = a_2 b_2 = a_3 b_3 b_2 = \dots$  eine unendliche Folge von Hauptidealen. Dann haben wir eine unendliche Kette  $(a_1) \subsetneq (a_2) \subsetneq (a_3) \subsetneq \dots$   $\square$

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

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

In  $R$ :

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

das heisst

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

$\rightsquigarrow$  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  $i = 1, \dots, n$ .

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

*Beweis:* “ $\Leftarrow$ ” 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.  $p_1 | q_i$  für ein  $i$ . OBdA  $i = 1$ .

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

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

Behauptung folgt per Induktion über  $n$ .

“ $\Rightarrow$ ” Man nehme an, es gibt ein  $p \in R$ , das irreduzibel aber nicht prim ist.

$$\Rightarrow \exists a, b \in R, \text{s.d. } p | ab \text{ aber } p \nmid a \text{ und } p \nmid b.$$

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  $\Rightarrow R$  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  $r|ab$  folgt, dass  $r|a$  oder  $r|b$ .

prim  $\implies$  irreduzibel, aber im Allgemeinen irreduzibel  $\not\implies$  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  $a|b$ . Falls  $c$  assoziiert ist zu  $a$ , so gilt  $c|b$ .

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

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

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

*Beweis:* “ $\implies$ ”

Falls  $a|b$ , so folgt  $p_1|b$ .

$\implies p_1|q_i$  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  $q_2$ .

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

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

“ $\Leftarrow$ ” 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)  $d|a$  und  $d|b$

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

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  $d|a$  und  $d|b$ .

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

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

$$\implies e|d.$$

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  $r|ab$  und  $r \nmid a$ .

**z.z:**  $r|b$ .

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.

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

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

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

$$\implies r|b$$

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

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

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

$\implies (q)$  ist maximal.

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

$\implies (q) \subsetneq (a) \subsetneq (1)$ , d.h.  $(q)$  ist nicht maximal.  $\square$

**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

$(a_1) \subsetneq (a_2) \subsetneq \dots$

**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  $n \implies a + b \in (a_n) \subseteq I$  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).  $\square$

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

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

Jedes Polynom in  $K[x] \setminus \{0\}$  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).  $\square$

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

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

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

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

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

**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  $f \Leftrightarrow (x - \alpha) | f$ .

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

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.  $\square$

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  $\sigma: R \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$ .

**Definition 55.**  $R$  ist ein **euklidischer Ring**, falls es eine Größenfunktion  $\sigma: R \setminus \{0\} \rightarrow \mathbb{Z}_{\geq 0}$  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

$$\begin{aligned}\frac{a}{b} &= \frac{a\bar{b}}{|b|^2} = \frac{m_1m_2 + n_1n_2}{m_2^2 + n_2^2} + i \frac{n_1m_2 - m_1n_2}{m_2^2 + n_2^2} \\ &= \underbrace{q_1 + iq_2}_{=:q \in \mathbb{Z}[i]} + (r_1 + ir_2)\end{aligned}$$

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

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

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

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

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

□

**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  $\sigma(b)$  minimal.

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

□

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

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

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

## Vorlesung 23

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

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

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

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

**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.  $f_1 = mf_0, f_0 \in \mathbb{Z}[x]$  primativ.

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

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

$$\implies ca_i = db_i$$

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

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

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

$$\implies f_0 = g_0 \text{ und } c = d.$$

□

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

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

**Bemerkung 64.** Falls  $f(x) \in \mathbb{Z}[x]$  primitiv ist, so ist  $\bar{f}(x) \in \mathbb{F}_p[x]$  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  $\mathbb{Z}[x] \rightarrow \mathbb{F}_p[x]$

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

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

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

**Satz 80.** (a) Seien  $f, g \in \mathbb{Q}[x]$  und  $f_0, g_0 \in \mathbb{Z}[x]$  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  $\mathbb{Q}[x]$  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.  $\underset{\text{Gauss}}{\implies} f_0$  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  $\mathbb{Z}[x]$ .

$\underset{(b)}{\implies} f_0$  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.

$f = ch_0f_1$  und  $g = ch_0g_1$  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  $\mathbb{Q}[x]$

$\xrightarrow{\text{Satz}}$   $f$  hat keine echten Teiler in  $\mathbb{Z}[x]$ .  $\square$

**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:* “ $\implies$ ” 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  $c = 1$  oder  $f_0 = 1$ .

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.  $\square$

**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  $f | gh$ .

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

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

$\xrightarrow[\text{Gauss}]{} h_0g_0$  primitiv.

$\implies$  es gibt einen Koeffizienten  $a$  von  $g_0h_0$ , der nicht durch  $p$  teilbar ist.

Da aber  $p | gh$  und  $gh = cdg_0h_0$

$\implies p | cda$

$\implies p | c$  oder  $p | d$

$\implies p | g$  oder  $p | h$ .

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

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

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

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

**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  $p_i, i = 1, 2, \dots$

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

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

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

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

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.  $\square$

**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).  $\square$

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

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

## Vorlesung 24

### Kriterien für Irreduzibilität

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

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

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

*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  $\pmod{p}$ .

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

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

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

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

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

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

$\implies \bar{f}$  ist nicht irreduzibel. □

**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  $\bar{f} \pmod{p}$  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:

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

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

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

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

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

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

- (i)  $p \nmid a_n$
- (ii)  $p | a_i$  für  $i = 0, \dots, n-1$
- (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  $\bar{f}$  die Restklasse von  $f \pmod{p}$ .

$$\implies \bar{f} = \bar{a}_n \bar{x}^n, \bar{a}_n \neq 0.$$

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

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

$$\implies \bar{g} \text{ und } \bar{h} \text{ teilen } \bar{a}_n \bar{x}^n$$

$$\implies \bar{g} \text{ und } \bar{h} \text{ sind Monome.}$$

$\implies$  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  $h$ .

$$\implies \text{der konstante Koeffizient von } f \text{ ist } a_0 = b_0 c_0.$$

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

$$\implies f \text{ ist irreduzibel.} \quad \square$$

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

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

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

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

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

Substituiere  $x = y + 1$

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

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

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

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

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

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

$f(y+1)$  ist irreduzibel.

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

## Vorlesung 25

### Körper

**Definition 59.** Ein **Körper** ist ein Ring, der nicht der Nullring ist, und in dem jedes Element ausser 0 invertierbar ist.

**Bemerkung 66.** Körper sind euklidisch:  $\forall a, b \in K^* \exists q \in K^*$  sodass  $a = qb + 0$ .

**Beispiel 51.** Teilkörper von  $\mathbb{C}$  (d.h. Unterringe, die auch Körper sind). Diese heißen **Zahlkörper**.

**Beispiel 52.** Endliche Körper, z.B.  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ,  $p$  prim (es gibt auch andere!).

**Definition 60.** Eine **Körpererweiterung** ist ein Paar von Körpern  $L \supseteq K$ . Wir schreiben oft  $L/K$  ( $L$  ist eine Erweiterung von  $K$ ).

**Beispiel 53.**  $\mathbb{C}$  ist eine Erweiterung von  $\mathbb{R}$ .

**Bemerkung 67.** Wenn  $L/K$  eine Körpererweiterung ist, dann ist  $L$  ein  $K$ -Vektorraum.

**Definition 61.** Sei  $L/K$  eine Körpererweiterung. Ein Element  $\alpha \in L$  heisst **algebraisch über  $K$** , falls es ein Polynom  $f(x) \in K[x] \setminus \{0\}$  gibt, sodass  $f(\alpha) = 0$ .

**Bemerkung 68.** Wir können immer annehmen, dass  $f$  normiert ist.

**Definition 62.** Ein  $\alpha \in L$  heisst **transzendent über  $K$** , wenn es nicht algebraisch ist.

**Beispiel 54.**  $\mathbb{C}/\mathbb{Q}$ , dann ist

- $\sqrt{2}$  ist algebraisch über  $\mathbb{Q}$ .
- $\pi$  ist transzendent über  $\mathbb{Q}$ .

- $i$  ist algebraisch über  $Q$ .

**Beispiel 55.**  $\mathbb{C}/\mathbb{R}$ , dann ist  $\pi$  algebraisch über  $R$ .

$$(f(x) = x - \pi \in \mathbb{R} \implies f(\pi) = 0).$$

Sei  $L/K$  eine Körpererweiterung. Wir betrachten den Homomorphismus  $\phi: K[x] \rightarrow L$   $f \mapsto f(\alpha)$ .

Dann ist  $\alpha$  transzendent genau dann, wenn  $\text{Kern } \phi = 0 \Leftrightarrow \phi$  injektiv.

Falls  $\alpha$  algebraisch ist, so ist  $\text{Kern } \phi \subseteq K[x]$  ein Ideal.

$\xrightarrow[K[x] \text{ ist HIR}]{} \text{Kern } \phi = (f)$ , wobei  $f$  das normierte Polynom vom kleinsten Grad in  $\text{Kern } \phi$  ist.

Dieses Polynom heisst das **Minimalpolynom** von  $\alpha$ .

**Bemerkung 69.** Dieses  $f$  ist das einzige normierte irreduzible Polynom in  $\text{Kern } \phi$ .

*Beweis:*

- $f$  ist irreduzibel: Falls  $f = gh$  in  $K[x]$ 
 $\implies f(\alpha) = g(\alpha)h(\alpha) = 0$ 
 $\implies g(\alpha) = 0$  oder  $h(\alpha) = 0$ 
 $\implies g$  oder  $h$  ist konstant.
- Sei  $g \in \text{Kern } \phi = (f)$ ,  $g \neq f$ , dann ist  $g = fh$ 
 $\implies g$  nicht irreduzibel (falls  $\deg g > \deg f$ ) oder  $g$  ist nicht normiert.

□

**Bemerkung 70.** Das Minimalpolynom  $f$  hängt sowohl von  $\alpha$  als auch von  $K$  ab.

**Beispiel 56.** Sei  $K = \mathbb{Q}[i] \subseteq \mathbb{C}$  und  $\alpha = \sqrt{i} = \frac{1}{2}\sqrt{2}(1+i)$ . Das Minimalpolynom von  $\alpha$  über  $\mathbb{Q}$  ist  $x^4 + 1$ . Über  $K$  ist aber  $x^4 + 1 = (x^2 + i)(x^2 - i)$ .

Das Minimalpolynom von  $\alpha$  über  $\mathbb{Q}[i]$  ist  $x^2 - i$ .

**Definition 63.** Seien  $L/K$  eine Körpererweiterung und  $\alpha \in L$ . Wir bezeichnen mit  $K(\alpha) \subseteq L$  den kleinsten Körper, der  $K$  und  $\alpha$  enthält.

Ähnlich für  $\alpha_1, \dots, \alpha_n \in L$  ist  $K(\alpha_1, \dots, \alpha_n)$  der kleinste Körper, der  $K$  und  $\alpha_1, \dots, \alpha_n$  enthält.

**Bemerkung 71.** Wir hatten  $K[\alpha] = \{a_n\alpha^n + \dots + a_0 \mid a_i \in K\} \subseteq L$ .

$K(\alpha)$  ist isomorph zum Quotientenkörper von  $K[\alpha]$ .

*Beweis:* Kleine Übung. □

**Bemerkung 72.** Falls  $\alpha \in L$  ein transzendentes Element ist, so ist  $K[\alpha] \simeq K[x]$  und somit  $K(\alpha) \simeq K(x)$ .

**Satz 87.** Seien  $L/K$  eine Körpererweiterung und  $\alpha \in L$  algebraisch über  $K$  mit Minimalpolynom  $f \in K[x]$ .

- (a) Der Homomorphismus  $\phi: K[x] \rightarrow K[\alpha]$   $g \mapsto g(\alpha)$  induziert einen Isomorphismus

$$K[x]/(f) \xrightarrow{\sim} K[\alpha]$$

und  $K[\alpha]$  ist ein Körper. Insbesondere ist  $K(\alpha) = K[\alpha]$ .

- (b) Seien allgemeiner  $\alpha_1, \dots, \alpha_n \in L$  algebraisch über  $K$ . Dann ist  $K[\alpha_1, \dots, \alpha_n] = K(\alpha_1, \dots, \alpha_n)$ .

*Beweis:*

- (a)  $\phi$  ist surjektiv  $\implies \phi$  induziert den Isomorphismus

$$K[x]/(f) + K[x]/\text{Kern } \phi \xrightarrow{\sim} K[\alpha]$$

Da  $f$  irreduzibel ist, ist  $(f)$  maximal

$\implies K[\alpha]$  ist ein Körper.

- (b) Das folgt per Induktion:

$$\begin{aligned} K[\alpha_1, \dots, \alpha_n] &= K[\alpha_1, \dots, \alpha_n][\alpha_n] \\ &= K(\alpha_1, \dots, \alpha_n)[\alpha_n] \\ &= K(\alpha_1, \dots, \alpha_n) \end{aligned}$$

□

Wir haben gesehen, dass für ein normiertes  $f \in R[x]$  so ist

$$K^n \xrightarrow{\sim} K[\alpha] = K[x]/(f)$$

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

eine Bijektion. Daraus folgt direkt:

**Satz 88.** Sei  $\alpha$  algebraisch über  $K$  mit Minimalpolynom  $f$ . Falls  $\deg f = n$ , so ist  $(1, \alpha, \dots, \alpha^{n-1})$  eine Basis von  $K[\alpha]$  als Vektorraum über  $K$ .

## Der Grad von einer Körpererweiterung

**Definition 64.** Sei  $L/K$  eine Körpererweiterung. Der **Grad**  $[L : K]$  von  $L/K$  ist die Dimension von  $L$  als  $K$ -Vektorraum.

$L/K$  heisst **endlich**, falls  $[L : K]$  endlich ist.

**Beispiel 57.**  $(1, i)$  ist eine Basis von  $\mathbb{C}$  als  $\mathbb{R}$ -Vektorraum.  $\Rightarrow [\mathbb{C} : \mathbb{R}] = 2$ .

**Satz 89.** Ist  $\alpha$  algebraisch über  $K$ , so ist  $[K(\alpha) : K]$  der Grad vom Minimalpolynom über  $\alpha$ .

*Beweis:* Folgt direkt aus Satz 88. □

Sei  $f \in K[x]$  das Minimalpolynom von  $\alpha$ .

$$\deg f = 1 \Leftrightarrow f(x) = x - a \Leftrightarrow \alpha \in K$$

**Bemerkung 73.** Grad  $\alpha$  ist  $\infty \Leftrightarrow \alpha$  ist transzendent über  $K$ .

**Satz 90.** Seien  $K \subseteq L \subseteq M$  Körper. Dann gilt:

$$[M : K] = [M : L][L : K]$$

*Beweis:* Sei  $(\alpha_1, \dots, \alpha_n)$  eine  $K$ -Basis von  $L$  und  $\beta_1, \dots, \beta_m$  eine  $L$ -Basis von  $M$ .

Behauptung:  $(\alpha_i \beta_j \mid 1 \leq i \leq n, 1 \leq j \leq m)$  ist eine  $K$ -Basis von  $M$ .

Bew: Sei  $x \in M$

$$\Rightarrow x = \sum_{j=1}^m a_j \beta_j, \quad a_j \in L$$

$$a_j = \sum_{i=1}^n a_{ij} \alpha_i, \quad a_{ij} \in K$$

$$\Rightarrow x = \sum_{i,j} a_{ij} \alpha_i \beta_j$$

$\Rightarrow (\alpha_i \beta_j)$  erzeugt  $M$  als  $K$ -Vektorraum.

Wir nehmen an, dass  $\sum a_{ij} \alpha_i \beta_j = \sum_{i=1}^n \left( \sum_{j=1}^m a_{ij} \alpha_j \right) \beta_i = 0$

$$\stackrel{(\beta_1, \dots, \beta_m) \text{ ist Basis}}{\Rightarrow} \sum a_{ij} \alpha_j = 0 \quad \forall i$$

$$\stackrel{(\alpha_1, \dots, \alpha_n) \text{ ist Basis}}{\Rightarrow} a_{ij} = 0 \quad \forall i, j$$

$\Rightarrow (\alpha_i \beta_j)$  ist linear unabhängig.

$\Rightarrow (\alpha_i \beta_j)$  ist Basis.

Falls  $[M : L]$  oder  $[L : K]$  unendlich sind, geht der Beweis ähnlich. □