# Einleitung: Was ist Algebra?

| | |
|---|---|
| historisch: | Lösen von Gleichungen |
| modern: | Studium algebraischer Strukturen |

Beispiel: Lineare Algebra: Lösen linearer Gleichungssysteme

$\rightsquigarrow$ · **algebraische Strukturen:**

Vektorräume, Körper, Gruppen

· **Lösen von Polynomgleichungen:**

$$f(X) := X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 = 0 \qquad (a_1, \ldots, a_{n-1} \in \mathbb{Z})$$

Frage: Wie viele Lösungen? Wo? Von welcher Art?

$\implies$ zum Beispiel: über $\mathbb{C}: f(X) = \prod_{i=1}^{n}(X - \lambda_i)$ mit $(\lambda_1, \ldots, \lambda_n) \in \mathbb{C}$

('Fundamentalsatz der Algebra' 18. Jahrhundert)

n=1: ✓

n=2: Lösungsformel: $\lambda_{1,2} = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_0}}{2}$

n=3: Formel von Cardano (1545)

n=4: Formel von Ferrari

n=5: ?

$\implies$ Satz von Abel-Ruffini:(1824):

Es gibt keine Lösungsformel für Gleichungen vom Grad $\geq 5$

Vollständige Erklärung: Evariste Galois (1832)

- **Studium kleinster Körper** $\mathbb{Q}(\lambda_1, \ldots, \lambda_n)$

$\mathbb{Q}(\lambda_1, \ldots, \lambda_n)$ hat die Eigenschaft, alle Lösunngen von $f(X) = 0$ zu enthalten.
$\rightsquigarrow$ Beziehung zwischen Eigenschaften der Gleichung $f(X) = 0$ (und ihren Lösungen) und der Gruppe der Automorphismen des Körpers $\mathbb{Q}(\lambda_1, \ldots, \lambda_n)$.

$$\begin{array}{lclcl} f(X) = 0 & \rightsquigarrow & \mathbb{Q}(\lambda_1, \ldots, \lambda_n) & \rightsquigarrow & \mathrm{Aut}(\mathbb{Q}(\lambda_1, \ldots, \lambda_n)) \\ \text{Ring} & \rightsquigarrow & \text{Körper} & \rightsquigarrow & \text{Gruppe} \end{array}$$

# Inhalt der Vorlesung

· **Einleitung:** Ganze Zahlen

· **Kapitel I:** Gruppen

· **Kapitel II:** Ringe

· **Kapitel III:** Körper

# Literatur

· **Bosch:** Algebra

# 0 Einleitung

## 0.1 Die ganzen Zahlen

### 0.1.1 Bemerkung

Wir nehmen die ganzen Zahlen

$$\mathbb{Z} = \{\ldots, -1, 0, 1, 2, \ldots\}$$

als bekannt und gegeben an.
Wir wissen: $(\mathbb{Z}, +, \cdot)$ ist ein (kommutativer) Ring:

**1)**
Addition ist assiozativ, kommutativ, mit neutralem Element 0 und Inversen -x

**2)**
Multiplikation: assiozativ, kommutativ

**3)**
Es gilt das Distributivgesetz:

$$a(b + c) = ab + ac \qquad (\forall a, b, c \in \mathbb{Z})$$

Konvention:

$$\mathbb{N} = \{1, 2, 3, \ldots\}$$

$$\mathbb{N}_0 = \{0, 1, 2, 3, \ldots\}$$

Eigenschaften von $\mathbb{Z}$:

· **Ordnung:** $a < b \iff b - a \in \mathbb{N}$

· **Wichtig:** für $a \in \mathbb{N}$ ist

$$\{x \in \mathbb{N} : x \leq a\}$$

endlich $\implies$ Jede Teilmenge $\emptyset \neq S \subset \mathbb{N}$ hat ein kleinstes Element.

### 0.1.2 Definition

Seien $a, b \in \mathbb{N}$. Dann:

$$a|b \quad \text{(a \underline{teilt} b)}$$

$:\iff \exists x \in \mathbb{N} : ax = b$

### 0.1.3 Bemerkung

$$a|b \implies a \leq b$$

### 0.1.4 Definition

Seien $a, b \in \mathbb{N}$

· $\mathrm{ggT}(a, b) := \max\{c \in \mathbb{N} : c|a \ \wedge \ c|d\}$
"größter gemeinsamer Teiler von a und b"

· $\mathrm{kgV}(a, b) := \min\{c \in \mathbb{N} : a|c \ \wedge \ b|c\}$
"kleinstes gemeinsames Vielfaches von a und b"

### 0.1.5 Satz (Division mit Rest)

Für $a \in \mathbb{N}_0, b \in \mathbb{N}$ gibt es eindeutig bestimmte $q, r \in \mathbb{N}_0$ mit

- $a = qb + r$
- $r < b$

**Beweis:**

- Existenz: Induktion
- Eindeutigkeit: Angenommen:

$$\begin{aligned} & a = qb + r = q'b + r', \quad (r, r' < b) \\ \Longrightarrow\ & (q - q')b = r - r' \\ \Longrightarrow\ & |q - q'|b = |r - r'| < b \\ \Longrightarrow\ & q - q' = 0 \implies r - r' = 0 \quad \square \end{aligned}$$

### 0.1.6 Satz

Für alle $a, b \in \mathbb{N}$ existieren $x, y \in \mathbb{Z}$ mit

$$\mathrm{ggT}(a, b) = ax + by$$

Beweis: Euklidischer Algorithmus

**Setze:** $r_0 = a, \quad r_1 := b$

**Schreibe:** $r_{i-1} := q_i r_i + r_{i+1} \quad (r_{i+1} < r_i)$
So lange bis $r_{n+1} = 0$

$$\Longrightarrow \quad \begin{aligned} r_0 &= q_1 r_1 + r_2 && \Longrightarrow r_n | r_0 \\ r_1 &= q_2 r_2 + r_3 && \Longrightarrow r_n | r_1 \\ &\vdots && \qquad \vdots \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n && \Longrightarrow r_n | r_{n-1} \\ r_{n-1} &= q_n r_n && \Longrightarrow r_n | r_{n-1} \end{aligned}$$

Einsetzen liefert:

$$r_n = r_0 x + r_1 y \quad (\text{mit } x, y \in \mathbb{Z})$$

Man sieht: $r_n \mid a\ , \quad r_n \mid b$.

Ist $c|a\ , \quad c|b, \quad$ so folgt

$$c | ax + by = r_n$$

also $c \leq r_n$ für beliebige $c$. Damit

$$r_n = \max\{c \in \mathbb{N} : c|a \ \wedge\ c|b\} \quad \square$$

### 0.1.7 Korollar

$$c|a \ \wedge\ c|b \implies c|\mathrm{ggT}(a, b)$$

### 0.1.8 Definition

$p \in \mathbb{N}$ Primzahl $\iff$

$\forall x \in \mathbb{N}:$

- $x|p \implies x = 1 \vee x = p$
- $p \neq 1$

### 0.1.9 Satz (Hauptsatz der Arithmetik)

(Satz über die eindeutige Primzerlegung)

Jedes $n \in \mathbb{N}$ lässt sich schreiben als

$$n = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r} \quad (r \in \mathbb{N}_0)$$

mit Primzahlen $p_1, \ldots, p_r$ und $e_1, \ldots, e_r \in \mathbb{N}$.
Dabei sind $p_1, \ldots, p_r$ und $e_1, \ldots, e_r$ eindeutig bis auf Reihenfolge.

Beweis: Induktion

$\Longrightarrow$ Später allgemeiner

### 0.1.10 Bemerkung

Man verallgemeinert für $a, b \in \mathbb{Z}$:

$$a|b \iff \exists x \in \mathbb{Z} : ax = b$$

$\mathrm{ggT}(a, b)$ ist das $c \in \mathbb{N}_0$ mit $c|a$ und $c|b$ und

$$\forall d \in \mathbb{Z} : d|a \wedge d|b \implies d|c$$

Satz 0.5 gilt entsprechend:

$$\forall a \in \mathbb{Z} \forall b \neq 0 \in \mathbb{Z} \exists q, r \in \mathbb{Z} \text{ mit } a = qb + r, \quad 0 \leq r < |b|$$

Satz 0.6 gilt entsprechend:

$$\forall a, b \in \mathbb{Z} \exists x, y \in \mathbb{Z} : \mathrm{ggT}(a, b) = ax + by$$

### 0.1.11 Definition

$$a \equiv b \mod n \iff n|(a - b)$$

### 0.1.12 Bemerkung

Durch $a \equiv b \mod n$ wird eine Äquivalenzrelation auf $\mathbb{Z}$ definiert mit Äquivalenzklassen:

$$\overline{a} := a + n\mathbb{Z} := \{b \in \mathbb{Z} : a \equiv b \mod n\} = \{a + kn : k \in \mathbb{Z}\}$$

Die Menge der Restklassen

$$\mathbb{Z}/_{n\mathbb{Z}} = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

wird durch

$$\overline{a} + \overline{b} = \overline{a + b}, \quad \overline{a} \cdot \overline{b} = \overline{ab}$$

zu einem Ring. (Wohldefinierheit zeigen) $a' = a + kn, \quad b' = b + ln$

$$a'b' = ab + (kb + al + kln)n \equiv ab \mod n$$

d.h. $a'b' \in \overline{ab}$

(vgl. $\mathbb{Z}_n = \{1, \ldots, n{-}1\}$ mit Addition und Multiplikation modulo n, die Ringe sind isomorph)

### 0.1.13 Satz

Für $a \in \mathbb{Z},\ n \in \mathbb{N}$ sind äquivalent:

(1) $\mathrm{ggT}(a, n) = 1$ (a und n sind teilerfremd)

(2) es existiert $x \in \mathbb{Z}$ mit $\overline{a} \cdot \overline{x} = \overline{1}$ ($ax \equiv 1 \mod n$, gilt in $\mathbb{Z}/_{n\mathbb{Z}}$)

(3) $\mathbb{Z}/_{n\mathbb{Z}} = \{\overline{a}, 2\overline{a}, \ldots\}$

**Beweis.**

(1) $\implies$ (2)

Nach 0.6 existieren $x, y \in \mathbb{Z}$ mit

$$\begin{aligned} & ax + ny = 1 \\ \implies\ & \overline{a} \cdot \overline{x} = \overline{ax} = \overline{1 - ny} = \overline{1} \end{aligned}$$

(2) $\implies$ (3)

$\overline{a} \cdot \overline{x} = \overline{1}$, O.B.d.A. $x \in \mathbb{N}$

$$\implies \overline{kax} = \overline{k} \quad \forall k \in \mathbb{N}_0$$

(3) $\implies$ (1)

$\overline{1} = \overline{ka} \implies$ ex. $y \in \mathbb{Z} : ka + ny = 1$

Dann gilt für $c \in \mathbb{N}$:

$$\begin{aligned} c|a \wedge c|n &\implies c|ka + ny = 1 \\ &\implies c = 1 \\ &\implies \mathrm{ggT}(a, n) = c = 1 \end{aligned}$$ □

### 0.1.14 Definition

$(\mathbb{Z}/_{n\mathbb{Z}})^{\times} := \{\overline{a} : \mathrm{ggT}(a, n) = 1\}$

Eulersche Phi-Funktion:

$$\phi(n) := |(\mathbb{Z}/_{n\mathbb{Z}})^{\times}|$$

### 0.1.15 Bemerkung

Ist $p \in \mathbb{N}$ eine Primzahl, dann gilt

$$\phi(p) = p - 1$$

# I Gruppen

## I.1 Grundlegende Definitionen

### I.1.1 Definition (Gruppe)

Sei G eine Menge, $\bullet : G \times G \to G$ eine Abbildung.

Dann heißt $(G, \bullet)$ Gruppe, wenn gilt:

(G1) $\forall x, y, z \in G : x \bullet (y \bullet z) = (x \bullet y) \bullet z$ (Assoziativität)

(G2) $\exists e \in G : \forall x \in G : x \bullet e = e \bullet x = x$ (neutrales Element)

(G3) $\forall x \in G : \exists x' \in G : x \bullet x' = x' \bullet x = e$ (Inverse)

$$\begin{aligned} \text{G ist abelsch } &:\iff \forall x, y \in G : x \bullet y = y \bullet x \\ \text{G ist Halbgruppe } &:\iff \text{ G erfüllt (G1)} \\ \text{G ist Monoid } &:\iff \text{ G erfüllt (G1), (G2)} \end{aligned}$$

### I.1.2 Bemerkung

a) Das neutrale Element eines Monoids ist eindeutig bestimmt (schreibe auch $e_G$)

b) In einer Gruppe existiert zu jedem $x \in G$ genau ein Inverses

c) Wir schreiben Gruppen meist <u>multiplikativ</u> (also $(G, \cdot)$ mit $e_G = 1$, Inverses $x^{-1}$)

d) es gelten die üblichen Konventionen:

- $xy = x \cdot y$
- $xyz = x(yz)$
- $x^n := \underbrace{x \cdot \ldots \cdot x}_{\text{n-mal}}$

### I.1.3 Beispiele

a) $(\mathbb{N}, +)$: Halbgruppe

b) $(\mathbb{N}_0, +)$: Monoid, $e_{\mathbb{N}_0} = 0$

c) $(\mathbb{N}, \cdot)$: Monoid, $e_{\mathbb{N}} = 1$

d) $(\mathbb{Z}, +)$: abelsche Gruppe

e) $(\mathbb{Q}^*, \cdot)$ abelsche Gruppe ($\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$)

f) $(\mathbb{Z}/_{n\mathbb{Z}}, +)$: abelsche Gruppe, $e_{\mathbb{Z}/_{n\mathbb{Z}}} = \overline{0}$

g) $\left((\mathbb{Z}/_{n\mathbb{Z}})^\times, \cdot\right)$: abelsche Gruppe, $e_{(\mathbb{Z}/_{n\mathbb{Z}})^\times} = \overline{1}$ (Satz 0.13)

h) $S_n$: die Gruppe der Permutationen der Menge $\{0, \ldots, n-1\}$ unter Komposition: die symmetrische Gruppe. $S_n$ abelsch $\iff n \in \{1, 2\}$

i) $\mathrm{GL}_n(\mathbb{Q})$: die Gruppe der invertierbaren $n \times n$-Matrizen über $\mathbb{Q}$. $\mathrm{GL}_n(\mathbb{Q})$ abelsch $\iff n = 1$

### I.1.4 Bemerkung

Sei G eine Gruppe, $x, y, a \in G$.

Es gelten:

- $(x^{-1})^{-1} = x$
- $(xy)^{-1} = y^{-1}x^{-1}$
- $ax = ay \implies x = y$
- $xa = ya \implies x = y$ (Kürzungsregeln)

### I.1.5 Definition

Sei G eine Gruppe, $\emptyset \neq H \subset G$. Dann heißt H <u>Untergruppe</u> ($H \leq G$) von G, wenn gilt

(UG1) $\forall x, y \in H : xy \in H$

(UG2) $\forall x \in H : x^{-1} \in H$

### I.1.6 Bemerkung

Es ist $H \leq G :\iff$

$\bullet : G \times G \to G$ lässt sich einschränken zu einer Abbildung. $\bullet_H : H \times H \to H$ und $(H, \bullet_H)$ ist Gruppe.

(d.h: $\bullet|_{H \times H} = \iota_H \circ \bullet_H, \quad \iota_H : H \to G$ : Inklusion)

Wir nennen nicht nur die Menge H, sondern auch die Gruppe $(H, \bullet_H)$ eine Untergruppe von G.

### I.1.7 Beispiele

(a) Jede Gruppe G hat die <u>trivialen</u> Untergruppen $H = G,\ H = e_G$

(b) $H \leq K$ und $K \leq G \implies H \leq G$ (Transitivität)

(c) $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R}$ (bezüglich $+$) $\mathbb{Z}^\times := \{+1, -1\} \leq \mathbb{Q}^\times \leq \mathbb{R}^\times := \mathbb{R} \setminus \{0\}$ (bezüglich $\cdot$)

### I.1.8 Definition (Gruppenhomomorphismus)

Seien G,H Gruppen, $f : G \to H$ eine Abbildung. Dann heißt f Homomorphismus

$$:\iff \forall x, y \in G : f(x \circ_G y) = f(x) \circ_H f(y)$$

Bezeichne mit $\mathrm{Hom}(G, H)$ die Menge der Homomorphismen von G nach H.

Sei $f \in \mathrm{Hom}(G, H)$. Dann ist der Kern von f definiert durch

$$\ker(f) := f^{-1}(e_H) = \{x \in G : f(x) = e_H\}$$

Weiter nenne:

f Monomorphismus $:\iff$ f injektiv

f Epimorphismus $:\iff$ f surjektiv

f Isomorphismus $:\iff$ f bijektiv

G und H heißen isomorph ($G \cong H$)

$$:\iff \quad \text{es existiert ein Isomorphismus } f : G \to H$$

### I.1.9 Lemma

Sei $f : G \to H$ ein Gruppenhomomorphismus. Dann gilt

a) $f(1) = 1$

b) $\forall x \in G : f(x^{-1}) = f(x)^{-1}$

c) $\forall x_1, \ldots, x_n \in G : f(x_1, \ldots, x_n) = f(x_1) \cdots f(x_n)$

d) $G_0 \leq G \implies f(G_0) \leq H$

e) $H_0 \leq H \implies f^{-1}(H_0) \leq G$

**Beweis.** Übung

### I.1.10 Beispiele

Seien $G, H$ Gruppen:

a) $\mathrm{id}_G \in \mathrm{Hom}(G, G)$

b) Die Konstante Abbildung $G \to H, \quad x \mapsto e_H$ ist ein Homomorphismus

c) $H \leq G \implies \iota : H \to G$ ist ein Homomorphismus

d) $(A, +)$ abelsche Gruppe, $k \in \mathbb{Z} \implies \begin{cases} A \to A \\ x \mapsto k \cdot x := \underbrace{x + \ldots + x}_{\text{k mal}} \end{cases}$ ist ein Homomorphismus

e) $\begin{cases} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \\ k \mapsto k + n\mathbb{Z} \end{cases}$ ist ein Homomorphismus

f) $(\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot), x \mapsto e^x$ ist ein Isomorphismus

### I.1.11 Bemerkung

a) $f \in \mathrm{Hom}(G,H)$ injektiv $\iff \ker(f) = \{1\}$

**Beweis.**

"$\Rightarrow$" ✓

"$\Leftarrow$" $f(g) = f(g') \implies f(g'g^{-1}) = f(g')f(g)^{-1} = 1$

$\implies g'g^{-1} \in \ker(f) = \{1\} \implies g' = g$

b) $f \in \mathrm{Hom}(G,H), g \in \mathrm{Hom}(H,K) \implies g \circ f \in \mathrm{Hom}(G,K)$

c) Isomorphie von Gruppen ist eine Äquivalenzrelation.

## I.2 Ordnung und Index

Sei $G$ eine Gruppe.

### I.2.1 Lemma

Ist $\mathcal{U}$ eine Menge von Untergruppen von $G$, so ist auch $\bigcap \mathcal{U} = \bigcap\limits_{H \in \mathcal{U}}$ eine Untergruppe von G.

**Beweis.** klar.

### I.2.2 Satz

Zu jeder Teilmenge $X \subseteq G$ gibt es eine eindeutig bestimmte kleinste Untergruppe von $G$, die $X$ enthält.

**Beweis.** Sei $\mathcal{U} = \{H \leq G : X \subseteq H\}$

(2.1) $\implies U := \bigcap \mathcal{U} \in \mathcal{U}$ ist das kleinste Element von $\mathcal{U}$

### I.2.3 Definition

Sei $X \subseteq G$.

Die von X erzeugte Untergruppe von $G$, $\langle X \rangle$, ist die kleinste Untergruppe von $G$, die $X$ enthält.

Für $x_1, \dots, x_n \in G$ ist $\langle x_1, \dots, x_n \rangle := \langle \{x_1, \dots, x_n\} \rangle$.

$G$ heißt endlich erzeugt $:\iff \exists X \subseteq G$ endlich mit $G = \langle X \rangle$

### I.2.4 Lemma

Für $X \subseteq G$ ist $\langle X \rangle = \{x_1^{\epsilon_1} \cdot \ldots \cdot x_n^{\epsilon_n} : n \in \mathbb{N}_0, x_1, \dots, x_n \in X, \epsilon_1, \dots, \epsilon_n \in \{\pm 1\}\}$

**Beweis.** "$\supseteq$": klar, denn $x_1, \dots, x_n \in X \subseteq \langle X \rangle$ und $\langle X \rangle \leq G$

"$\subseteq$": rechte Seite ist Untergruppe, die X enthält.

### I.2.5 Beispiele

a) $\langle\emptyset\rangle = \{e_G\} \leq G, \langle G\rangle = G$

b) G endlich $\implies$ G endlich erzeugt

c) $\mathbb{Z}$ ist endlich erzeugt: $\mathbb{Z} = \langle\{1\}\rangle = \langle 1\rangle = \langle 2, 3\rangle$

d) $n\mathbb{Z}$ ist $\langle n\rangle = n\mathbb{Z}$

### I.2.6 Definition

Die Ordnung von $G$ ist $\#G \in \mathbb{N} \cup \{\infty\}$.

Die Ordnung von $g \in G$ ist $\operatorname{ord}(g) := \#\langle g\rangle$.

### I.2.7 Beispiele

a) $\#\mathbb{Z} = \infty, \quad \#\mathbb{Z}/_{n\mathbb{Z}} = n, \quad \#S_n = n!$

b) $G = \mathbb{Z}, \quad k \in \mathbb{Z}, \quad \operatorname{ord}(k) = \begin{cases} \infty & k \neq 0 \\ 1 & k = 0 \end{cases}$

c) $G = \mathbb{Z}/_{n\mathbb{Z}}, \quad \operatorname{ord}(\overline{1}) = n$

### I.2.8 Lemma

Für $g \in G$ mit $\operatorname{ord}(g) = n < \infty$ ist

$$\langle g\rangle = \{1, g, g^2, \dots, g^{n-1}\}$$

und

$$\operatorname{ord}(g) = \min\{k \in \mathbb{N} : g^k = 1\}$$

**Beweis.** Sei $m := \min\{k \in \mathbb{N} : g^k = 1\}$

- $m < \infty$:
  $\#\langle g\rangle < \infty$ (Schubfachprinzip) $\implies \exists k_1, k_2 \in \mathbb{N}, k_1 \neq k_2$ mit $g^{k_1} = g^{k_2}$
  $\implies$ o.E. $k_1 < k_2, \quad g^{k_2 - k_1} = 1$
- $\#\{1, g, \dots, g^{n-1}\} = m$:
  Ist $g^k = g^l$ für $0 \leq k \leq l < m$, so ist $g^{l-k} = 1$ und $0 \leq l - k < m$, deshalb $l = k = 0$ wegen Minimalität von m
- $\langle g\rangle = \{1, g, \dots, g^{m-1}\}$:

  "$\supseteq$":✓

  "$\subseteq$": Nehme $g^k \in \langle g\rangle, k \in \mathbb{Z}$. Schreibe $k = qm + r$ mit $q, r \in \mathbb{Z}, 0 \leq r < m$. Dann ist $g^k = g^{qm+r} = g^{qm}g^r = (g^m)^q g^r = 1^q g^r = g^r \in \{1, g, \dots, g^{m-1}\}$

Es folgt $m = n$ und daraus beide Behauptungen.

### I.2.9 Definition

Seien $A, B \subseteq G, H \leq G$ und $g \in G$.

1) $AB := A \cdot B := \{ab : a \in A, b \in B\}$, das Komplexprodukt von A und B.
2) $gH := \{g\} \cdot H = \{gh : h \in H\}$, $Hg := H\{g\}$ Links- bzw. Rechtsnebenklasse von H bzgl. g
3) $G/_H := \{gH : g \in G\}, \quad {}_H\backslash G := \{Hg : g \in G\}$

### I.2.10 Lemma

Seien $H \leq G, g, g' \in G$

a) $gH = g'H \iff g' = gh$ für ein $h \in H$
   $Hg = Hg' \iff g' = hg$ für ein $h \in H$
b) Es ist entweder $gH = g'H$ oder $gH \cap g'H = \emptyset$ und entweder $Hg = Hg'$ oder $Hg \cap Hg' = \emptyset$.
c) Durch $gH \mapsto Hg^{-1}$ wird eine Bijektion $G/_H \to {}_H\backslash G$ definiert.

**Beweis.**

a) "$\Rightarrow$": $g' = g' \cdot 1 \in g'H = gH \implies \exists h \in H$ mit $g' = gh$

   "$\Leftarrow$": Sei $g' = gh, h \in H \implies g'H = ghH \underset{\text{Kürzungsregel}}{=} gH$
b) Angenommen $gH \cap g'H \neq \emptyset$. Dann existiert $h, h' \in H$ mit $gh = g'h' \implies gH = ghH = g'h'H = g'H$
c) Abbildung ist wohldefiniert. Ist $gH = g'H$, so ist $g' = gh$ mit $h \in H$ nach a). Dann ist $H(g')^{-1} = \underbrace{H \cdot h^{-1}}_{=H} g^{-1} = Hg^{-1}$

   Umkehrabbildung: $Hg \mapsto g^{-1}H$

### I.2.11 Definition

Für $H \leq G$ ist der Index definiert durch

$$(G : H) := \#G/_H = \#_H\backslash G \in \mathbb{N} \cup \{\infty\}$$

### I.2.12 Beispiele

- $(\mathbb{Z} : \mathbb{Z}_n) = n$
- $(G : \{e_G\}) = \#G$
- $(G : G) = 1$
- $(S_n : A_n) = 2$ ($A_n :=$ alternierende Gruppe gerader Permutationen)

### I.2.13 Satz

Der Index ist multiplikativ.

Für $K \leq H \leq G$ ist
$$(G : K) = (G : H) \cdot (H : K)$$

**Beweis.** Wähle Vertretersysteme der Nebenklassen:

$$G/_H = \{g_i H : i \in I\},\ \#I = (G : H)$$
$$H/_K = \{h_j K : j \in J\},\ \#J = (H : K)$$

Da $g = g \cdot 1 \in gH$ ist $G = \bigcup\limits_{g \in G} gH = \bigcup\limits_{i \in I} g_i H$, und nach 2.10(b) ist diese Vereinigung disjunkt, in Zeichen: $G = \biguplus_{i \in I} g_i H$. Analog $H = \biguplus_{j \in J} h_j K$. Da $g \mapsto g_i g$ eine Permutation von G ist, folgt:

$$\begin{aligned} g_i H &= \biguplus_{j \in J} g_i h_j K \\ \implies G &= \biguplus_{i \in I} g_i H = \biguplus_{i \in I} \biguplus_{j \in J} g_i h_j K \\ \implies (G : K) &= \#I \times J \\ &= \#I \#J \\ &= (G : H)(H : K) \end{aligned}$$

### I.2.14 Korollar (Satz von Lagrange)

Ist $G$ endlich und $H \leq G$, so gilt $\#H | \#G$ und $(G : H) | \#G$.

**Beweis.** $\#G = (G : \{1\}) \overset{2.13}{=} (G : H)(H : \{1\}) = (G : H)\#H$

### I.2.15 Beispiel

Es folgt: Ist $\#G = p$ prim, so ist $G = \langle g \rangle$ für jedes $1 \neq g \in G$

### I.2.16 Korollar

Ist $G$ endlich und $n = \#G$, so ist $g^n = 1$ für jedes $g \in G$.

**Beweis.**
$\mathrm{ord}(g) \overset{2.14}{\implies} n = k \cdot m$ für ein $m \in \mathbb{N} \implies g^n = g^{km} = (g^k)^m \overset{2.8}{=} 1^m = 1$

### I.2.17 Beispiel

Für $G = (\mathbb{Z}/_{n\mathbb{Z}})^\times$ folgt $\overline{a}^{\Phi(n)} = \overline{1}\ \forall \overline{a} \in (\mathbb{Z}/_{n\mathbb{Z}})^\times$.

Für $n = p$ prim ist dies mit 0.15 der "Kleine Satz von Fermat":

$$a^p \equiv a \bmod p \text{ für alle } a \in \mathbb{Z}$$

## I.3 Normalteiler und Qoutientengruppen

Sei $G$ eine Gruppe.

### I.3.1 Lemma

Ist $f : G \to H$ ein Gruppenhomomorphismus, so ist $N := \ker(f)$ eine Untergruppe von $G$ mit $g^{-1}ng \in N \ \forall n \in N \forall g \in G$

**Beweis.**

Nach 1.9(e) ist $N \leq G$. Für $n \in N$ und $g \in G$ ist $f(g^{-1}ng) = f(g^{-1})f(n)f(g) = f(g)^{-1}1f(g) = 1$, somit $g^{-1}ng \in \ker(f) = N$

### I.3.2 Definition

Sei $N \leq G$. Die Untergruppe $N$ ist normal in $G$ (oder ein Normalteiler von $G$), in Zeichen $N \trianglelefteq G$, wenn

$$g^{-1}ng \in N \ \forall n \in N \forall g \in G$$

### I.3.3 Lemma

Seien $H \leq G$ und $N \trianglelefteq G$.

a) $H \trianglelefteq G \iff gH = Hg \ \forall g \in G$

b) $HN = NH$, $HN \leq G$, $N \trianglelefteq HN$, $H \cap N \leq N$, $H \cap N \trianglelefteq G$

c) $N, H \trianglelefteq G \implies H \cap N \trianglelefteq G, \ HN \trianglelefteq G$

d) Für $g, g' \in G$ ist $gN \cdot g'N = gg'N$

**Beweis.**

a) "$\Leftarrow$": $gH = Hg \ \forall g \in G \implies g^{-1}Hg = H \ \forall g \in G \implies g^{-1}hg \in H \ \forall g \in G \forall h \in H$ "$\Rightarrow$":

$$\begin{aligned} & g^{-1}hg \in H \ \forall g \in G \forall h \in H \\ \implies & g^{-1}Hg \subseteq H \ \forall g \in G \\ \implies & Hg \subseteq gH \ \forall g \in G \\ \implies & g^{-1}H \subseteq Hg^{-1} \ \forall g \in G \\ \implies & gH \subseteq Hg \ \forall g \in G \end{aligned}$$

Und damit: $gH = Hg \ \forall g \in G$.

b) $HN = \bigcup_{h \in H} hN \overset{a)}{=} \bigcup_{h \in H} Nh = NH$

$HN \leq G$: $HNHN = HHNN = HN$, $(HN)^{-1} = N^{-1}H^{-1} = NH = HN$

Rest: Übung

c) $HN \trianglelefteq G$: $gHN \overset{H \trianglelefteq G}{=} Hg \cdot N \overset{N \trianglelefteq G}{=} H \cdot Ng \ \forall g \in G \overset{a)}{\implies} HN \trianglelefteq G$

Rest: Übung

d) $gN \cdot g'N = g \cdot Ng' \cdot N \overset{N \trianglelefteq G}{=} g \cdot g'N \cdot N = gg'N$

### I.3.4 Definition

Sei $N \trianglelefteq G$. Die Quotientengruppe $G/_N$ ist die Menge $G/_N$ zusammen mit Komplexprodukt als Multiplikation.

### I.3.5 Satz

Sei $N \trianglelefteq G$. Dann ist $G/_N$ eine Gruppe und $\pi_n : \begin{cases} G \to G/_N \\ g \mapsto gN \end{cases}$ ein Gruppenepimorphismus mit Kern $\ker(\pi_N) = N$

**Beweis.**

- Komplexprodukt liefert eine Abb.

$$G/_N \times G/_N \to G/_N \quad (3.3(\mathrm{d}))$$

- Gruppenaxiome übertragen sich von $G$ auf $G/_N$, z.B. $gN \cdot g^{-1}N = gg^{-1}N = N$ neutrales Element.
- $\pi_N$ ist Homomorphismus: $\pi_N(gg') = gg'N \overset{3.3(d)}{=} gN \cdot g'N = \pi_N(g)\pi_N(g')\ \forall g, g' \in G$
- $\ker(\pi_N) = N$: $g \in \ker(\pi_N) \iff gN = N \iff g \in N$

### I.3.6 Korollar

Die Normalteiler sind genau die Kerne von Gruppenhomomorphismen.

### I.3.7 Lemma

Sei $N \trianglelefteq G$. Für $H \leq G$ ist $\pi_N(H) = HN/_N \leq G/_N$. Insbesondere liefert $\varphi : H \mapsto \pi_N(H)$ eine Bijektion zwischen den $H \leq G$ mit $N \leq H$ und den $U \leq G/_N$.

**Beweis.**

- $HN \leq G$ nach 3.3 $\implies HN/_N \leq G/_N$
- $\pi_N(h) = hN = hnN = \pi_N(hn)\ \forall h \in H \forall n \in N \implies \pi_N(H) = \pi_N(HN) = HN/_N$
- Umkehrabbildung zu $\varphi$: $\psi(U) := \pi_N^{-1}(U)$ für $U \leq G/_N$

$$\varphi(\psi(U)) = \pi_N(\pi_N^{-1}(U)) = U \text{ für } U \leq G/_N$$

$$\begin{aligned} \psi(\varphi(H)) = \pi_N^{-1}(\pi_N(H)) &= \{g \in G : \pi_N(g) \in \pi_N(H)\} \\ &= \{g \in G : gN \subseteq HN\} \\ &= \{g \in G : gN \subseteq H\} \text{ falls } N \subseteq H \\ &= H \end{aligned}$$

### I.3.8 Satz (Homomorphiesatz für Gruppen)

Sei $\varphi : G \to H$ ein Gruppenhomomorphismus und $N \trianglelefteq G$ mit $N \subseteq \ker(\varphi)$. Dann ex. genau ein Gruppenhom. $\overline{\varphi} : G/_N \to H$ mit $\varphi = \overline{\varphi} \circ \pi_N$

**Beweis.**

Eindeutigkeit:

$$\overline{\varphi}(gN) = \overline{\varphi}(\pi_N(g)) = \varphi(g) \forall g \in G$$

Existenz: Definition $\overline{\varphi}(gN)$

Wohldefiniertheit:

$$g'N = gN \implies g' = gn \text{ für ein } n \in N \implies \varphi(g') = \varphi(gn) = \varphi(g)\underbrace{\varphi(n)}_{=1} = \varphi(g)$$

$\overline{\varphi} \in \mathrm{Hom}(G/_N, H)$ : klar.

### I.3.9 Korollar

Ein Gruppenhomomorphismus $\varphi \in \mathrm{Hom}(G, H)$ induziert einen Isomorphismus

$$G/_{\ker(\varphi)} \cong Im(\varphi)$$

**Beweis.**
Wende 3.8 an auf $N = \ker(\varphi)$. Prüfe, dass $\overline{\varphi} : G/_{\ker(\varphi)} \to H$ injektiv ist mit $Im(\varphi) = Im(\overline{\varphi})$

### I.3.10 Korollar (1. Isomorphiesatz)

Sei $H \leq G$, $N \trianglelefteq G$. Die Abbildung

$$\varphi : H \hookrightarrow HN \to HN/_N$$

induziert einen Isomorphismus

$$H/_{H\cap N} \cong HN/_N$$

**Beweis.**

- $\varphi$ ist surjektiv:

$$hnN = hN = \varphi(h) \quad \forall h \in H \forall n \in N$$

- $\varphi(h) = N \iff hN = N \iff h \in N$, somit gilt $\ker(\varphi) = N \cap H$

Wende 3.9 an auf $\varphi$

### I.3.11 Korollar (2. Isomorphiesatz)

Sei $N \trianglelefteq G$ und $N \leq H \trianglelefteq G$. Die Abbildung

$$\pi_H : G \to G/_H$$

induziert einen Isomorphismus

$$(G/_N)/_{(H/_N)} \cong G/_H$$

**Beweis.**
$N \leq H \overbrace{\Longrightarrow}^{3.8} \pi_H$ induziert einen Homomorphismus $\overline{\pi}_H : G/_N \to G/_H$

- $\overline{\pi}_H$ ist surjektiv.
- $\ker(\overline{\pi}_H) = \{gN : \pi_H(g) = H\} = \{gH : gH = H\} = H/_N$

Wende 3.9 auf $\overline{\pi}_H$ an.

### I.3.12 Definition

Seien $x, x', g \in G$ und $H \leq G$. Definiere:

1) Konjungation von x und g:

$$x^g := g^{-1}xg$$

2) $x, x'$ sind konjungiert $:\iff \exists g \in G : x' = x^g$
3) Automorphismen auf G:

$$\mathrm{Aut}(G) := \{\varphi \in \mathrm{Hom}(G, G) : \varphi \text{ ist Isomorphismus}\}$$

   $(= \mathrm{Iso}(G, G))$

   Mit $\varphi$:

$$\varphi \circ \varphi' := \varphi' \circ \varphi$$

   bildet $\mathrm{Aut}(G)$ die Automorphismengruppe.

### I.3.13 Lemma

Die Abbildung

$$\mathrm{int} := \begin{cases} G \to \mathrm{Aut}(G) \\ g \mapsto (x \mapsto x^g) \end{cases}$$

("Interior ") ist ein Gruppenhomomorphismus.

**Beweis.**

1) $\mathrm{int}(g) \in \mathrm{Hom}(G, G) \forall g \in G$:

$$\begin{aligned} \mathrm{int}(g)(xy) &= g^{-1}xyg \\ &= g^{-1}xgg^{-1}yg \\ &= \mathrm{int}(g)(x) \cdot \mathrm{int}(g)(y) \end{aligned}$$

2) $\mathrm{int}(g)$ ist bijektiv

$$\begin{aligned} (\mathrm{int}(g^{-1}) \cdot \mathrm{int}(g))(x) &= \mathrm{int}(g^{-1})(g^{-1}xg) \\ &= gg^{-1}xgg^{-1} \\ &= x \end{aligned}$$

   Also ist $\mathrm{int}(g^{-1})$ die Umkehrabbildung.

3) $\mathrm{int} \in \mathrm{Hom}(G, \mathrm{Aut}(G))$:

   Seien $g, g' \in G$. Dann:

$$\begin{aligned} \mathrm{gg}'(x) = x^{gg'} &= (gg')^{-1}xgg' \\ &= (g')^{-1}g^{-1}xgg' \\ &= (\mathrm{int}(g) \cdot \mathrm{int}(g'))(x) \quad \square \end{aligned}$$

### I.3.14 Definition

1)
$$\mathrm{Inn}(G) := \mathrm{im}(\mathrm{int}) \leq \mathrm{Aut}(G)$$
Die Gruppe der <u>linearen Automorphismen</u> von G.

2)
$$Z(G) := \mathrm{Zent}(G) := \ker(\mathrm{int}) = \{g \in G : xg = gx \forall x \in G\}$$
Das <u>Zentrum</u> von G

3) $H \leq G$ ist <u>charakteristisch</u>
$$:\iff \sigma(H) = H \forall \sigma \in \mathrm{Aut}(G)$$

### I.3.15 Bemerkung

$H \leq G$ normal $\iff \sigma(H) = H \forall \sigma \in \mathrm{Inn}(G)$
Jede charakteristische Untergruppe von G ist normal.

### I.3.16 Beispiel

Sei $G := \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Dann ist jede Untergruppe normal, da G abelsch, aber
$$\mathbb{Z}/2\mathbb{Z} \times \{\bar{0}\} \leq G$$
ist nicht charakteristisch (z.B. unter $(a, b) \mapsto (b, a)$ )

## I.4 Zyklische Gruppen

Sei $G$ eine Gruppe.

### I.4.1 Definition

G ist <u>zyklisch</u>
$$:\iff G = \langle g \rangle$$
für ein $g \in G$

### I.4.2 Lemma

Die Untergruppen von $(\mathbb{Z}, +)$ sind genau die Gruppen

- $\langle k \rangle = \mathbb{Z} \cdot k, \quad k \in \mathbb{N}_0$
- $k_1, \ldots, k_n \in \mathbb{Z} : \langle k_1, \ldots, k_n \rangle = \langle k \rangle$ mit $k = \mathrm{ggT}(k_1, \ldots, k_n)$

**Beweis.**
Sei $H \leq \mathbb{Z}$. Ist $H = \{0\}$, dann ist $H = \langle 0 \rangle$. Sei also $H \neq \{0\}$. Dann existiert
$$k := \min H \cap \mathbb{N} \in \mathbb{N}$$

Behauptung: $H = \langle k \rangle$

" $\supset$ ": ✓

" $\subset$ ": Sei $h \in H$ und schreibe

$$h = qk + r \quad (q, r \in \mathbb{Z}, 0 \leq r < k)$$

Da $r = h - qk \in H$, muss $r = 0$ (Da k minimal in $H \cap \mathbb{N}$ und $0 \leq r < k$).

Also $k \in \mathbb{Z}k = \langle k \rangle$.

Ist $\langle k_1, \ldots, k_n \rangle = \langle k \rangle$, so gilt $k | k_i$ für $i = 1, \ldots, r$

Umgekehrt ist

$$k = n_1 k_1 + \cdots + n_r k_r \quad (n_1, \ldots n_r \in \mathbb{Z})$$

Ist also $c \in \mathbb{N}$ mit $c | k_1, \ldots, k_r$, so auch $c | k$. Also $k = \mathrm{ggT}(k_1, \ldots, k_r)$ □

### I.4.3 Satz

Sei G zyklisch. Dann ist G abelsch.

Weiterhin gilt

$$\begin{aligned} \text{entweder:} \quad & G \cong (\mathbb{Z}, +) \\ \text{oder:} \quad & G \cong (\mathbb{Z}/n\mathbb{Z}, +) \quad (n = \#G) \end{aligned}$$

**Beweis.**

Sei $G = \langle g \rangle$. Betrachte die Abbildung

$$\varphi : \begin{cases} \mathbb{Z} \to G \\ k \mapsto g^k \end{cases}$$

Dann ist $\varphi \in \mathrm{Hom}((\mathbb{Z}, +), G)$ und surjektiv (mit 2.4).

Nach 3.9 ist

$$G \cong \mathrm{im}(\varphi) \cong \mathbb{Z}/_{\ker \varphi}$$

Nach 4.2 ist

$$\ker(\varphi) = \langle k \rangle = \mathbb{Z}k \quad (k \in \mathbb{N}_0)$$

Ist $k = 0$, so ist

$$G \cong \mathbb{Z}/_{\{0\}} \cong \mathbb{Z}$$

Ist $k > 0$, dann ist

$$G \cong \mathbb{Z}/_{k\mathbb{Z}}$$

also $k = \#G$

### I.4.4 Definition

Für $n \in \mathbb{N}$ bezeichne $C_n$ die bis auf Isomorphie eindeutig bestimmte zyklische Gruppe der Ordnung n (multiplikativ)

### I.4.5 Satz

Sei $G = (G, +) = \langle g \rangle$ zyklisch der Ordnung $n \in \mathbb{N}$.

a) Zu jedem $d \in \mathbb{N}$ mit $d|n$ gibt es genau eine Untergruppe der Ordnung $d$, nämlich $U_d = \langle \frac{n}{d} g \rangle$

b) Für $d|n$, $d'|n$ ist $U_d \subseteq U_{d'} \iff d|d'$.

c) Für $k_1, \ldots, k_r \in \mathbb{Z}$ ist $\langle k_1 g, \ldots, k_r g \rangle = \langle dg \rangle = U_{\frac{n}{d}}$ mit $d = \mathrm{ggT}(k_1, \ldots, k_r, n)$.

d) Für $k \in \mathbb{Z}$ ist $\mathrm{ord}(kg) = \frac{n}{\mathrm{ggT}(k,n)}$.

**Beweis.** Betrachte wieder $\varphi : \begin{cases} \mathbb{Z} \to G \\ k \mapsto kg \end{cases}$

a) Nach 3.7 und 4.2 liefert $\varphi$ Bijektion:

$$\{e \in \mathbb{N} : n\mathbb{Z} \subseteq e\mathbb{Z}\} \to \{U \leq G\}$$

und $n\mathbb{Z} \subseteq e\mathbb{Z} \iff e|n$. Ist $U = \varphi(e\mathbb{Z}) = \langle eg \rangle$, so ist $U \overset{3.9}{\cong} e\mathbb{Z}/_{n\mathbb{Z}}$, also $n = (\mathbb{Z} : n\mathbb{Z}) = (\mathbb{Z} : e\mathbb{Z})(e\mathbb{Z} : n\mathbb{Z}) = e\#U$, d.h. $\#U = \frac{n}{e} = d$, $U = \langle eg \rangle = \langle \frac{n}{d} g \rangle$

b)

$$\begin{aligned} U_d \subseteq U_{d'} &\iff \langle \frac{n}{d} g \rangle \subseteq \langle \frac{n}{d'} g \rangle \iff \frac{n}{d}\mathbb{Z} \subseteq \frac{n}{d'}\mathbb{Z} \\ &\iff \frac{n}{d'} | \frac{n}{d} \iff d|d' \end{aligned}$$

c) Setze $H = \langle k_1, \ldots, k_r, n \rangle \leq \mathbb{Z}$
Nach 4.2 ist $H = \langle d \rangle$ mit $d = \mathrm{ggT}(k_1, \ldots, k_r, n)$. Es ist $n\mathbb{Z} \subseteq H$ und $\langle dg \rangle = \varphi(H) = \langle k_1, \ldots, k_r, n \rangle$

d) $\mathrm{ord}(kg) = \#\langle kg \rangle \overset{(c)}{=} \#\langle dg \rangle = \#U_{\frac{n}{d}} = \frac{n}{d}$ mit $d = \mathrm{ggT}(k, n)$

### I.4.6 Definition

Das direkte Produkt von Gruppen $G_1, \ldots, G_n$ ist das kartesische Produkt $G_1 \times \ldots \times G_n$ mit komponentenweiser Multiplikation, auch geschrieben $\prod_{i=1}^n G_i$. Im Fall additiver Notation spricht man auch von der direkten Summe und schreibt $\bigoplus_{i=1}^n G_i$ oder $G_1 \oplus G_2$.

### I.4.7 Satz (Struktursatz für abelsche Gruppen)

Jede endlich erzeugte abelsche Gruppe $G$ ist eine direkte Summe zyklischer Gruppen: $G \cong \mathbb{Z}^r \oplus \bigoplus_{i=1}^k \mathbb{Z}/_{d_i\mathbb{Z}}$ (wobei $\mathbb{Z}^r = \bigoplus_{i=1}^r \mathbb{Z}$) mit eindeutig bestimmten $r \in \mathbb{N}_0, k \in \mathbb{N}_0$ und $d_1, \ldots, d_k \in \mathbb{N}$ mit $d_1 \ldots, d_k \in \mathbb{N}$ mit $d_i | d_{i+1} \forall i$.
**Beweis.** Bosch Algebra Kapitel 2.9, Korollar 9

### I.4.8 Beispiele

Die folgenden Gruppen sind endlich erzeugt und abelsch, und deshalb von obiger Form:

a) $(\mathbb{Z}/n\mathbb{Z})^\times$ (Kapitel 2)

b) $(K, +), (K \setminus \{0\}, \cdot)$, $K$ endlicher Körper (Kapitel 3)

c) $Z(S_n), Z(D_4), \ldots$

d) $\mathrm{Aut}(C_n)$

### I.4.9 Lemma

Sei $G = (G, +) = \langle g \rangle$ zyklisch von Ordnung $n < \infty$. Die Endomorphismes von $G$ sind genau die

$$\varphi_{\overline{k}} = \begin{cases} G \to G \\ x \mapsto kx \end{cases} , \quad \overline{k} = k + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$$

Dabei ist $\varphi_{\overline{l}} \circ \varphi_{\overline{k}} = \varphi_{\overline{kl}}$ $(\overline{k}, \overline{l} \in \mathbb{Z}/n\mathbb{Z})$.
**Beweis.**

- $\varphi_{\overline{k}}$ ist wohldefiniert: $k' = k + nm \implies k'x = (k+nm)x = kx + m\underbrace{nx}_{=0} = kx$, denn $nx = 0 \forall x \in G$ nach 2.16.
- $\varphi_{\overline{k}} \in \mathrm{Hom}(G, G)$: 1.10 (d)
- $\forall \varphi \in \mathrm{Hom}(G,G) \exists \overline{k} \in \mathbb{Z}/n\mathbb{Z} : \varphi = \varphi_{\overline{k}}$:

$$\begin{aligned} \varphi(g) \in G &\implies \varphi(g) = kg \text{ für ein } k \in \mathbb{Z} \\ &\implies \varphi(sg) \overset{\varphi \text{ Hom.}}{=} s\varphi(g) = skg = ksg \forall s \in \mathbb{Z} \\ &\implies \varphi = \varphi_{\overline{k}} \end{aligned}$$

- $\varphi_{\overline{k}} = \varphi_{\overline{l}} \iff \overline{k} = \overline{l}$: $kg = \varphi_{\overline{k}}(g) \varphi_{\overline{l}}(g) = lg$
  $\implies (k-l)g = 0 \implies n|(k-l) \implies \overline{k} = \overline{l}$

### I.4.10 Satz

Ist $G$ zyklisch der Ordnung $n \in \mathbb{N}$, so ist $\mathrm{Aut}(G) \cong (\mathbb{Z}/n\mathbb{Z})^\times$ **Beweis.** Nach 4.9 ist:

$$\begin{aligned} \varphi_{\overline{k}} \in \mathrm{Aut}(G) &\iff \exists l \in \mathbb{Z} : \varphi_{\overline{k}} \circ \varphi_{\overline{l}} = \mathrm{id}_G \\ &\iff \exists l \in \mathbb{Z} : \varphi_{\overline{kl}} = \varphi_{\overline{1}} \\ &\iff \exists l \in \mathbb{Z} : \overline{kl} = \overline{1} \end{aligned}$$

Die Abb. $\begin{cases} (\mathbb{Z}/n\mathbb{Z})^\times \to \mathrm{Aut}(G) \\ \overline{k} \mapsto \varphi_{\overline{k}} \end{cases}$ ist ein Isomorphismus.

# II Ringe

## II.1 Grundlegende Definitionen

### II.1.1 Definition

Ein Ring ist ein Tripel $(R, +, -)$ bestehend aus einer Menge $R$, einer Verknüpfung
$+ : R \times R \to R$ ("Addition") und einer Verknüpfung
$\cdot : R \times R \to R$ ("Multiplikation"), welche die folgenden Axiome erfüllen:

(R1) $(R, +)$ ist eine abelsche Gruppe

(R2) $(R, \cdot)$ ist eine Halbgruppe

(R3) Es gelten die Distributivgesetze

$$a(x + y) = ax + ay, \quad (x + y)a = xa + ya \ (a, x, y \in R)$$

Ein Ring heißt kommutativ, falls $ab = ba \forall a, b \in R$. Ein neutrales Element der Multiplikation heißt ein Einselement von $R$. Ein Unterring eines Rings $(R, +, \cdot)$ ist eine Teilmenge $S \subseteq R$, die mit der geeigneten Einschränkung der Addition und Multiplikation ein Ring ist.

### II.1.2 Bemerkung

Das neutrale Element der Addition wird oft mit 0 bezeichnet und es gilt $x0 = 0x = 0 \forall x \in R$. Es gelten die üblichen Konventionen, z.B. $xy + z = (xy) + z$

### II.1.3 Beispiele

a) Der Nullring $R = \{0\}$ ist ein kommutativer Ring mit Einselement 0.

b) $(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$ sind kommutative Ringe mit Einselement 1.

c) $\mathrm{Mat}_{n \times n}(\mathbb{R})$ ist Ring, der für $n > 1$ nicht kommutativ ist.

d) $2\mathbb{Z} = \{\dots, -4, -2, 0, 2, 4, \dots\}$ ist ein kommutativer Ring ohne Einselement.

e) $(\mathbb{Z}/_{n\mathbb{Z}})$ ist ein kommutativer Ring mit dem Einselement $\overline{1}$

### II.1.4 Konvention

In diese Vorlesung sind Ringe <u>immer kommutativ mit Einselement</u>!

### II.1.5 Definition

Sei $R$ ein Ring, $x \in R$.

a) Die <u>Charakteristik</u>, $\operatorname{char}(R)$, von R ist das kleinste $n \in \mathbb{N}$ mit $\underbrace{1 + \ldots + 1}_{n-\text{mal}} = 0$, falls so ein $n$ existiert. Andernfalls ist $\operatorname{char}(R) = 0$.

b) $x$ ist ein <u>Nullteiler</u> $:\iff x \neq 0 \wedge \exists 0 \neq y \in R : xy = 0$

c) $R$ ist <u>nullteilerfrei</u> $:\iff R$ hat keine Nullteiler.

d) $x$ ist <u>invertierbar</u> (oder eine Einheit von $R$) $:\iff \exists y \in R : xy = 1$.

e) $R^\times := \{x \in R : x \text{ ist Einheit von } R\}$

f) $R$ ist <u>Körper</u> $:\iff R^\times = R \setminus \{0\}$

### II.1.6 Lemma

Sei $R$ ein Ring.

a) Ist $x \in R^\times$, so ist $x$ kein Nullteiler.

b) $(R^\times, \cdot)$ ist eine Gruppe

**Beweis.**

a) $xx' = 1 \wedge xy = 0 \implies y = x'xy = x'0 = 0$

b)
- jedes $x \in R^\times$ hat Inverses nach Definition
- $1 \in R^\times$
- $xx' = 1 \wedge yy' = 1 \implies xyx'y' = xx'yy' = 1 \cdot 1 = 1$

### II.1.7 Beispiele

a) $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ sind Körper der Charakteristik 0.

b) $\mathbb{Z}$ ist nullteilerfreier Ring der Charakteristik 0 mit $\mathbb{Z}^\times = \{\pm 1\}$

c) $\mathbb{Z}/n\mathbb{Z}$ ist Ring der Charakteristik n. Nach 0.13 $(\mathbb{Z}/n\mathbb{Z})^\times = \{\overline{a} : \operatorname{ggT}(a, n) = 1\}$. Ist $n = p$ eine Primzahl, so ist $\#(\mathbb{Z}/n\mathbb{Z})^\times = \Phi(p) = p - 1$, also $(\mathbb{Z}/p\mathbb{Z})^\times = (\mathbb{Z}/p\mathbb{Z}) \setminus \{\overline{0}\}$, d.h. $\mathbb{F}_p := (\mathbb{Z}/p\mathbb{Z})$ ist ein Körper, insbesondere nullteilerfrei.
Ist $n$ keine Primzahl, also $n = ab$ mit $1 < a, b < n$, so ist $\overline{0} = \overline{n} = \overline{a}\overline{b}$, und $\overline{a}, \overline{b} \neq \overline{0}$, also besitzt $\mathbb{Z}/n\mathbb{Z}$ Nullteiler und ist somit kein Körper.

### II.1.8 Definition

Seien $R, S$ Ringe. Eine Abbildung $f : R \to S$ ist ein <u>Ringhomomorphismus</u>, wenn für $x, y \in R$ gilt:

(RH1) $f(x + y) = f(x) + f(y)$

(RH2) $f(xy) = f(x)f(y)$

Die Menge der Ringhomomorphismen $f : R \to S$ wird mit $\operatorname{Hom}(R, S)$ bezeichnet. Ein $f \in \operatorname{Hom}(R, S)$ ist ein Mono-, Epi- oder Isomorphismus, wenn $f$ injektiv, surjektiv oder bijektiv ist. Gibt es einen Isomorphismus $f : R \to S$, so nennt man $R$ und $S$ isomorph, in Zeichen $R \cong S$. Der Kern von $f \in \operatorname{Hom}(R, S)$ ist $\ker(f) := f^{-1}(0_S)$.

### II.1.9 Bemerkung

a) $f \in \mathrm{Hom}(R,S)$ ist injektiv $\iff$ $\ker(f) = \{0_R\}$

b) $f \in \mathrm{Hom}(R,S), g \in \mathrm{Hom}(S,T) \implies g \circ f \in \mathrm{Hom}(R,T)$

c) Isomorphie ist eine Äquivalenzrelation.

### II.1.10 Beispiel

$\begin{cases} \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \\ a \mapsto \overline{a} = a + n\mathbb{Z} \end{cases}$ ist ein Ringepimorphismus mit Kern $n\mathbb{Z} = \mathbb{Z}n$.

## II.2 Polynomringe

Sei $R$ ein Ring.

### II.2.1 Definition

Der Polynomring in einer Variablen $X$ über $R$ ist

$$R[X] := \left\{ \sum_{i=0}^{\infty} a_i X^i : a_i \in R, \text{fast alle gleich Null} \right\}$$

mit der Addition:

$$\sum_{i\geq 0} a_i X^i + \sum_{i \geq 0} b_i X^i := \sum_{i\geq 0} (a_i + b_i) X^i$$

und der Multiplikation:

$$\left(\sum_{i\geq 0} a_i X^i\right) \cdot \left(\sum_{j\geq 0} b_j X^j\right) = \sum_{k\geq 0} \left(\sum_{i+j=k} a_i b_j\right) X^k$$

Ist $f = \sum_{i=0}^n a_i X^i \in R[X]$ mit $a_n \neq 0$, so ist $\deg(f) := n$ der Grad von $f$ (mit $\deg(0) := -\infty$), $\mathrm{LC}(f) := a_n$ der Leitkoeffizient von $f$, und $f$ heißt normiert, falls $\mathrm{LC}(f) = 1$.

### II.2.2 Bemerkung

$R[X]$ ist wieder ein Ring (Übung). Wir identifiziern $R$ mit dem Teilring von $R[X]$ der Polynome mit dem Grad $\leq 0$ ("konstante Polynome").

### II.2.3 Lemma

Seien $f, g \in R[X]$.

a) $\deg(f+g) \leq \max\{\deg(f), \deg(g)\}$

b) $\deg(fg) \leq \deg(f) + \deg(g)$

c) Ist $LC(g)$ kein Nullteiler in $R$, so ist $\deg(fg) = \deg(f) + \deg(g)$.

**Beweis.**

a) ✓

b) $f = \sum_{i=0}^n a_i X^i, a_n \neq 0, g = \sum_{j=0}^m b_j X^j, b_m \neq 0$

$$\implies fg = a_n b_m X^{n+m} + \sum_{k<n+m} \left(\sum_{i+j=k} a_i b_j\right) X^k$$

c) $b_m = \mathrm{LC}(g)$ kein Nullteiler $\implies a_n b_m \neq 0 \implies \deg(fg) = n+m$

### II.2.4 Korollar

Ist $R$ nullteilerfrei, so auch $R[X]$, und $(R[X])^\times = R^\times$.
**Beweis.**

- $R[X]$ nullteilerfrei: $fg = 0 \implies -\infty = \deg(0) = \deg(fg) \overset{2.3(c)}{=} \deg(f) + \deg(g) \implies f = 0 \vee g = 0$
- $R^\times \subseteq (R[X])^\times$: ✓
- $(R[X])^\times \subseteq R^\times$:

$$\begin{aligned} fg = 1 &\implies 0 = \deg(1) = \deg(fg) = \deg(f) + \deg(g) \implies \deg(f) = \deg(g) = 0, \text{d.h. } f, g \in R \\ &\implies fg = 1 \implies f, g \in R^\times \end{aligned}$$

### II.2.5 Satz (Universelle Eigenschaft des Polynomrings)

Ist $\varphi : R \to S$ ein Ringhomomorphismus und $s \in S$, so gibt es genau einen Ringhomomorphismus $\varphi_s : R[X] \to S$ mit $\varphi_s|_R = \varphi$ und $\varphi_s(X) = s$.
**Beweis.** Eindeutigkeit: $\varphi_s\left(\sum_{i\geq 0} a_i X^i\right) \overset{\varphi_s \text{ Hom.}}{=} \sum_{i\geq 0} \varphi_s(a_i)\varphi_s(X)^i = \sum_{i\geq 0} \varphi(a_i) s^i$
Existenz: Definiere $\varphi_s : R[X] \to S$:

$$\varphi_s(\sum_{i\geq 0} a_i X^i) := \sum_{i\geq 0} \varphi(a_i) \cdot s^i \in S$$

Dann gilt

- $\varphi_s|_R = \varphi$ :✓
- $\varphi_s(X) = s^1 = s$
- $\varphi_s \in \mathrm{Hom}(R[X], S)$ :

$$\begin{aligned} \varphi_s(\sum_{i\geq 0} a_i X^i + \sum_{j\geq 0} b_j X^j) &= \varphi_s(\sum_{i\geq 0} (a_i + b_i) X^i) \\ &= \sum_{i\geq 0} \varphi(a_i + b_i) \cdot X^i \\ &= \sum_{i\geq 0} (\varphi(a_i) + \varphi(b_i)) \cdot X^i \\ &= \sum_{i\geq 0} \varphi(a_i) \cdot X^i + \sum_{j\geq 0} \varphi(b_j) \cdot X^j \\ &= \varphi_s(\sum_{i\geq 0} a_i \cdot X^i) + \varphi_s(\sum_{j\geq 0} b_j \cdot X^j) \qquad \square \end{aligned}$$

(Multiplikation analog)

### II.2.6 Beispiel

Insbesondere hat man für $a \in R$ den sog. Einsetzungshomomorphismus (oder Auswertungsabbildung)
Für $a \in R$

$$\Phi_a : \begin{cases} R[X] \to R \\ f \mapsto f(a) \end{cases}$$

gegeben durch $\Phi_a|_R = \mathrm{id}_R$ und $\Phi_a(X) = a$

Dieser liefert eine Abbildung

$$\begin{cases} R[X] \to \mathrm{Abb}(R, R) \\ f \mapsto \tilde{f} \end{cases}$$

mit $\tilde{f}(a) := \varphi_a(f)$. Im Allgemeinen ist diese Abbildung $R[X] \to \mathrm{Abb}(R, R)$ nicht injektiv, man muss deshalb Polynome f und Polynomfunktionen $\tilde{f}$ unterscheiden.

### II.2.7 Satz (Polynomdivision)

Sei $0 \neq g \in R[X]$ mit $LC(g) \in R^\times$.

Zu jedem $f \in R[X]$ gibt es eindeutig bestimmte $q, r \in R[X]$ mit $f = qg + r$ und $\deg(r) < \deg(g)$

**Beweis.**

- Existenz: Sei $f = \sum_{i=0}^n a_i X^i, a_n \neq 0, \quad g = \sum_{i=0}^m b_i X^i, b \in R^\times$

  Induktion nach n:

  $n < m$: Nehme $q = 0, r = f$
  $n \geq m$: Setze $f_n = f - a_n b_m^{-1} X^{n-m} g \in R[X]$.

  Dann ist $\deg(f_n) < n \implies$ ex. $q, r \in R[X]$ mit $f_n = qg + r, \deg(r) < m$.

  $$\implies f = (q + a_n b_m^{-1} X^{n-m})g + r$$

- Eindeutigkeit: Seien $f = q_1 g + r_1 = q_2 g + r_2$ mit $q_1, q_2, r_1, r_2 \in R[X]$ und $\deg(r_1), \deg(r_2) < n, m$, wobei $m = \deg(g), n = \deg(f)$

  $$(q_1 - q_2)g = r_2 - r_1$$
  $$\deg(r_2 - r_1) < m$$
  $$\implies \deg(q_1 - q_2)g < m$$

  $\deg(g) = m, b_m \in R^\times$:

  $$\implies b_m \text{ ist nicht Nullteiler}$$
  $$\implies \deg((q_1 - q_2)g) = \deg((q_1 - q_2)) + \deg(g)$$
  $$\implies \deg(q_1 - q_2) = -\infty \implies q_1 - q_2 = 0, r_1 - r_2 = 0 \quad \square$$

### II.2.8 Korollar

Ist $f \in R[X]$ mit $a \in R$ und $f(a) = 0$ (a ist Nullstelle von f)

So ist

$$f(X) = (X - a) \cdot g(X) \text{ mit } g \in R[X]$$

**Beweis.**

Schreibe $f(X) = q(X)(X - a) + r(X)$ mit $q, r \in R[X]$.
Dann ist $\deg(r) < \deg(X - a) = 1$, d.h. $r \in R$

Da $\phi_a \in \mathrm{Hom}(R[X], R)$, folgt:

$$\underbrace{f(a)}_{0} = q(a) \cdot \underbrace{(a-a)}_{0} + r(a)$$

$$\implies r(a) = 0$$
$$\implies r = 0 \quad \square$$

### II.2.9 Korollar

Ist R nullteilerfrei, so hat jedes $0 \neq f \in R[X]$ höchstens $\deg(f)$ viele Nullstellen.

**Beweis.** : Induktion nach $n = \deg(f)$

$\underline{n = 0}$: ✓

$\underline{n - 1 \to n}$: $f(a) = 0 \to f(X) = (X - a) \cdot q(X)$

nullteilerfrei $\implies$ $\deg(q) = \deg(f) - \deg(X - a) = n - 1$

$$\overset{\text{IH}}{\implies} q \text{ hat höchstens } n-1 \text{ Nullstellen in R} \quad \square$$

### II.2.10 Bemerkung

Eine Möglichkeit, $R[X]$ streng formal zu definieren, ist wie folgt:

Sei $R[X]$ die Menge der endlichen Folgen $(a_\mu)_{\mu\in\mathbb{N}_0}$ in R (also $a_\mu = 0$ für fast alle $\mu$), mit

- Addition: $(a_\mu)_{\mu\in\mathbb{N}_0} + (b_\mu)_{\mu\in\mathbb{N}_0} := (a_\mu + b_\mu)_{\mu\in\mathbb{N}_0}$
- Multiplikation: $(a_\mu)_{\mu\in\mathbb{N}_0} \cdot (b_\mu)_{\mu\in\mathbb{N}_0} := \left(\sum_{\mu+\nu=\lambda} a_\mu \cdot b_\nu\right)_{\lambda\in\mathbb{N}_0}$

Zur besseren Lesbarkeit definieren wir

$$X := (\delta_{\mu,1})_{\mu\in\mathbb{N}_0}, \quad a := (a\delta_{\mu,0})_{\mu\in\mathbb{N}_0}$$

Dann ist

$$(a_\mu)_{\mu\in\mathbb{N}_0} = \sum_{\mu\in\mathbb{N}_0} a_\mu X^\mu$$

### II.2.11 Definition

Für eine Menge I definieren wir die Halbgruppe

$$\mathbb{N}_0^{(I)} := \{(\mu_i)_{i\in I} \in \prod_{i\in I} \mathbb{N}_0 : \text{ fast alle } \mu_i = 0\}$$

mit Addition

$$(\mu_i)_{i\in I} + (\nu_i)_{i\in I} := (\mu_i + \nu_i)_{i\in I}$$

sowie den Ring

$$R[X_i : i \in I] := \{(a_\mu)_{\mu\in\mathbb{N}_0^{(I)}} : a_\mu \in R \text{ fast alle } = 0\}$$

mit Addition

$$(a_\mu)_{\mu\in\mathbb{N}_0^{(I)}} + (b_\mu)_{\mu\in\mathbb{N}_0^{(I)}} := (a_\mu + b_\mu)_{\mu\in\mathbb{N}_0^{(I)}}$$

und Multiplikation

$$(a_\mu)_{\mu\in\mathbb{N}_0^{(I)}} \cdot (b_\mu)_{\mu\in\mathbb{N}_0^{(I)}} := \left(\sum_{\lambda+\nu=\mu} a_\lambda b_\nu\right)_{\mu\in\mathbb{N}_0^{(I)}}$$

genannt Polynomring in den Variablen $X_i, i \in I$

Wir schreiben:

$$X_i := (\delta_{\mu\nu_i})_{\mu\in\mathbb{N}_0^{(I)}}, \quad \nu_i := (\delta_{ij})_{j\in I}$$

$$X^\mu := \prod_{i\in I} X_i^{\mu_i}$$

$$a := (a \cdot \delta_{\mu,\underline{0}})_{\mu\in\mathbb{N}_0^{(I)}}, \quad \underline{0} := (0)_{i\in I}$$

so dass

$$(a_\mu)_{\mu\in\mathbb{N}_0^{(I)}} = \sum_{\mu\in\mathbb{N}_0^{(I)}} a_\mu X^\mu$$

Weiter ist $R[X_1, \dots, X_n] := R[X_i : i \in \{1, \dots, n\}]$

### II.2.12 Beispiele

(a) $R[X_1] = R[X_i : i \in \{1\}]$

(b) $R[X_1, X_2] \cong (R[X_1])\,[X_2]$

(c) $R[X_1, X_2] \cong R[X_2, X_1]$

(d) $R[X_1, X_2, X_3] \cong (R[X_1, X_2])\,[X_3]$

## II.3 Teilbarkeit

Sei R ein Ring.

### II.3.1 Definition

Seien $a, b \in R$

(1) a <u>teilt</u> b $(a|b)$

$$:\iff \exists x \in R : b = ax$$

(2) a ist <u>assoziiert</u> zu b $(a \sim b)$

$$:\iff \exists x \in R^\times : b = ax$$

### II.3.2 Lemma

Für $a, b, c, d \in R$ gilt:

(i) $a|a$ (reflexiv)

(ii) $a|b \wedge b|c \implies a|c$ (transitiv)

(iii) $a|b \wedge a|c \implies a|(b+c)$

(iv) $a|b \wedge c|d \implies ac|bd$

### II.3.3 Lemma

Für $a, b, c, d \in R$ gilt:

(i) $a \sim a$ (reflexiv)

(ii) $a \sim b \wedge b \sim c \implies a \sim c$ (transitiv)

(iii) $a \sim b \implies b \sim a$ (symmetrisch)

(iv) $a \sim b \wedge c \sim d \implies ac \sim bd$

### II.3.4 Bemerkung

Teilbarkeit auf R ist insbesondere eine Präordnung (reflexiv und transitiv)

Assoziiertheit ist eine Äquivalenzrelation.

### II.3.5 Lemma

Ist R nullteilerfrei, so gilt für $a, b \in R$:

$$a \sim b \iff a|b \wedge b|a$$

**Beweis.** :

- " $\implies$ "

  $b = ax, x \in R^{\times} \implies a|b$

  $bx^{-1} = a, x \in R^{\times} \implies b|a$

- " $\impliedby$ "

  $b = ax, a = by, \quad x, y \in R$

  $\implies a = (ax)y = axy$

  $\implies a(xy - 1) = 0$

  nullteilerfrei $\implies a = 0$ (dann $b = 0, a \sim b$)

  oder $\implies xy = 1 \implies x, y \in R^{\times} \implies a \sim b$ □

### II.3.6 Definition

Seien $a, b \in R$

(1 $c \in R$ ist <u>ein</u> größter gemeinsamer Teiler von a und b (in Zeichen $c = \mathrm{ggT}(a, b)$)

$$:\iff c|a \wedge c|b \wedge (\forall d \in R : d|a \wedge d|b \implies d|c)$$

(2 $c \in R$ ist <u>ein</u> kleinstes gemeinsames Vielfaches von a und b (in Zeichen $c = kgV(a, b)$)

$$:\iff a|c \wedge b|c \wedge (\forall d \in R : a|d \wedge b|d \implies c|d)$$

### II.3.7 Bemerkung

Wenn ggT und kgV in einem nullteilerfreien Ring existieren, sind sie eindeutig bestimmt <u>bis auf Assoziiertheit</u>.

### II.3.8 Definition

Sei $0 \neq x \in R \setminus R^\times$.

1) x ist <u>irreduzibel</u> ("unzerlegbar")

$$:\iff \text{ Ist } x = ab \text{ mit } a, b \in R, \text{ dann ist } a \in R^\times \text{ oder } b \in R^\times$$

2) x ist <u>prim</u>

$$:\iff \text{ Ist } x|ab \text{ mit } a, b \in R, \text{ so ist } x|a \text{ oder } x|b$$

### II.3.9 Bemerkung

In $R = \mathbb{Z}$ fallen die Begriffe prim und irreduzibel zusammen.

$\underline{R = \mathbb{Q}[t]}$: jedes lineare Polynom"$f = at + b, a \in \mathbb{Q}^\times, b \in \mathbb{Q}$ ist irreduzibel (2.4) und prim (denn $f|g \iff g\left(-\frac{b}{a}\right) = 0$ nach 2.8).
$f = t^2 - 1$ ist nicht irreduzibel (also reduzibel)
$f = t^2 - 2$ ist irreduzibel

### II.3.10 Bemerkung

Man sieht: Ist $p \in R$ prim und $p|a_1 \dots a_n$ mit $a_1, \dots, a_n \in R$, so gilt $p|a_i$ für ein $i$.

### II.3.11 Satz

Sei R nullteilerfrei. Ist $0 \neq p \in R \setminus R^\times$ prim, so ist $p$ irreduzibel.
**Beweis.** Sei $p$ prim, $p = ab$ mit $a, b \in R$.

$$p = ab \implies p|ab \overset{p \text{ prim}}{\implies} p|a \vee p|b$$

Sei o.E. $p|a$, also $a = px$ mit $x \in R$.

$$\implies p = ab = pxb \implies p(xb - 1) = 0 \overset{R \text{ nullteilerfrei}}{\implies} xb = 1$$

Insbesondere $b \in R^\times$.

## II.4 Ideale

Sei R ein Ring.

### II.4.1 Lemma

Ist $\varphi : R \to S$ ein Ringhomomorphismus, so ist $I = \ker(\varphi)$ eine Untergruppe von $(R, +)$ mit $ra \in I$ für alle $a \in I$ und $r \in R$.
**Beweis.**

- $I \leq (R, +)$: I.3.1, denn $\varphi \in \mathrm{Hom}((R, +), (S, +))$.
- $a \in I, r \in I \implies \varphi(ra) \overset{\varphi \text{ Hom.}}{=} \varphi(r)\varphi(a) = \varphi(r) \cdot 0 = 0 \implies ra \in I$.

### II.4.2 Definition

Eine Untergruppe $I$ von $(R, +)$ mit $ra \in I$ für alle $r \in R$ und $a \in I$ heißt ein Ideal von $R$, in Zeichen $I \trianglelefteq R$

### II.4.3 Beispiel

Für $a \in R$ ist $(a) := Ra := \{ra : r \in R\} = \{b \in R : a|b\}$ das von a „erzeugte“ Hauptideal.
Beispiele:

- $(0) = \{0\}$, das Nullideal von $R$
- $(1) = R$, das triviale Ideal von $R$

(ein Ideal $I$ heißt echt, wenn $I \neq (1)$.)

### II.4.4 Bemerkung

a) $I \subseteq R$ Ideal $\iff I + I \subseteq I, 0 \in I, R \cdot I \subseteq I$ (Dabei insbes. $(-1)x = -x \in I$).

b) Sei $I \trianglelefteq R$. Dann: $I = (1) \iff 1 \in I$

c) Sei $a \in R$. Dann: $(a) = (1) \iff a \in R^\times$
Insbesondere gilt: $R$ ist ein Körper $\iff R$ hat genau zwei Ideale ($(0) \neq (1)$)

d) Sind $I, J \trianglelefteq R$, so auch $I + J \trianglelefteq R$ und $I \cap J \trianglelefteq R$.

e) Der Durchschnitt einer Menge $\mathcal{I}$ von Idealen von $R$ ist wieder ein Ideal von $R$ (vgl. I.2.1). Insbesondere gibt es zu $A \subseteq R$ ein kleinstes Ideal von $R$, das $A$ enthält (vgl. I.2.2), das von $A$ erzeugte Ideal $\langle A \rangle$.
Es gilt (vgl. I.2.4) $\langle A \rangle = \{\sum_{i=1}^n r_i a_i : n \in \mathbb{N}_0, r_i \in R, a_i \in A\}$
Man schreibt auch: $(a_1, \ldots, a_n) = \langle \{a_1, \ldots, a_n\} \rangle$

### II.4.5 Definition

Sei $I \trianglelefteq R$. Der <u>Quotientenring</u> (oder <u>Faktorring</u>) $R/I$ ist die Menge der Restklassen

$$R/I = \{x + I : x \in R\}$$

mit Addition: $(x + I) + (y + I) := (x + y) + I,\ x, y \in R$
und Multiplikation $(x + I)(y + I) := (xy) + I,\ x, y \in R$.

### II.4.6 Satz

$R/I$ ist ein Ring und $\pi_I : \begin{cases} R \to R/I \\ x \mapsto x + I \end{cases}$ ist ein Ringepimorphismus mit Kern $I$.

**Beweis.** Nach I.3.5 ist $(R/I, +)$ eine Gruppe und $\pi_I$ ein Gruppenepimorphismus.
Multiplikation ist wohldefiniert: $x' = x + a, y' = y + b$ mit

$$a, b \in I \implies x'y' = (x + a)(y + b) = xy + \underbrace{xb}_{\in I} + \underbrace{ya}_{\in I} + \underbrace{ab}_{\in I} \in xy + I$$

Die Ringaxiome übertragen sich von $R$ auf $R/I$. $\pi_I$ ein Ringhomomorphismus nach Definition.

### II.4.7 Korollar

Ideale sind genau die Kerne von Ringhomomorphismen.

### II.4.8 Bemerkung

Für $I \trianglelefteq R$ und $a, b \in R$ schreibt man:

$$\begin{aligned} a \equiv b \mod I :&\iff a - b \in I \\ &\iff a + I = b + I \\ &\iff \pi_I(a) = \pi_I(b) \\ &\iff: \overline{a} = \overline{b} \end{aligned}$$

### II.4.9 Satz (Homomorphiesatz)

Sei $\varphi : R \to S$ ein Ringhomomorphismus und $I \trianglelefteq R$ mit $I \subseteq \ker(\varphi)$. Dann existiert genau ein Ringhom. $\overline{\varphi} : R/I \to S$ mit $\varphi = \overline{\varphi} \circ \pi_I$

**Beweis.** Analog zu I.3.8.

### II.4.10 Korollar

Ist $\varphi : R \to S$ ein Ringepimorphismus, so ist $R/\ker(\varphi) \cong S$.

### II.4.11 Lemma

Sei $\varphi : R \to S$ ein Ringhomomorphismus.

a) Für $J \trianglelefteq S$ ist $\varphi^{-1}(J) \trianglelefteq R$.

b) Ist $\varphi$ surjektiv und $I \trianglelefteq R$, so ist $\varphi(I) \trianglelefteq S$.

**Beweis.** $\varphi^{-1}(J), \varphi(I)$ sind Untergruppen, siehe I.1.1.9

a) $a \in \varphi^{-1}(J), r \in R \implies \varphi(ra) = \underbrace{\varphi(r)}_{\in S}\underbrace{\varphi(a)}_{\in J} \in J \implies ra \in \varphi^{-1}(J)$

b) $a \in I, s \in S \overset{\varphi \text{ surj.}}{\implies} s = \varphi(r)$ für ein $r \in R \implies s\varphi(a) = \varphi(ra) \in \varphi(I)$

### II.4.12 Satz

Ist $I \trianglelefteq R$, so liefert $\pi_I$ eine Bijektion zwischen den Idealen von $R$, die $I$ enthalten, und den Idealen von $R/I$.
**Beweis.** $\pi_I$ liefert Bijektion zwischen Untergruppen von $(R, +)$, die $I$ enthalten, und Untergruppen von $(R/I, +)$ (I.3.7). Behauptung folgt mit 4.11.

### II.4.13 Definition

Sei $I \trianglelefteq R$.

1) $I$ ist <u>maximal</u> $:\iff I \neq R$ und ist $I \subsetneq J \trianglelefteq R$, so ist $J = R$.

2) I heißt <u>prim</u> $:\iff I \neq R$ und $a, b \in R$ mit $a \cdot b \in I$, so ist $a \in I \vee b \in I$

### II.4.14 Bemerkung

Für $0 \neq p \in R$ gilt:
$$p \text{ ist prim} \iff (p) \text{ ist prim}$$

### II.4.15 Satz

Sei $I \trianglelefteq R$.

a) $I$ ist prim $\iff R/_I$ ist nullteilerfrei

b) I ist maximal $\iff R/_I$ ist Körper

c) I ist maximal $\implies I$ ist prim

<u>Beweis:</u>

a) klar, da $ab \in I \iff \bar{a} \cdot \bar{b} = \overline{ab} = 0$

b) I ist maximal

$\iff$ R hat nur zwei Ideale, die I enthalten

$\overset{4.12}{\iff}$ $R/_I$ hat genau zwei Ideale

$\overset{4.4.c}{\iff}$ $R/_I$ ist Körper

c) aus a), b), denn Körper sind nullteilerfrei $\square$

### II.4.16 Beispiel

Im Ring $R = \mathbb{Z}$: Ideale sind genau die Untergruppen von $(\mathbb{Z}, +)$, also die Hauptideale.

- $(n) = \mathbb{Z}n, n \in \mathbb{N}_0$ (I.4.2)
- $(n)$ ist prim $\iff n = 0$ oder $n \in \mathbb{P}$ Primzahl
- $(n)$ ist maximal $\iff n \in \mathbb{P}$ Primzahl
- $(n) + (m) = (\text{ggT}(m, b))$, $(n) \cap (m) = (\text{kgV}(m, n))$

### II.4.17 Satz (Lemma von Zorn)

Sei $(\mathcal{X}, \leq)$ eine Halbordnung (d.h. $\leq$ ist reflexiv, transitiv, antisymmetrisch).

Besitzt jede Kette $\mathcal{C}$ in $\mathcal{X}$ (d.h. $\forall x, y \in \mathcal{C}$ ist $x \leq y$ oder $y \leq x$) eine obere Schranke in $\mathcal{X}$ (d.h. es existiert $s \in \mathcal{X}$, s.d. $\forall x \in \mathcal{C} : x \leq s$), so besitzt $\mathcal{X}$ ein maximales Element (d.h. es existiert $y \in \mathcal{X} : \forall x \in \mathcal{X} : y \leq x \implies y = x$).

Beweis: Äquivalent zum Auswahlaxiom, siehe z.B. Lang, Algebra, Appendix 2.

### II.4.18 Satz

Jedes echte Ideal $I \underset{\neq}{\lhd} R$ ist in einem maximalen Ideal von $R$ enthalten.

Beweis: Sei $\mathcal{X} = \{J \underset{\neq}{\lhd} R : I \subseteq J\}$. Wir wenden 4.17 an auf die Halbordnung $(\mathcal{X}, \subseteq)$:

- $\mathcal{X} \neq \emptyset : I \in \mathcal{X} \checkmark$.
- Sei $\mathcal{C} \subseteq \mathcal{X}$ eine nichtleere Kette in $\mathcal{X}$:
  Dann ist $J_0 := \bigcup \mathcal{C} \in \mathcal{X}$:
  - $I \subseteq J_0 : I \subseteq J$ für jedes $J \in \mathcal{C}$
  - $J_0 \trianglelefteq R$: Sind $a_1, a_2 \in J_0$, so gibt es $J_1, J_2 \in \mathcal{C}$, s.d. $a_1 \in J_1, a_2 \in J_2$. O.B.d.A. $J_1 \subseteq J_2$, also $a_1, a_2 \in J_2$. Dann gilt $a_1 + a_2 \in J_2 \subseteq J_0$ und für alle $r \in R$ $ra_1 \in J_2 \subseteq J_0$.
  - $J_0 \subsetneq R$: $J \underset{\neq}{\lhd} R \forall J \in \mathcal{C} \implies 1 \notin J \forall J \in \mathcal{C} \implies 1 \notin \bigcup_{J \in \mathcal{C}} J = J_0 \implies J_0 \underset{\neq}{\lhd} R$

Somit ist $J_0$ obere Schranke von $\mathcal{C}$. Nach 4.17 existiert ein max. Element $J \subseteq \mathcal{X}$. Dieses $J$ ist dann ein max. Ideal von $R$, das $I$ enthält.

## II.5 Chinesischer Restsatz und Einheitengruppen

Sei R ein Ring.

### II.5.1 Definition

Ideale $I, J \trianglelefteq R$ heißen teilerfremd, wenn $I + J = R$.

### II.5.2 Beispiel

In $R = \mathbb{Z}$: $(n), (m)$ teilerfremd $\iff \text{ggT}(n, m) = 1$

### II.5.3 Definition

Das direkte Produkt der Ringe $R_1, \ldots, R_n$ ist das kartesische Produkt $\prod_{i=1}^{n} R_i$ mit komponentenweiser Addition und Multiplikation.

### II.5.4 Bemerkung

$\prod_{i=1}^n R_i$ ist wieder ein Ring, und $(\prod_{i=1}^n R_i)^\times \cong \prod_{i=1}^n R_i^\times$.

### II.5.5 Satz (allgemeiner chinesischer Restsatz)

Sind $I_1, \dots, I_r \trianglelefteq R$ paarweise teilerfremd, so induzieren die Abbildungen $\pi_i := \pi_{I_i} : R \to R/I$ einen Isomorphismus:

$$\overline{\pi} : R/_{\bigcap_{i=1}^r I_i} \xrightarrow{\cong} \prod_{i=1}^r R/_{I_i}$$

Beweis: Wende Homomorphiesatz 4.10 an auf: $\pi : \begin{cases} R \to \prod_{i=1}^r R/_{I_i} \\ x \mapsto (\pi_i(x))_i = (\pi_1(x), \dots, \pi_r(x)) \end{cases}$

- $\ker(\pi) = \bigcap_{i=1}^r \ker(\pi_i) = \bigcap_{i=1}^r I_i$✓
- $\pi$ ist surjektiv: Sei $(y_1, \dots, y_r) \in \prod_{i=1}^r R/_{I_i}$. Für $i = 1, \dots, r$ wähle $x_i \in R$ mit $\pi_i(x_i) = y_i$. Fixiere ein $i$. Für $j \neq i$ ist $I_i + I_j = R$, es ex. also $a_j \in I_i, b_j \in I_j$ mit $a_j + b_j = 1$. Definiere $e_i := \prod_{j \neq i} b_j$. Dann ist

$$\pi_k(e_i) = \prod_{j \neq i} \pi_k(b_j) = \begin{cases} \prod_{j \neq i} \pi_i(1 - a_j) = 1, k = i \\ \pi_k(b_k) \prod_{j \neq i,k} \pi_k(b_j) = 0, k \neq i \end{cases}$$

$$\implies \pi\left(\sum_{i=1}^r x_i e_i\right) = \left(\sum_{i=1}^r \pi_k(x_i)\pi_k(e_k)\right)_k = (\pi_k(x_k))_k = (y_1, \dots, y_r)$$

### II.5.6 Korollar

Sind $n_1, \dots, n_r \in \mathbb{N}$ pw. teilerfremd und $n = n_1 \cdot \ldots \cdot n_r$, so ist

$$\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_r\mathbb{Z}$$

und somit

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/n_1\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/n_r\mathbb{Z})^\times$$

für

$$n := \prod_{i=1}^r n_i$$

Beweis:

Es gilt:

$$\begin{aligned} \bigcap_{i=1}^r (n_i) &= (\mathrm{kgV}(n_1, \dots, n_r)) \\ &= (\prod_{i=1}^r n_i) \\ &= (n). \end{aligned}$$

$$\begin{aligned} (5.5) \implies \mathbb{Z}/n\mathbb{Z} &= \mathbb{Z}/\bigcap_{i=1}^r (n_i) \\ &\cong \prod_{i=1}^r \mathbb{Z}/(n_i) \\ &= \prod_{i=1}^r \mathbb{Z}/n_i\mathbb{Z} \\ \implies (\mathbb{Z}/n\mathbb{Z})^\times &\cong \prod_{i=1}^r (\mathbb{Z}/n_i\mathbb{Z})^\times. \quad \square \end{aligned}$$

### II.5.7 Bemerkung

(a) Insbesondere gilt:

Sind $n_1, \dots, n_r$ paarweise teilerfremd und $y_1, \dots, y_r \in \mathbb{Z}$, so gibt es $x \in \mathbb{Z}$ mit

$$\begin{aligned} x &\equiv y_1 \mod n_1 \\ &\vdots \\ x &\equiv y_r \mod n_r \end{aligned}$$

und genau die Elemente aus

$$x + n\mathbb{Z}(n := \prod_{i=1}^{r} n_i)$$

erfüllen diese Kongruenzen.

(b) Der Beweis liefert ein Verfahren, so ein x zu finden.

(c) Die Vorraussetzung der Teilerfremdheit ist notwendig. So ist zum Beispiel

$$\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$$

aber

$$\begin{aligned} \mathbb{Z}/4\mathbb{Z} &\ncong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = V_4 \\ \mathbb{Z}/2\mathbb{Z} &\ncong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \end{aligned}$$

(d) Es folgt: sind $n, m \in \mathbb{N}$ teilerfremd, so ist

$$C_{nm} \cong C_n \times C_m$$

### II.5.8 Satz

Seien $m, n \in \mathbb{N}$

(a) Ist $\text{ggT}(n.m) = 1 \implies \phi(mn) = \phi(m) \cdot \phi(n)$

(b) Ist $n = p$ prim, so ist $\phi(p^r) = (p-1)p^{r-1}$

(c) Sind $p_1, \dots, p_r$ die verschiedenen Primteiler von n, so

$$\phi(n) = n \cdot \prod_{i=1}^{r} (1 - \frac{1}{p_i})$$

<u>Beweis:</u>

(a) S.6 ✓

(b) Für $k \in \{0, \dots, p^r - 1\}$ ist

$$\begin{aligned} \overline{k} \in (\mathbb{Z}/p^r\mathbb{Z})^\times &\iff \text{ggT}(k, p^r) = 1 \\ &\iff p \nmid k \\ &\iff k \notin \{0, p, 2p, \dots, p^r - p\} \end{aligned}$$

$$\begin{aligned} \implies \phi(p^r) &= p^r - \#k \\ &= p^r - p^{r-1} \\ &= (p-1)p^{r-1} \end{aligned}$$

(c) Sei $n = p_1^{r_1} \cdot \dots \cdot p_l^{r_l}$ die Primzerlegung. Dann gilt

$$\begin{aligned}\phi(n) &\overset{(a)}{=} \phi(p_1^{r_1}) \cdot \dots \cdot \phi(p_l^{r_l}) \\ &\overset{(b)}{=} \prod_{i=1}^{l} (p_i - 1) p_i^{r_i - 1} \\ &= n \cdot \prod_{i=1}^{l} (1 - \frac{1}{p_i}) \quad \square\end{aligned}$$

### II.5.9 Lemma

Sei $(G, +)$ eine abelsche Gruppe. Sind $a, b \in G$ mit

$$\mathrm{ord}(a) = n \in \mathbb{N}, \mathrm{ord}(b) = m \in \mathbb{N}$$

so gibt es ein $c \in G$ mit

$$\mathrm{ord}(c) = \mathrm{kgV}(m, n)$$

Beweis:

Sei $m = \mathrm{ord}(a), n = \mathrm{ord}(b)$. Schreibe

$$m = \prod_{i=1}^{l} p_i^{r_i}; n = \prod_{j=1}^{l} p_j^{s_j}$$

Primzerlegung mit $p_i$ prim paarweise verschieden.

Definiere mit $I := \{i : r_i \geq s_i\}$

$$m_0 := \prod_{i \in I} p_i^{r_i}, n_0 = \prod_{j \notin I} p_j^{s_j}$$

Dann gilt:

- $m_0 n_0 = \mathrm{kgV}(m, n); \mathrm{ggT}(m_0, n_0) = 1$
- $m_0 | m, n_0 | n$

Setze $a' := \frac{m}{m_0} a, b' := \frac{n}{n_0} b, c := a' + b'$

Dann ist $\mathrm{ord}(a') = m_0, \mathrm{ord}(b') = n_0$

$$\begin{aligned}\implies m_0 \cdot n_0 \cdot c = n_0 m_0 a' + m_0 n_0 b' = 0 \\ \implies \mathrm{ord}(c) | m_0 n_0\end{aligned}$$

Ist $k \in \mathbb{N}$ mit $k \cdot c = 0$, so ist

$$k \cdot n_0 \cdot a' = k \cdot n_0 \cdot a' + k \cdot \underbrace{n_0 \cdot b'}_{=0} = n_0 \cdot \underbrace{k \cdot c}_{=0} = 0$$

$$\implies m_0 = \mathrm{ord}(a') | k n_0$$

Da $\mathrm{ggT}(m_0, n_0) = 1$ folgt

$$m_0 | k$$

Analog folgt

$$n_0|k$$

Wir setzen

$$m_0 n_0 | k \implies m_0 n_0 | \operatorname{ord}(c)$$

Mit dem obigen folgt

$$\operatorname{ord}(c) = m_0 n_0 = \operatorname{kgV}(m, n) \quad \square$$

### II.5.10 Satz

Ist $\mathbb{K}$ ein Körper und $H \leq \mathbb{K}^\times$ endlich, so ist H zyklisch.

Beweis:

Sei $n = \#H, m = \max_{h \in H} \operatorname{ord}(h) \overset{I.2.16}{\leq} n$.

Nach 5.9 gilt $\operatorname{ord}(h)|m$ für alle $h \in H$.

$\implies$ Jedes $h \in H$ ist Nullstelle des Polynoms

$$f := X^m - 1 \in \mathbb{K}[X]$$

$\implies \#H \leq \deg(f) = m$, also $m = n$.

### II.5.11 Korollar

Für $p \in \mathbb{P}$ ist

$$(\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$$

zyklisch.

Beweis: $\mathbb{Z}/p\mathbb{Z}$ ist Körper □

### II.5.12 Lemma

Sei $p \in \mathbb{P}, e \in \mathbb{N}$, sodass $p^e > 2$.

Dann gilt für $a, b \in \mathbb{Z}$

$$\begin{aligned} & a \equiv 1 + bp^e \mod p^{e+1} \\ \implies & a^p \equiv 1 + bp^{e+1} \mod p^{e+2} \end{aligned}$$

**Beweis.**

Schreibe $a = 1 + bp^e + b'p^{e+1}$ für ein $b' \in \mathbb{Z}$ Also:

$$a = 1 + cp^e \quad (c = b + b'p)$$

$$\implies a^p = \sum_{i=0}^{p} \binom{p}{i} c^i p^{ei} = 1 + cp^{e+1} + \sum_{i=2}^{p} \binom{p}{i} c^i p^{ei}$$

Für $i \in \{2, \dots, p-1\}$ gilt $p|\binom{p}{i}$ und $ei \geq e+1$, somit gilt

$$\binom{p}{i} c^i p^{ei} \equiv 0 \mod p^{e+2}$$

Für $i = p$ gilt $ei = ep \geq e + 2$, somit

$$\binom{p}{p} c^p p^{ep} = 0 \mod p^{e+2}$$

Somit gilt

$$a^p \equiv 1 + cp^{e+1} = 1 + bp^{e+1} + \underbrace{b'p^{e+2}}_{\equiv 0} \mod p^{e+2} \quad \square$$

### II.5.13 Satz

Sei $n \in \mathbb{N}$ mit Primzerlegung

$$n = \prod_{i=1}^{r} p_i^{r_i}$$

Dann ist

$$(\mathbb{Z}/n\mathbb{Z})^\times \cong \prod_{i=1}^{r} (\mathbb{Z}/p_i^{r_i}\mathbb{Z})^\times$$

wobei gilt

(a) Für $p > 2$ prim und $r \in \mathbb{N}$ ist

$$(\mathbb{Z}/p^r\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)p^{r-1}\mathbb{Z} \cong \mathbb{Z}/(p-1)\mathbb{Z} \oplus \mathbb{Z}/p^{r-1}\mathbb{Z}$$

zyklisch.

(b) Für $p = 2, r \geq 2$ ist

$$(\mathbb{Z}/2^r\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2^{r-1}\mathbb{Z}$$

(c)

$$(\mathbb{Z}/2\mathbb{Z})^\times = \{1\}$$

Beweis:

Nach 5.7 ist $(\mathbb{Z}/n\mathbb{Z})^\times \cong \prod(\mathbb{Z}/p_i^{r_i}\mathbb{Z})^\times$

(c) ist klar

(b) ähnlich zu (a) [siehe „Elementare und alg. Zahlentheorie“, §7, Müller-S.,Pionth.]

(a) Es genügt zu zeigen, dass

$$G := (\mathbb{Z}/p^r\mathbb{Z})^\times$$

zyklisch ist, denn

$$G \underset{1.4.3}{\cong} \mathbb{Z}/\phi(p^r)\mathbb{Z} \underset{5.3}{=} \mathbb{Z}/(p-1)p^{r-1}\mathbb{Z} \underset{5.7}{\cong} \mathbb{Z}/(p-1)\mathbb{Z} \oplus \mathbb{Z}/p^{r-1}\mathbb{Z}$$

Setze $H := (\mathbb{Z}/p\mathbb{Z})^\times$ Der Ringhomomorphismus

$$\pi : \begin{cases} \mathbb{Z}/p^r\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} \\ x + p^r\mathbb{Z} \mapsto x + p\mathbb{Z} \end{cases}$$

(z.B. aus 4.9 mit $\varphi = \pi_{(p)}, I = (p^r)$) liefert einen Gruppenhomomorphismus

$$\pi^\times := \pi|_G : G \to H$$

mit Kern $N := \ker(\pi^\times) \leq G$

- $\pi(G) \subset H$ und $\pi^\times$ ist surjektiv:

  Für $x \in \mathbb{Z}$ ist

$$\begin{aligned} x + p^r\mathbb{Z} \in G &\iff \mathrm{ggT}(x, p^r) = 1 \\ &\iff \mathrm{ggT}(x, p) = 1 \\ &\iff x + p\mathbb{Z} \in H \end{aligned}$$

- $G/_N \cong H$: I.3.9 (Hom.-satz für Gruppen)

- $\#N = p^{r-1}$: $\#G = \#G/_N \cdot \#N = \#H \cdot \#N$

$$\implies \#N = \frac{\#G}{\#H} = \frac{\phi(p^r)}{\phi(p)} = \frac{(p-1)p^{r-1}}{p-1} = p^{r-1}$$

- H ist zyklisch : 5.11
- N ist zyklisch:

  Sei $a := 1 + p, \overline{a} = a + p^r\mathbb{Z} \in G$

  Mit $\pi^\times$ sieht man $\overline{a} \in N$ Also

$$\operatorname{ord}(\overline{a}) \underset{\text{Lagrange}}{\mid} \#N = p^{r-1}$$

  Weiterhin gilt

$$\begin{aligned} a &\equiv 1 + 1 \cdot p \mod p^2 \\ \implies a^{p^{r-2}} &\equiv 1 + p^{r-1} \mod p^r \\ \implies \overline{a}^{p^{r-2}} &\neq 1 \end{aligned}$$

  Da also (falls $\operatorname{ord}(\overline{a}) = p^s$ mit $1 \leq s < r-2$, dann wäre nach Potenzgesetz $\overline{a}^{p^{r-2}} = 0$) $\operatorname{ord}(\overline{a}) > p^{r-2}$, ist $\operatorname{ord}(\overline{a}) = p^{r-1}$

  Also ist $N = \langle a \rangle$ zyklisch.
- G ist zyklisch:

  Sei $b \in \mathbb{Z}$, sodass $\langle \pi(\bar{b}) \rangle = H$

  Es ist $p - 1 = \operatorname{ord}(\pi(\bar{b})) | \operatorname{ord}(\bar{b})$, denn ist $\bar{b}^n = 1$ mit $n \in \mathbb{N}$, so auch $\pi(\bar{b})^n = \pi(\bar{b}^n) = 1$

  Nach 5.9 existiert $\bar{c} \in G$ mit

$$\operatorname{ord}(\bar{c}) = \operatorname{kgV}(\operatorname{ord}(\overline{a}), \operatorname{ord}(\bar{b})) = (p-1)p^{r-1} = \#G$$

  Folglich ist $G = \langle \bar{c} \rangle$ zyklisch. □

## II.6 Hauptidealringe

Sei R ein nullteilerfreier Ring.

### II.6.1 Definition

R ist ein Hauptidealring $:\iff$ jedes Ideal von R ist ein Hauptideal.

### II.6.2 Beispiel

$\mathbb{Z}$ ist ein Hauptidealring (I.4.2)

### II.6.3 Definition

Eine euklidische Gradfunktion auf R ist eine Abbildung

$$\delta : R \setminus \{0\} \to \mathbb{N}_0$$

für die gilt:

Für $a \in R$ und $b \in R \setminus \{0\}$ gibt es $q, r \in R$ mit

- $a = bq + r$
- $r = 0$ oder $\delta(r) < \delta(b)$

Der Ring R heißt euklidisch, wenn es eine euklidische Gradfunktion auf R gibt.

### II.6.4 Beispiele

a) Auf $R = \mathbb{Z}$ ist $\delta(x) := |x|$ eine euklidische Gradfunktion.

b) Auf $R = \mathbb{K}[t]$, $\mathbb{K}$ Körper, ist $\delta(f) = \deg(f)$ eine euklidische Gradfunktion, siehe 2.7

c) Die Gaußschen Zahlen $R = \mathbb{Z}[i] = \{x + iy : x, y \in \mathbb{Z}\} \leq \mathbb{C}$ bilden einen Teilring von $\mathbb{C}$ mit der euklidischen Gradfunktion
$$\delta(z) = z \cdot \overline{z} = |z|^2$$

### II.6.5 Satz

Ist R euklidisch, so ist R Hauptidealring.
Beweis: Sei $\delta$ eine euklidische Gradfunktion auf $R$. Sei $I \trianglelefteq R$.

- $I = \{0\} \implies I = (0)$ ein Hauptideal
- $I \neq \{0\}$, so existiert $0 \neq a \in I$ mit $\delta(a) = \min\{\delta(b) : 0 \neq b \in I\}$. Es ist dann $I = (a)$.

  $\supseteq$: ✓

  $\subseteq$: $b \in I \implies b = qa + r,\ q, r \in R, r = 0$ oder $\delta(r) < \delta(a)$

$$r = \underbrace{b}_{\in I} - \underbrace{qa}_{\in I} \in I$$

$$\implies r = 0 \vee \underbrace{\delta(r) \geq \delta(a)}_{\text{kann nicht eintreten}}$$

$$\implies r = 0 \implies b = qa \in (a)$$

### II.6.6 Korollar

Die Ringe $\mathbb{Z}, \mathbb{K}[t]$ ($\mathbb{K}$ Körper) sind Hauptidealringe.

### II.6.7 Lemma

Sei $R$ ein Hauptidealring, $a, b \in R$. Es gibt ein $c \in R$ mit $c = \mathrm{ggT}(a, b)$ und $(c) = (a, b)$. Insbesondere existieren $x, y \in R$ mit $c = ax + by$ und $\mathrm{ggT}(x, y) = 1$
Beweis: Da $R$ ein Hauptidealring ist, existiert ein $c \in R$ mit $(c) = (a, b)$. Insbesondere ist $c|a$, $c|b$ und $c = ax + by$ mit $x, y \in R$. Wir sehen: $c = \mathrm{ggT}(a, b)$
Ist $d \in R$ mit $d|x$ und $d|y$, so gilt: $cd|ax + by = c$, also $d \in R^\times$. Somit ist $\mathrm{ggT}(x, y) = 1$.

### II.6.8 Satz

Sei $R$ ein Hauptidealring und $(0) \neq \mathcal{P} \trianglelefteq R$. Ist $\mathcal{P}$ prim, so ist $\mathcal{P}$ maximal.
Beweis: Sei $\mathcal{P} \subseteq I \trianglelefteq R$. Da $R$ Hauptidealring ist, ist $I = (a)$ mit $a \in R$, $\mathcal{P} = (p)$ mit $p \in R$ prim, insbesondere irreduzibel.

$$(p) \subseteq (a) \implies p|a \overset{p \text{ irreduzibel}}{\implies} a \sim 1 \vee a \sim p$$

$$\implies I = (a) = (1) = R \vee I = (a) = (p) = \mathcal{P}$$

### II.6.9 Beispiel

a) In $R = \mathbb{Z}$ ist $(0)$ prim, aber nicht maximal. Die Primideale $(p), p \in \mathbb{P}$, sind alle maximal (Erinnerung: $\mathbb{Z}/n\mathbb{Z}$ nullteilerfrei $\iff$ $\mathbb{Z}/n\mathbb{Z}$ ist Körper).

b) $\mathbb{Q}[X, Y]$ ist kein Hauptidealring: $(Y)$ ist prim, aber nicht maximal:

$$\mathbb{Q}[X, Y]/(Y) \cong \mathbb{Q}[X] \text{ ist nullteilerfrei aber kein Körper}$$

Übung: (X,Y) ist kein Hauptideal

### II.6.10 Lemma

Sei $R$ ein Hauptidealring. Ist $I_1 \subseteq I_2 \subseteq \dots$ eine Kette von Idealen von $R$, so existiert ein $n \in \mathbb{N}$ mit $I_n = I_{n+1} = I_{n+1} = \dots$
Beweis: $I := \bigcup_{n \in \mathbb{N}} I_n$ ist ein Ideal von $R$, vgl. 4.18. Da $R$ ein Hauptidealring, gibt es $x \in R$ mit $I = (x)$.

$$x \in \bigcup_{n \in \mathbb{N}} I_n \implies \exists n \in \mathbb{N} : x \in I_n$$

Dann:

$$(x) \subseteq I_n \subseteq I_{n+1} \subseteq I_{n+2} \subseteq \dots \subseteq I = (x)$$

## II.7 Faktorielle Ringe

### II.7.1 Definition

$R$ ist faktoriell $:\iff$ Jedes $0 \neq x \in R \setminus R^\times$ ist Produkt von Primelementen.

### II.7.2 Lemma

Ist $R$ faktoriell und $0 \neq x \in R \setminus R^\times$. Ist $x$ irreduzibel, so auch prim.
Beweis: Da R faktoriell ist, ist $x = p_1 \cdot \dots \cdot p_n$ mit $p_i \in R$ prim.

$$x \text{ irreduzibel} \implies n = 1 \implies x = p_1 \text{ prim}$$

### II.7.3 Satz

Ist $R$ Hauptidealring, so ist $R$ faktoriell.
Beweis: Sei $X = \{a \in R : a \text{ ist Produkt von Primelementen}\} \cup \{0\} \cup R^\times$.
Zu zeigen: $X = R$ Angenommen es existiert ein $a_0 \in R \setminus X$. $a_0$ nicht prim $\implies$ $a_0$ nicht irreduzibel, d.h. $a_0 = a_1 a_1'$ mit $a_1, a_1' \notin R^\times$. Wären $a_1 \in X$ und $a_1' \in X$, so auch $a_0 = a_1 a_1' \in X$, also o.E. $a_1 \notin X$.
Iterativ finden wir $a_2, a_3, \dots$ mit $a_i \not\sim a_{i-1}$. Es ist $(a_0) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \dots$, ein Widerspruch zu 6.11.

### II.7.4 Korollar

$\mathbb{Z}$ und $K[X]$, $K$ ein Körper, sind faktoriell.

### II.7.5 Lemma

Sind $p_1, \dots, p_r \in R$ prim, $q_1, \dots, q_s \in R$ irreduzibel mit $\prod_{i=1}^r p_i = \prod_{j=1}^s q_j$, ist $r = s$ und nach Umnummerierung ist $p_i \sim q_i$ für $i = 1, \dots, r$.
Beweis: Induktion nach $r$, unter der schwächeren Annahme, dass $\prod_{i=1}^r \sim \prod_{j=1}^s q_j$.

$r = 0$: $1 \sim \prod_{j=1}^s q_j \implies q_j \in R^\times \forall j \implies j = 0$

$r - 1 \mapsto r$:

$$\begin{aligned}
&\prod_{i=1}^r p_i \sim \prod_{j=1}^s q_j \\
&\implies p_1 | \prod_{j=1}^s q_j \overset{p_1 \text{ prim}}{\implies} p_1 | q_j \text{ für ein } j, \text{ o.E. } j = 1 \\
&\overset{q_1 \text{ irred.}}{\implies} p_1 \sim q_1 \implies \prod_{i=2}^r p_i \sim \prod_{j=2}^s q_j \\
&\overset{\text{IH}}{\implies} r - 1 = s - 1 \text{ und nach Umnummerierung ist } p_i \sim q_i, i = 2, \dots, r
\end{aligned}$$

### II.7.6 Satz

Ist $R$ faktoriell, so lässt sich jedes $0 \neq x \in R \setminus R^\times$ auf eindeutige Weise (bis auf Reihenfolge und Assoziiertheit) als Produkt von irreduziblen Elementen schreiben.
Beweis: Nach 7.2 sind Primelemente genau die irreduziblen Elemente. Die Eindeutigkeit folgt daher aus 7.5.

### II.7.7 Korollar

Sei $R$ ein faktorieller Ring. Ist $P \subseteq R$ ein Vertretersystem der Primelemente modulo Assoziiertheit, so lässt sich jedes $0 \neq x \in R$ darstellen als

$$x = u \prod_{p \in P} p^{v_p(x)} \tag{$*$}$$

mit eindeutig bestimmten $u \in R^\times, v_p(x) \in \mathbb{N}_0$, fast alle gleich Null. Es ist

$$v_p(x) = \max\{r \in \mathbb{N}_0 : p^r | x\}$$

**Beweis.** Wissen: $x = p_1 \cdot \ldots \cdot p_r$ mit $p_1, \ldots, p_r$ prim. Für jedes $i$ ist $p_i \sim p \in P$ von der Form $(*)$. Daher ist auch $x$ von der Form $(*)$.

### II.7.8 Beispiele

a) **Hauptsatz der Arithmetik.** Jedes $n \in \mathbb{N}$ lässt sich eindeutig schreiben als

$$n = \prod_{p \in \mathbb{P}} p^{v_p(n)}$$

mit $v_p(n) \in \mathbb{N}_0$, fast alle 0.

b) Sei $K$ ein Körper. Bezeichnet $M$ die Menge der normierten, irreduziblen Polynome in $R = K[X]$, so hat jedes $0 \neq f \in K[X]$ eine eindeutige Darstellung

$$f = c \prod_{g \in M} g^{v_g(f)}$$

mit $c \in K^\times, v_g(f) \in \mathbb{N}_0$, fast alle 0.

## II.8 Ringe mit Brüchen

Sei $R$ ein Ring, $S \subseteq R$.

### II.8.1 Definition

$S$ ist multiplikativ $:\iff$ $1 \in S$ und sind $s, t \in S$, so ist auch $st \in S$.

### II.8.2 Beispiele

a) $S = R^\times$

b) $S = \{x \in R : x \text{ ist kein Nullteiler}\}$

c) $S = \{1, s, s^2, \ldots\}$ für ein $s \in R$

d) $S = R \setminus \mathcal{P}$ für ein Primideal $\mathcal{P} \trianglelefteq R$

### II.8.3 Definition

Sei $S \subseteq R \setminus \{0\}$ multiplikativ und ohne Nullteiler. Definiere die Äquivalenzrelation $\sim$ auf $R \times S$ durch

$$(r, s) \sim (r', s') \iff rs' = r's$$

Schreibe $\frac{r}{s}$ für die $\sim$-Äquivalenzklasse von $(r, s)$ und

$$S^{-1}R = R \times S/_\sim = \{\frac{r}{s} : r \in R, s \in S\}$$

Für $r_1, r_2 \in R, s_1, s_2 \in S$ definiere:

$$\frac{r_1}{s_1} + \frac{r_2}{s_2} := \frac{r_1 s_2 + r_2 s_1}{s_1 s_2}$$
$$\frac{r_1}{s_1} \cdot \frac{r_2}{s_2} := \frac{r_1 r_2}{s_1 s_2}$$

### II.8.4 Satz

Die Addition und Multiplikation sind wohldefiniert und machen $S^{-1}R$ zu einem Ring. Die Abbildung

$$\iota : \begin{cases} R \to S^{-1}R \\ r \mapsto \frac{r}{1} \end{cases}$$

ist ein Ringmonomorphismus mit $\iota(S) \subseteq (S^{-1}R)^\times$.
**Beweis.**

- $\sim$ ist Äquivalenzrelation:
  - reflexiv: ✓
  - symmetrisch: ✓
  - transitiv:

$$\begin{aligned} &r_1 s_2 = r_2 s_1, r_2 s_3 = r_3 s_2 \\ \implies &s_2 r_1 s_3 = r_2 s_1 s_3 = r_3 s_2 s_1 \\ \implies &r_1 s_3 = r_3 s_1, \text{ da } s_1 \text{ kein Nullteiler} \end{aligned}$$

- Addition ist wohldefiniert:

$$\frac{r_1}{s_1} = \frac{r_1'}{s_1'}, \frac{r_2}{s_2} = \frac{r_2'}{s_2'} \qquad (*)$$

$$\begin{aligned} \frac{r_1' s_2' + r_2' s_1'}{s_1' s_2'} &= \frac{s_1 s_2 r_1' s_2' + s_1 s_2 r_2' s_1'}{s_1 s_2 s_1' s_2'} \\ &\overset{*}{=} \frac{r_1 s_1' s_2 s_2' + s_1 s_2' r_2 s_1'}{s_1 s_2 s_1' s_2'} = \frac{r_1 s_2 + r_2 s_1}{s_1 s_2} \end{aligned}$$

- Multiplikation: analog.
- $(S^{-1}R, +, \cdot)$ ist ein Ring: Selbststudium.
- $\iota$ ist Homomorphismus:

$$(r_1 r_2) = \frac{r_1 r_2}{1} = \frac{r_1}{1} \cdot \frac{r_2}{1} = \iota(r_1)\iota(r_2)$$

  (Addition analog)
- $\iota(S) \subseteq (S^{-1}R)^\times$:

$$\iota(s) \cdot \frac{1}{s} = \frac{s}{1} \cdot \frac{1}{s} = \frac{s}{s} = \frac{1}{1}$$

  Dies ist das Einselement.□

### II.8.5 Korollar

Ist $R$ nullteilerfrei, so ist $(R \setminus \{0\})^{-1}R$ ein Körper und $\iota : R \to (R \setminus \{0\})^{-1}R$ ist ein Ringmonomorphismus.

### II.8.6 Definition

Ist $R$ nullteilerfrei, so ist $\mathrm{Quot}(R) = (R \setminus \{0\})^{-1}R$ der Quotientenkörper von $R$. Wir identifizieren $R$ mit einem Teilring von $\mathrm{Quot}(R)$ mittels $\iota$.

### II.8.7 Korollar

$R$ ist genau dann isomorph zu einem Teilring eines Körpers, wenn $R$ nullteilerfrei ist. **Beweis.** 8.5 und Körper sind nullteilerfrei.

### II.8.8 Beispiele

a) $\mathrm{Quot}(\mathbb{Z}) = \mathbb{Q}$

b) $\mathrm{Quot}(\mathbb{R}) = \mathbb{R}$

c) $K(X) = \mathrm{Quot}(K[X])$, $K$ ein Körper, der rationale Funktionenkörper einer Variablen $X$ über $K$.

d) $R_{\mathcal{P}} := (R \setminus \mathcal{P})^{-1}R$, die Lokalisierung von $R$ im Primideal $\mathcal{P}$, z.B. $\mathbb{Z}_{(0)} = \mathbb{Q}$, $\mathbb{Z}_{(2)} = \left\{\frac{m}{n} : m \in \mathbb{Z}, n \in \mathbb{N}, 2 \nmid n\right\}$.

### II.8.9 Satz

Sei $R$ faktoriell mit $K = \mathrm{Quot}(R)$. Ist $P$ ein Vertretersystem der Primelemente von $R$ modulo Assoziiertheit, so lässt sich jedes $x \in K^\times$ als

$$x = u \prod_{p \in P} p^{v_p(x)}$$

schreiben mit eindeutig bestimmten $u \in R^\times, v_p(x) \in \mathbb{Z}$ fast alle Null.
**Beweis.**

- *Existenz:* Sei $x = \frac{r}{s}, r \in R, s \in R \setminus \{0\}$. Nach 7.7 ist

$$r = u \prod_{p \in P} p^{v_p(r)},\ s = u \prod_{p \in P} p^{v_p(s)}$$

mit $u, u' \in R^\times,\ v_p(r), v_p(s) \in \mathbb{N}_0$

$$\Longrightarrow \frac{r}{s} = u(u')^{-1} \prod_{p \in P} p^{\overbrace{v_p(r) - v_p(s)}^{\in \mathbb{Z}}}$$

- *Eindeutigkeit:*

$$x = u \prod_{p \in P} p^{k_p} = u' \prod_{p \in P} p^{l_p}\ (k_p, l_p \in \mathbb{Z})$$

$$\Longrightarrow u \prod_{\substack{p \in P \\ k_p \geq l_p}} p^{\overbrace{k_p - l_p}^{\geq 0}} = u' \prod_{\substack{p \in P \\ k_p < l_p}} p^{\overbrace{l_p - k_p}^{\geq 0}}$$

$$\overset{7.7}{\Longrightarrow} k_p = l_p \forall p,\ u = u'$$

### II.8.10 Lemma

Seien $x, y \in K,\ p \in R$ prim.

a) $v_p(xy) = v_p(x) + v_p(y)$

b) $v_p(x+y) \leq \min\{v_p(x), v_p(y)\}$

**Beweis.**

a) klar aus 8.9

b) Für $x, y \in R$ klar aus 7.7. Für $x, y \in K$ schreibe $x = \frac{r_1}{s_1}, y = \frac{r_2}{s_2}$. O.E. $s_1 = s_2 = 2$.

$$v_p(x+y) = v_p(r_1 + r_2) - v_p(s) \geq \min\{v_p(r_1), v_p(r_2)\} - v_p(s) = \min\{v_p(x), v_p(y)\}$$

### II.8.11 Beispiel

Sei $R = \mathbb{Z}, p \in \mathbb{P}$. Die Abb.

$$|\cdot|_p : \begin{cases} \mathbb{Q} \to R_{\geq 0} & \\ x \mapsto p^{-v_p(x)} & , x \neq 0 \\ x \mapsto 0 & , x = 0 \end{cases}$$

i) $|x|_p = 0 \iff x = 0$

ii) $|x+y|_p \leq \max\{|x|_p, |y|_p\} \leq |x|_p + |y|_p$

iii) $|xy|_p = |x|_p |y|_p$

### II.8.12 Bemerkung

Für $x \in K = \text{Quot}(R)$ gilt:

$$x \in R \iff v_p(x) \geq 0 \forall p \in R \text{ prim}$$

## II.9 Der Satz von Gauß

Sei R ein faktorieller Ring, $K := \text{Quot}(R)$ und $p \in R$ prim.

### II.9.1 Bemerkung

Ziel: R faktoriell $\implies$ $R[X]$ faktoriell

Dafür studieren wir folgende Ringe:

$$\begin{array}{ccc} R[X] & \hookrightarrow & K[X] \\ \uparrow & & \uparrow \\ R & \hookrightarrow & K \end{array}$$

Strategie: Verstehen der Primelemente von $R[X]$

### II.9.2 Definition

Für

$$f := \sum_{i=0}^{n} a_i X^i \in K[X]$$

sei

$$v_p(f) := \min_{i=1,\dots,n} v_p(a_i) \in \mathbb{Z} \cup \{\infty\}$$

### II.9.3 Bemerkung

a)

$$\begin{aligned} f \in R[X] &\iff a_i \in R \\ &\iff v_p(a_i) \geq 0 \forall p \in \mathbb{P}_R \\ &\iff v_p(f) \geq 0 \forall p \in \mathbb{P}_R \end{aligned}$$

b)

$$v_p(f+g) \geq \min\{v_p(f), v_p(g)\}$$

(für $f, g \in K[X]$)

### II.9.4 Bemerkung

Der Homomorphismus

$$\pi_{(p)} : \begin{cases} R \to R/(p) \\ x \mapsto \overline{x} := x + (p) \end{cases}$$

setzt sich nach 2.5 fort zu einem Homomorphismus

$$\begin{cases} R[X] \to (R/(p))[X] \\ f = \sum_{i \geq 0} a_i X^i \mapsto \overline{f} := \sum_{i \geq 0} \overline{a}_i X^i \end{cases}$$

genannt <u>Koeffizientenreduktion</u>. Dabei ist

$$\overline{f} = 0 \iff v_p(f) > 0$$

### II.9.5 Satz (Lemma von Gauß)

Für $f, g \in K[X]$ ist

$$v_p(fg) = v_p(f) + v_p(g)$$

<u>Beweis:</u> o.E $f, g \neq 0$

Für $h := \sum a_i X^i$ und $c \in K^\times$ ist

$$\begin{aligned} v_p(ch) &= \min_i v_p(ca_i) \\ &\overset{8.11}{=} v_p(c) + v_p(h) \end{aligned}$$

wir dürfen deshalb $f, g$ mit Konstanten multiplizieren.
$\implies$ o.E. $f, g \in R[X]$ (mult. mit Produkt der Nenner)
$\implies$ o.E. $v_p(f) = v_p(g) = 0$ (mult. mit $p^{-v_p(f)}$ bzw. $p^{-v_p(g)}$)
Somit ist $\overline{f} \neq 0, \overline{g} \neq 0$. Dann gilt

$$\begin{aligned} p \text{ prim} &\implies (p) \text{ Primideal} \\ &\implies R/(p) \text{ ntf.} \\ &\implies (R/(p))[X] \text{ ntf.} \end{aligned}$$

also

$$\overline{fg} = \overline{f} \cdot \overline{g} \neq 0$$

$$\implies v_p(fg) = 0 = v_p(f) + v_p(g) \quad \square$$

### II.9.6 Korollar

$p \in R$ prim $\implies$ p prim in $R[X]$
Beweis:

$$\begin{aligned} p|fg &\implies 0 < v_p(fg) = v_p(f) + v_p(g) \\ &\implies v_p(f) > 0 \text{ oder } v_p(g) > 0 \\ &\implies p|f \text{ oder } p|g \quad \square \end{aligned}$$

### II.9.7 Korollar

Ist $f \in R[X]$ normiert und $f = gh$ mit $g, h \in K[X]$ normiert, dann sind $g, h \in R[X]$
Beweis:
Sei $p \in R$ prim

- $f \in R[X] \implies v_p(f) \geq 0$
- $f, g, h$ normiert $\implies v_p(f), v_p(g), v_p(h) \leq 0$

Dann gilt:

$$\begin{aligned} 0 = v_p(f) &= v_p(g) + v_p(h) \\ &\implies v_p(g) = v_p(h) = 0 \\ &\implies g, h \in R[X] \quad \square \end{aligned}$$

### II.9.8 Korollar

Sei $f \in R[X]$ normiert. ist $a \in K$ mit $f(a) = 0$, so ist schon $a \in R$

Beweis:

$$\begin{aligned} f(a) = 0 &\implies f(X) = (X-a)g mit g \in K[X] normiert \\ &\overset{9.7}{\implies} (X-a) \in R[X] \\ &\implies a \in R \quad \square \end{aligned}$$

### II.9.9 Definition

Sei $f := \sum_{i \geq 0} a_i X^i \in R[X]$

1) $I(f) := \text{ggT}(a_1, \ldots, a_n)$ (Inhalt von f)
2) f primitiv $\iff I(f) \sim 1$

### II.9.10 Bemerkung

a) $I(f)$ ist nur bis auf Einheiten bestimmt.

   Ist $\overline{\mathbb{P}}_R$ ein Vertretersystem der Primelemente in R modulo Assoziiertheit, so ist

$$I(f) = \prod_{p \in \overline{\mathbb{P}}_R} p^{v_p(f)}$$

b) Umformulierung des Lemma von Gauß:

$$I(fg) = I(f) \cdot I(g)$$

c) Zu $f \in R[X]$ ex. $c \in R$, s.d. $f_0 \in R[X]$ primitiv, wenn

$$f = c \cdot f_0$$

   nämlich $c := I(f), f_0 := c^{-1} f$

d) Zu $f \in K[X]$ existiert $c \in K, f_0 \in R[X]$ primitiv mit $f = f_0 \cdot c$ :

$$f := \sum_{i=0}^{n} \frac{r_i}{s_i} X^i$$

   schreibe

$$f = \frac{1}{s_1 - s_n} f_1$$

   und wende c) auf $f_1$ an

### II.9.11 Theorem (Satz von Gauß)

Sei R ein faktorieller Ring und $K := \mathrm{Quot}(R)$

Dann ist auch $R[X]$ faktoriell.

Ein $f \in R[X]$ ist genau dann prim, wenn es einer der Klassen

(A) f ist ein Primelement in R

(B) f ist primitiv und ein Primelement in $K[X]$

angehört.

<u>Beweis:</u>

Seien $0 \neq f \in R[X] \setminus R[X]^{\times}, g, h \in R[X]$

- f vom Typ A $\implies$ f prim in $R[X]$ (Satz 5.6)
- f vom Typ B $\implies$ f prim:

  $$\begin{aligned} f|gh \text{ in } R[X] &\implies f|gh \text{ in } K[X] \\ &\implies f|g \text{ (o.E.) in } K[X] \text{ d.h. } g = f \cdot q, q \in K[X] \end{aligned}$$

  Für alle $p \in R$ prim ist

  $$0 \leq v_p(g) \overset{9.5}{=} \underbrace{v_p(f)}_{=0} + v_p(q) = v_p(q)$$

  also

  $$q \in R[X], f|g \text{ in } R[X]$$

- f ist Produkt von Elementen vom Typ (A) oder (B):

  Schreibe $f = c \cdot f_0, c \in R, f_0 \in R[X]$ primitiv (9.10 c))

  Entweder ist $c \in R^{\times}$ oder c ist Produkt von Primelementen vom Typ A (da R faktoriell)

  Da $K[X]$ faktoriell ist, ist

  $$f_0 = c_0 g_1 \cdots g_n, c_0 \in K^{\times}$$

  $g_1, \dots g_n \in K[X]$ prim.

  nach (9.10 d)) o.E. $g_1, \dots, g_n \in R[X]$ primitiv, also $g_1, \dots, g_n$ vom Type (B).

  Für $p \in R$ prim sieht man

  $$\underbrace{v_p(f_0)}_{=0} = v_p(c_0) + \sum_{i=1}^{n} \underbrace{v_p(g_i)}_{=0}$$

  $$\implies v_p(c_p) = 0$$

  somit $c_0 \in R^{\times}$

Wir haben gezeigt:

- $R[X]$ ist faktoriell

- ist $f \in R[X]$ prim, so ist

$$f = f \cdots f_n$$

  $f_i$ prim, Typ A/B

  also wegen Eindeutigkeit $n = 1$

  $f = f_1$ vom Typ A oder B $\square$

### II.9.12 Beispiele

(a) $\mathbb{Z}[X]$ ist faktoriell, aber kein Hauptidealring

(b) Für einen Körper F ist $F[X_1, \ldots, X_n]$ faktoriell, aber für $n \geq 2$ kein Hauptidealring.

## II.10 Irreduzibilitätskriterien

Sei $R$ faktoriell, $K = \mathrm{Quot}(R)$, $f \in K[X]$

### II.10.1 Bemerkung

Wir suchen hinreichende Kriterien dafür, dass $f$ irreduzibel (=prim) ist.

(a) Für $c \in K^\times$ ist $f$ irreduzibel $\iff$ $cf$ irreduzibel. Es genügt also, **normierte** Polynome zu betrachten.

(b) $\deg f = 1 \implies f$ irreduzibel und hat eine Nullstelle in $K$

(c) $\deg f \geq 2$: $f$ hat Nullstelle in $K \implies f$ ist nicht irreduzibel.

$$f(a) = 0 \implies f = (X-a)g(X), \deg g = \deg f - 1 \geq 1$$

(d) $\deg f \leq 3$: $f$ hat keine Nullstelle $\implies f$ ist irreduzibel.

$$\begin{aligned} f = gh,\ g,h \notin K &\implies \deg g = 1 \vee \deg h = 1 \\ &\implies g \text{ hat Nullstelle oder } h \text{ hat Nullstelle} \\ &\implies f \text{ hat Nullstelle} \end{aligned}$$

### II.10.2 Beispiel

$f = (X^2+1)^2 \in \mathbb{Q}[X]$ hat keine Nullstellen in $\mathbb{Q}$, ist aber **nicht** irreduzibel.

### II.10.3 Satz

Sei $f \in R[X]$ normiert. Ist $\alpha \in K$ eine Nullstelle von $f$, so ist $\alpha \in R$ und $\alpha | f(0)$ in $R$.
**Beweis.**

$$\begin{aligned} f(\alpha) = 0 &\implies f(X) = (X-\alpha)g(X),\ g \in K[X] \text{ normiert} \\ &\overset{9.7.}{\implies} (X-\alpha) \in R[X], g(X) \in R[X] \\ &\implies \underbrace{f(0)}_{\in R} = \underbrace{-\alpha}_{\in R} \cdot \underbrace{g(0)}_{\in R} \end{aligned}$$

### II.10.4 Satz (Reduktionskriterium)

Sei $f \in R[X]$ normiert, $p \in R$ prim. Ist $f \in (R/(p))[X]$ irreduzibel, so ist $f$ irreduzibel in $R[X]$, also insbesondere auch in $K[X]$.
**Beweis.** Sei $f = gh$ mit $g, h \in R[X]$

$$\begin{aligned} &\implies \overline{f} = \overline{gh} = \overline{g}\overline{h} \text{ in } (R/(p))[X] \\ &\overset{\overline{f} \text{ irred.}}{\implies} \text{o.E. } \overline{g} \in (R/(p))[X]^\times \subseteq (R/(p))[X] \end{aligned}$$

Es gilt:

$$\deg g + \deg h = \deg f \overset{f \text{ normiert}}{=} \deg \overline{f} = \underbrace{\deg \overline{g}}_{=0} + \deg \overline{h} \leq \deg h$$

Damit folgt $\deg g = 0$, also $g \in R \overset{f \text{ normiert}}{\implies} g \in R^\times \subseteq R[X]^\times$. Somit ist $f$ irreduzibel in $R[X]$, nach 9.11 auch in $K[X]$, da $f \notin R$.

### II.10.5 Satz (Eisenstein)

Sei $f = \sum_{i=0}^{n} a_i X^i \in R[X] \setminus R$ primitiv und $p \in R$ prim, $p \nmid a_n$, $p | a_i$ für $i = 0, \dots, n-1$, $p^2 \nmid a_0$. Dann ist $f$ irreduzibel in $R[X]$, somit auch in $K[X]$.
**Beweis.** Sei $f = gh$ mit

$$g = \sum_{i=0}^{k} b_i X^i,\ h = \sum_{i=0}^{l} c_i X^i,\ k + l = n,\ b_i, c_i \in R$$

$$p \nmid a_n = b_k c_l \implies p \nmid b_k, p \nmid c_l$$
$$p^2 \nmid a_0 = b_0 c_0, p | a_0 \overset{p \text{ prim}}{\implies} \text{o. E. } p | b_0, p \nmid c_0$$

Sei $m := \max\{i : p | b_i\} \in \{0, \dots, k-1\}$

$$\implies a_{m+1} = \underbrace{b_0 c_{m+1} + b_1 c_m + \ldots + b_m c_1}_{\equiv 0 \mod p} + \underbrace{b_{m+1} c_0}_{\not\equiv 0 \mod p}$$

$$\implies p \nmid a_{m+1} \implies k \geq m + 1 = n \implies l = 0$$

Damit $h \in R$ und da $f$ primitiv: $h \in R^\times \subseteq R[X]^\times$ $\square$

### II.10.6 Beispiele

Sei $p \in R$ prim, $n > 0$. Dann $f = X^n - p$ nach 10.5. irreduzibel in $K[X]$.

(a) $R = \mathbb{Z}$: $X^2 - 5, X^6 - 2 \in \mathbb{Q}[X]$ sind irreduzibel

(b) $R = \mathbb{Q}[Y]$: $X^2 - Y$ irreduzibel in $(\mathbb{Q}[Y])[X] \cong \mathbb{Q}[X, Y]$ und $\mathbb{Q}(Y)[X]$. Ebenso: $X^5 + Y + 1$, $X^3 + (Y-1)X + Y^2 - 1$

### II.10.7 Beispiel

Für $p \in \mathbb{N}$ prim ist $\Phi_p := \frac{X^{p-1}}{X-1} = X^{p-1} + X^{p-2} + \ldots + X + 1 \in \mathbb{Z}[X]$ das $p$-te Kreisteilungspolynom. Die Nullstellen von $\Phi_p$ in $\mathbb{C}$ liegen auf dem Einheitskreis, sind genau die $1 \neq z \in \mathbb{C}$ mit $z^p = 1$, d.h. $z = e^{\frac{2k\pi i}{p}}$ mit $k = 1, \dots, p-1$.
**Behauptung.** $\Phi_p$ ist irreduzibel in $\mathbb{Q}[X]$
**Beweis.**

$$\Phi_p(X+1) = \frac{(X+1)^p - 1}{X} = X^{p-1} + \binom{p}{1} X^{p-2} + \ldots + \binom{p}{p-1}$$

Es gilt: $p \nmid 1$, $p | \binom{p}{k}$, $k = 1, \dots, p-1$, $p^2 \nmid \binom{p}{p-1} = p$
$\implies \Phi_p(X+1)$ ist irreduzibel in $\mathbb{Q}[X]$. Die Abbildung

$$\tau : \begin{cases} \mathbb{Q}[X] \to \mathbb{Q}[X] \\ f(X) \mapsto f(X+1) \end{cases}$$

ist ein Automorphismus von $\mathbb{Q}[X]$ (universelle Eigenschaft, Inverses $f(X) \mapsto f(X-1)$)
Insbesondere also: $\Phi_p$ irreduzibel $\iff \tau(\Phi_p) = \Phi_p(X+1)$ irreduzibel.

# III Körper

## III.1 Körpererweiterungen

Seien $K, L, M$ Körper.

### III.1.1 Bemerkung

(a) Ein Körper ist ein Ring $R$ (kommutativ mit 1) in dem die folgenden äquivalenten Bedingungen gelten:

(1) $R^\times = R \setminus \{0\}$ $(II.1.5)$

(1) $R$ hat genau zwei Ideale $(0) \neq (1)$ $(II.4.4)$

(1) $(0)$ ist ein maximales Ideal. $(II.4.15)$

(b) Ist $\varphi : K \to L$ ein Ringhomomorphismus, so ist

$$\ker\varphi \underset{\neq}{\lhd} K$$

Somit ist jeder Ringhomomorphismus zwischen Körpern injektiv, da $\ker\varphi = (0) = \{0\}$

(c) Der Durchschnitt einer Familie von Teilkörpern von $K$ (d.h. Teilringen von $K$, die Körper sind), ist wieder ein Teilkörper.

(d) Es gibt genau einen Ringhomomorphismus

$$\chi_K : \begin{cases} \mathbb{Z} \to K \\ n \mapsto \underbrace{1_K + \cdots + 1_K}_{n} \end{cases}$$

und $\ker_K \underset{\neq}{\lhd} \mathbb{Z}$. Da $\mathbb{Z}/\ker\chi_K \cong \mathrm{im}\chi_K$ isomorph zu einem Teilring von $K$ und damit nullteilerfrei, ist $\ker\chi_K$ prim. Somit ist die Charakteristik $\mathrm{char}(K) \in \mathbb{R} \cup \{0\}$, dann $\ker\chi_K = (\mathrm{char}(K))$. Ist $K_0$ ein Teilkörper von $K$, so ist $\mathrm{char}(K_0) = \mathrm{char}(K)$.

### III.1.2 Definition

Der <u>Primkörper</u> von $K$ ist der kleinste Teilkörper von $K$ (ex. nach 1.1.c)

### III.1.3 Satz

Sei $\mathbb{F}$ der Primkörper von $K$.

(a) $\mathrm{char}(K) = 0 \iff \mathbb{F} \cong \mathbb{Q}$

(b) $\mathrm{char}(k) = p > 0 \iff \mathbb{F} \cong \mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$

**Beweis.**

$\Leftarrow$ ✓

$\Rightarrow$ $b)$: $\ker\chi_K = (p)$ ist maximal

$$\implies \mathrm{im}(\chi_K) \cong \mathbb{Z}/p\mathbb{Z} \text{ ist Körper}$$

$\implies$ kleinster solcher Körper.

$$\mathbb{F} : \mathrm{im}\chi_K \cong \mathbb{F}_p$$

$a)$

$$\begin{aligned} \chi_K = (0) &\implies \chi_K \text{ injektiv} \\ &\implies \mathrm{im}\chi_K \cong \mathbb{Z} \end{aligned}$$

Setze $\chi_K$ zu einem R-Homomorphismus

$$\chi'_K : \begin{cases} \mathbb{Q} \to K \\ \frac{a}{b} \mapsto \chi_K(b)^{-1} \cdot \chi_K(a) \end{cases}$$

eindeutig fortsetzen. Dann im$\chi'_K = \mathbb{Q}$ Teilkörper von $K$ und offensichtlich der kleinste. □

### III.1.4 Definition

Ist $K$ ein Teilkörper von $L$, so nennt man $L$ eine Körpererweiterung von $K$; in Zeichen $L|K$

### III.1.5 Definition

Seien $L_1|K$ und $L_2|K$ Körpererweiterungen. Ein Ringhomomorphismus $\varphi : L_1 \to L_2$ heißt $K$-Homomorphismus, in Zeichen

$$\varphi : L_1 \to_K L_2$$

wenn $\varphi|_K = id$. Wir schreiben

$$\mathrm{Hom}_K(L_1, L_2) = \{\varphi : L_1 \to_K L_2\}$$

$L_1$ und $L_2$ sind $K$-isomorph, in Zeichen

$$L_1 \cong_K L_2$$

wenn es einen Isomorphismus $\varphi \in \mathrm{Hom}_K(L_1, L_2)$ gibt.

### III.1.6 Bemerkung

Ist $L|K$ eine Körpererweiterung, so wird $L$ durch Einschränkung der Multiplikation $L \times L \to L$ auf $K \times L \to L$ zu einem $K$-Vektorraum.

### III.1.7 Definition

Für eine Körpererweiterung $L|K$ ist

$$[L : K] := \dim_K(L) \in \mathbb{N} \cup \{0\}$$

der Grad (Körpergrad) von $L|K$. $L|K$ heißt endlich, wenn $[L : K] < \infty$

### III.1.8 Beispiel

(a) $[K : K] = 1$

(b) $[\mathbb{C} : \mathbb{R}] = 2 \quad (\mathbb{C} = \mathbb{R} + i \cdot \mathbb{R})$

(c) $[\mathbb{Q}(i) : \mathbb{Q}] = 2 \quad (\mathbb{Q}(i) := \mathbb{Q} + i \cdot \mathbb{Q} \subset \mathbb{C})$

$\mathbb{Q}(i)$ ist Körper:

- Teilring von $\mathbb{C}$ ✓
- Inverse : $x, y \in \mathbb{Q}, (x, y) \neq (0, 0)$

$$\implies \frac{1}{x + iy} = \frac{x - iy}{(x + iy)^2} = \frac{x - iy}{x^2 + y^2} = \frac{x}{x^2 + y^2} - \frac{iy}{x^2 + y^2} \in \mathbb{Q} + \mathbb{Q}i$$

(d) $[\mathbb{R} : \mathbb{Q}] = \infty$

- Kardinalitätsargument
- oder $III.2$

(e) $[\mathbb{F}_p(X) : \mathbb{F}_p] = \infty$

- $1, X, X^2, \ldots$ paarweise verschieden, somit $\mathbb{F}_p(X)$ unendlich

(f) $[\mathbb{Q}(X) : \mathbb{Q}] = \infty$

- $(1, X, X^2, \ldots)$ ist Basis von $\mathbb{Q}[X]$

### III.1.9 Satz

Für Körper $K \subset L \subset M$ ist

$$[M : K] = [M : L][L : K]$$

**Beweis.**

Behauptung:

- $x_1, \ldots, x_n \in L$ $K$-lin unabhängig
- $y_1, \ldots, y_m \in M$ $L$-lin unabhängig

$$\implies \{x_i y_j | (i,j) \in \{1, \ldots, n\} \times \{1, \ldots, m\}\} =: B_{n,m}$$

ist $K$ - lin. unabhängig

Beweis: $\sum_{i,j} \lambda_{ij} x_i y_j = 0$ mit $\lambda_{ij} \in K$

$$\implies \sum_{j=1}^{m} \underbrace{(\sum_{i=1}^{n} \lambda_{ij} x_i)}_{\in L} y_j = 0$$

### III.1.10 Bemerkung

(a) $L|K$ endlich $\implies$ $L|K$ endlich erzeugt

(b) $K[a_1, \ldots, a_n]$ ist das Bild des $K$-Homomorphismus

$$\begin{cases} K[X_1, \ldots, X_n] \to L \\ f \mapsto f(a_1, \ldots, a_n) \end{cases}$$

(c)

$$\begin{aligned} K(a_1, \ldots, a_n) &= \{\frac{\alpha}{\beta} : \alpha, \beta \in K[a_1, \ldots, a_n]\} \\ &\cong \mathrm{Quot}(K[a_1, \ldots, a_n]) \end{aligned}$$

## III.2 Algebraische Körpererweiterung

Sei $L|K$ eine Körpererweiterung, $\alpha \in L$.

### III.2.1 Definition

Gibt es ein $0 \neq f \in K[X]$ mit $f(\alpha) = 0$, so heißt $\alpha$ algebraisch über $K$, sonst transzendent über $K$.

### III.2.2 Beispiel

(a) $i = \sqrt{-1} \in \mathbb{C}$ ist algebraisch über $\mathbb{Q}$:

$$f(i) = 0 \text{ für } f(X) = X^2 + 1 \in \mathbb{Q}[X]$$

(b) Die Eulersche Zahl $e \in \mathbb{R}$ ist transzendent über $\mathbb{Q}$ (Hermite 1873)

(c) Die Kreiszahl $\pi \in \mathbb{R}$ ist transzendent über $\mathbb{Q}$ (Lindemann 1882)

### III.2.3 Lemma

Genau dann ist $\alpha$ algebraisch über $K$, wenn $1, \alpha, \alpha^2, \ldots$ $K$-linear abhängig sind.

**Beweis.**

Für $\lambda_0, \ldots, \lambda_n$ ist

$$\sum_{i=0}^{n} \lambda_i \alpha^i = 0 \iff f(\alpha) = 0 \text{ für}$$
$$f(X) = \sum_{i=0}^{n} \lambda_i X^i \in K[X] \quad \square$$

### III.2.4 Bemerkung

Betrachte den Einsetzunghomomorphismus

$$\varphi : \begin{cases} K[X] \to K[\alpha] \\ f \mapsto f(\alpha) \end{cases}$$

Genau dann ist $\alpha$ algebraisch über $K$, wenn $\ker\varphi_\alpha \neq (0)$

In diesem fall ist $\ker\varphi_\alpha = (f_\alpha)$ für ein $f_\alpha \in K[X]$

Dieses Polynom $f_\alpha$ ist

- irreduziebel: da $K[\alpha]$ nullteilerfrei, ist $(f_\alpha)$ prim
- eindeutig, wenn wir fordern, dass $f_\alpha$ normiert.

### III.2.5 Definition

Sei $\alpha \in L$ algebraisch über $K$,

$$\ker\varphi_\alpha = (f_\alpha) \text{ mit } f_\alpha \text{ normiert.}$$

(1) $\text{MinPol}(a|K) := f_\alpha$ : das <u>Minimalpolynom</u> von $\alpha$ über $K$

(2) $\deg(a|K) := \deg f_\alpha$ : den <u>Grad von $\alpha$</u> über $K$

### III.2.6 Satz

(a) $\alpha$ transzendent über $K$
- $K[\alpha] \cong K[X]$
- $K(\alpha) \cong K(x)$
- $[K(\alpha) : K] = \infty$

(b) $\alpha$ algebraisch über $K$
- $K[\alpha] \cong K(\alpha) \cong K[x]/(f_\alpha)$
- $f_\alpha = \mathrm{MinPol}(\alpha|K)$
- $[K(\alpha) : K] = \deg(\alpha|K) < \infty$

**Beweis.**

(a) $\alpha$ transzendent

$$\begin{aligned}&\implies \ker\varphi_\alpha = (0)\\ &\implies \varphi_\alpha \text{ ist Isomorphismus}\\ &\implies K(\alpha) = \mathrm{Quot}(K[\alpha]) \cong \mathrm{Quot}(K[X]) = K[X]\end{aligned}$$

Da $1, X, X^2, X^3, \dots \in K(x)$ lin- unabhängig über $K$

$$\implies [K(\alpha) : K] = [K(X) : K] = \infty$$

(b)

$$\begin{aligned}f_\alpha \text{ irreduzibel } &\implies n := \deg(f_\alpha) = \min\{\deg(g)|0 \neq g \in K[X], g(\alpha) = 0\}\\ &\implies 1, \alpha, \alpha^2, \dots, \alpha^{n-1} K\text{-lin. unabhängig}\\ &\implies [K(\alpha) : K] \geq n\end{aligned}$$

Für $g \in K[X]$ ist $g = q \cdot f_\alpha + r, \quad q, r \in K[X]$, mit $r = 0$ oder $\deg(r) < \deg(f_\alpha) = n$. Es gilt

$$g(\alpha) = q(\alpha) \cdot \underbrace{f_\alpha(\alpha)}_{0} + r(\alpha) = r(\alpha)$$

$$\implies K[\alpha] = \mathrm{im}\varphi_\alpha = \sum_{i=0}^{n-1} K\alpha^i$$

$$\implies [K(\alpha) : K] \leq n \quad \square$$

### III.2.7 Beispiel

(a) $p \in \mathbb{Z} \implies \sqrt[n]{p} \in \mathbb{Q}$ algebraisch über $\mathbb{Q}$ Nach (10.5) ist $f(X) = X^n - p$ irreduzibel in $\mathbb{Q}[X]$ (Eisenstein).

Also ist $\mathrm{MinPol}(\sqrt[n]{p}|\mathbb{Q}) = X^n - p$, $[\mathbb{Q}(\sqrt[n]{p}) : \mathbb{Q}] = n$

(b) Für $p \in \mathbb{N}$ prim ist $\zeta_p = e^{2\pi i/p} \in \mathbb{C}$ algebraisch über $\mathbb{Q}$

$$f(\zeta_p) = 0 \text{ für } f(X) = X^p - 1 \in \mathbb{Q}[X]$$

Nach $II.10.7$ ist $\phi_p(X) = \frac{X^p-1}{X-1} \in \mathbb{Q}[X]$ irreduzibel über $\mathbb{Q}$

$$\implies \mathrm{MinPol}(\zeta_p|\mathbb{Q}) = X^{p-1} + \dots + X + 1, \quad [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$$

(c) $\pi \in \mathbb{R}$ transzendent über $\mathbb{Q}$

$$\implies [\mathbb{Q}(\pi) : \mathbb{Q}] = \infty$$

### III.2.8 Definition

$$L|K \text{ algebraisch } :\iff \text{ jedes } \alpha \in L \text{ ist algebraisch über } K$$

### III.2.9 Satz

$$L|K \text{ endlich } \implies L|K \text{ algebraisch}$$

**Beweis.**
Sei $\alpha \in L$. Dann

$$\infty > [L : K] = [L : K(\alpha)][K(\alpha) : K]$$

$$\begin{aligned} &\implies [K(\alpha) : K] < \infty \\ &\overset{(2.6)}{\implies} \alpha \text{ nicht transzendent} \\ &\implies \alpha \text{ algebraisch} \quad \square \end{aligned}$$

### III.2.10 Korollar

Ist $L = K(\alpha_1, \dots, \alpha_n)$ mit $\alpha_1, \dots, \alpha_n$ algebraisch über $K$, so ist $L|K$ endlich, insbesondere algebraisch.

**Beweis.** Induktion nach $n$, dann (2.9)

$n = 0$: $L = K$ ✓

$n - 1 \implies n$: $K_1 := K(\alpha_1, \dots, \alpha_{n-1}), \alpha_n$ algebraisch über $K$

$$\text{mit } K[X] \subset K_1[X] \implies \alpha_n \text{ algebraisch über } K_1$$

$$\implies [L : K] = \underbrace{[\underbrace{K_1(\alpha_1)}_{=L} : K_1]}_{<\infty (2.6)} \underbrace{[K_1 : K]}_{<\infty (IH)} < \infty \quad \square$$

### III.2.11 Korollar

Es sind äquivalent:

(1) $L|K$ endlich

(2) $L|K$ ist endlich erzeugt und algebraisch

(3) $L = K(\alpha_1, \dots, \alpha_n)$ mit $\alpha_1, \dots, \alpha_n$ algebraisch über $K$

**Beweis.**

(1) $\implies$ (2): (1.11)+ (2.9)

(2) $\implies$ (3): $\alpha_1, \dots \alpha_n$ algebraisch

(3) $\implies$ (1): (2.10) $\square$

### III.2.12 Satz

Für Körper $K \subset L \subset M$ sind äquivalent:

(1) $M|K$ ist algebraisch

(2) $M|L$ ist algebraisch und $L|K$ ist algebraisch

**Beweis.**

(1) $\implies$ (2): – $M|K$ algebraisch $\implies$ $L|K$ algebraisch

– $M|K$ algebraisch $\implies$ $M|L$ algebraisch: $K[X] \subset L[X]$

(2) $\implies$ (1): Sei $\alpha \in M$. Sei $f := \text{MinPol}(\alpha|L) = \sum_{i=0}^{n} \alpha_i X^i \in L[X]$

Definiere $L_0 := K(\alpha_0, \ldots, \alpha_n) \subset L$

$$\begin{aligned}
&\implies f \in L_0[X], f(\alpha) = 0 \\
&\implies \alpha \text{ ist algebraisch über } L_0 \\
&\implies [K(\alpha) : K] \geq [K(\alpha_1, \ldots, \alpha_n) : K] = \underbrace{[L_0(\alpha) : L_0]}_{<\infty(2.6)} \underbrace{[L_0 : K]}_{<\infty(2.10)}
\end{aligned}$$

□

### III.2.13 Beispiel

$\pi$ ist transzendent über $\mathbb{Q}(i)$, denn wäre $\mathbb{Q}(i)(\pi)$ algebraisch über $\mathbb{Q}(i)$, so (da $\mathbb{Q}(i)|\mathbb{Q}$ algebraisch) auch $\mathbb{Q}(i)(\pi)|\mathbb{Q}$ algebraisch.

## III.3 Wurzel- und Zerfällungskörper

Sei $K$ ein Körper, $0 \neq f \in K[X]$ und $n := \deg(f) > 0$.

### III.3.1 Beispiel

Ist $K := \mathbb{Q}$, so hat $f$ eine Nullstelle ("Wurzel") $\alpha \in \mathbb{C}$ (Fudamentalsatz der Algebra) und $L := \mathbb{Q}(\alpha)$ ist die kleinste Erweiterung von $\mathbb{Q}$ in $\mathbb{C}$, die diese Nullstelle enthält, z.B.: $f = X^2 + 1, \mathbb{Q}(i)$

### III.3.2 Definition

Ein <u>Wurzelkörper</u> von $f$ ist eine Erweiterung $L|K$ der Form

$$L = K(\alpha) \text{ mit } f(\alpha) = 0$$

### III.3.3 Lemma

Sei $L = K(\alpha)$ mit $f(\alpha) = 0$ ein Wurzelkörper von $f$. Dann ist $[L : K] = n$ und $g \mapsto g(\alpha)$ induziert einen Isomorphismus

$$K[X]/(f) \xrightarrow{\cong}_K L$$

**Beweis.**

- Ist $f$ irreduzibel, so ist $f = c \cdot \mathrm{MinPol}(\alpha|K)$ mit $c \in K^\times$, daher folgt die Behauptung aus 2.6.
- Ist $f$ beliebig, schreibe $f = f_1 \cdot \ldots \cdot f_r$ mit $f_i \in K[X]$ irreduzibel.

$$f(\alpha) = 0 \implies \text{o.E. } f_1(\alpha) = 0 \implies [L : K] = \deg f_1 \leq deg f = n$$

### III.3.4 Satz

Sei $f$ irreduzibel

a) $L := K[X]/(f)$ ist ein Wurzelkörper von $f$.

b) Ein Wurzelkörper von $f$ ist eindeutig bestimmt im folgenden Sinn: Sind $L_1 = K(\alpha_1)$, $L_2 = K(\alpha_2)$ mit $f(\alpha_1) = f(\alpha_2) = 0$, so existiert genau ein $K$-Isomorphismus $\varphi : L_1 \to_K L_2$ mit $\varphi(\alpha_1) = \alpha_2$.

**Beweis.**

a) Betrachte den Ringepimorphismus

$$\pi = \pi(f) : \begin{cases} K[X] \to K[X]/(f) = L \\ g \mapsto g + (f) \end{cases}$$

und setze $\alpha = \pi(X)$.

- $K$ Körper $\implies$ $\pi|_K$ injektiv $\implies$ können $K$ via $\pi$ mit einem Teilkörper von $L$ identifizieren.
- $f$ irreduzibel $\overset{\text{II.6.9}}{\implies}$ $(f)$ ist maximal $\implies$ $K[X]/(f)$ ist Körper.
- $f(\alpha) = f(\pi(X)) = \pi(f(X)) \overset{f \in \ker(\pi)}{=} 0$
- $L = \pi(K[X]) = K[\alpha]$, insbesondere $L = K(\alpha)$.

b) 3.3. liefert Isomorphismen:

$$\begin{array}{c} L_1 \; {}_K\!\overset{\cong}{\underset{\varphi_1}{\longleftarrow}} K[X]/(f) \overset{\cong}{\underset{\varphi_2}{\longrightarrow}}_K \; L_2 \\ \alpha_1 \longleftarrow\!\!\shortmid X + (f) \longmapsto \alpha_2 \end{array}$$

Damit $\varphi_2 \circ \varphi_1^{-1} : L_1 \xrightarrow{\cong}_K L_2$ mit $(\varphi_2 \circ \varphi_1^{-1})(\alpha_1) = \alpha_2$. Umgekehrt ist jeder $K$-Isomorphismus $\varphi : L_1 \longrightarrow_K L_2$ schon durch $\varphi(\alpha_1)$ bestimmt, denn $L_1 = K(\alpha_1)$.

### III.3.5 Korollar

Es gibt zu jedem $f \in K[X] \setminus K$ einen Wurzelkörper $L|K$.
**Beweis.** Schreibe $f = f_1 \cdot \ldots \cdot f_r$ mit $f_i$ irreduzibel, setze $L = K[X]/(f_1)$.

### III.3.6 Korollar

Zu jedem $f \in K[X] \setminus K$ gibt es eine Körpererweiterung $L|K$, über der $f$ in Linearfaktoren zerfällt, genauer:

$$f(X) = c \cdot \prod_{i=1}^{n} (X - \alpha_i),\ c \in K^\times,\ \alpha_1, \ldots, \alpha_n \in L$$

**Beweis.** Schreibe $f = c \cdot f_0$ mit $c \in K^\times, f_0 \in K^\times$ normiert. Induktion nach $n = \deg f$.

$n = 1$ $L = K$✓

$n-1 \to n$ Nach 3.5 existiert $L_1|K$, wobei $L_1 = K(\alpha_1)$, $f_0(\alpha_1) = 0$, also $f_0 = (X - \alpha_1) \cdot f_1$, $f_1 \in L_1[X]$, $\deg f_1 = n - 1$, $LC(f_1) = 1$. Damit existiert nach der Induktionshypothese eine Körpererweiterung $L|L_1$ sowie $\alpha_2, \ldots, \alpha_n$ mit $f_1 = \prod_{i=2}^n (X - \alpha_i)$

### III.3.7 Definition

Ein Zerfällungskörper von $f$ ist eine Erweiterung der Form $L = K(\alpha_1, \ldots, \alpha_n)$ mit

$$f = c \cdot \prod_{i=1}^{n} (X - \alpha_i),\ c \in K^\times$$

### III.3.8 Satz

Jedes $f \in K[X] \setminus K$ besitzt einen Zerfällungskörper $L$. Dieser ist eindeutig bestimmt bis auf $K$-Isomorphie und $[L : K] \leq n!$.
**Beweis.**

- Existenz: Ist $L$ wie in 3.6, so ist $L = K(\alpha_1, \ldots, \alpha_n)$
- Eindeutigkeit: vgl. 3.4 b), siehe auch Bosch.
- Grad: Sei $L = K(\alpha_1, \ldots, \alpha_n)$, $f = c \cdot \prod_{i=1}^n (X - \alpha_i)$, $c \in K^\times$. Induktion nach $n$:

$n = 1$ $L = K$

$n-1 \to n$ $L_1 = K(\alpha_1)$ ist ein Wurzelkörper von $f$. Mit 3.2 folgt $[L_1 : K] \leq n$. Schreibe $f = c \cdot (X - \alpha_1) f_1, f_1 = \prod_{i=2}^n (X - \alpha_i) \in L_1[X]$. Dann ist $L$ Zerfällungskörper von $f_1 \in L_1[X]$. Damit folgt:

$$[L : K] = \underbrace{[L : L_1]}_{\leq (n-1)! \text{ nach IH}} \cdot \underbrace{[L_1 : K]}_{\leq n} \leq n!$$

### III.3.9 Beispiele

a) $\deg f = 2$: Jeder Wurzelkörper von $f$ ist ein Zerfällungskörper von $f$, z.B. $f = X^2 - 5 \in \mathbb{Q}[X]$, dabei ist $\mathbb{Q}(\sqrt{5})$ der Zerfällungskörper, $f = (X - \sqrt{5})(X + \sqrt{5})$, $\sqrt{5}, -\sqrt{5} \in \mathbb{Q}(\sqrt{5})$

b) $\deg f = 3$, $f$ irreduzibel. Sei $L_1 = K(\alpha_1)$, $f = (X - \alpha_1) \cdot f_1, f_1 \in L_1[X]$.
Ist $f_1 \in L_1[X]$ reduzibel, so ist der Wurzelkörper $L = L_1$ von $f$ schon ein Zerfällungskörper von $f$ vom Grad $[L : K] = \deg(f) = 3$.
Ist $f_1$ irreduzibel, so ist jeder Wurzelkörper $L$ von $f_1$ ein Zerfällungskörper von $f$ mit $[L : K] = [L : L_1][L_1 : K] = 2 \cdot 3 = 6$
**konkretes Beispiel:** $f = X^3 - 2 \in \mathbb{Q}[X]$, also

$$f = (X - \sqrt[3]{2})(X - e^{\frac{2\pi i}{3}} \sqrt[3]{2})(X - e^{\frac{4\pi i}{3}} \sqrt[3]{2}$$

$L_1 := \mathbb{Q}(\sqrt[3]{2}) \implies [L_1 : \mathbb{Q}] = 3$. $\alpha_2, \alpha_3 \notin \mathbb{Q}(\alpha_1) \subseteq \mathbb{R}$, denn $\alpha_2, \alpha_3 \notin \mathbb{R}$. Zerfällungskörper ist $L = L_1(\alpha_2) = \mathbb{Q}(\sqrt[3]{2}, e^{\frac{2\pi i}{3}} \sqrt[3]{2})$ mit $[L : \mathbb{Q}] = 6$.
Ausrechnen zeigt, dass tatsächlich $f = (X - \sqrt[3]{2}) \cdot f_1$ mit $f_1 \in \mathbb{Q}(\sqrt[3]{2})[X]$
**Beispiel für den anderen Fall:** $f$ über $\mathbb{Q}(e^{\frac{2\pi i}{3}})$

## III.4 Endliche Körper

Klassifikation und Konstruktion endlicher Körper

### III.4.1 Lemma

Ist $K$ ein endlicher Körper, dann existieren $p \in \mathbb{P}$ und $n \in \mathbb{N}$ mit $\#K = p^n$

**Beweis.**

Da $K$ endlich, ist der Primkörper von $K$ gleich $\mathbb{F}_p$ für ein $p \in \mathbb{P}$ (III.1.3).

Nach (III.1.6) ist $K$ ein $\mathbb{F}_p$-Vektorraum.

Sei $n$ die Dimension von $K$ als $\mathbb{F}_p$-VR. Dann gibt es $p^n$ Elemente in $K$.

**Bemerkung.** Konstruktion endlicher Körper.

- Wähle $p \in \mathbb{P}, n \in \mathbb{N}$
  - $n = 1 \implies K \cong \mathbb{F}_p$
  - $n \geq 2$ Wähle irreduzibles (und normiertes) Polynom

    $$f(X) = \sum_{i=0}^{n} b_i X^i \in \mathbb{F}_p[X]$$

    mit $deg(f) = n$.
- zwei ähnliche Konstruktionen:
  (a) Konstruktion als Faktorring:

  $$K := \mathbb{F}_p[X]/(f)$$

  ist nach III.2.6 Körper mit $p^n$ Elementen.

  Elemente: $f + (f) = 0 + (f)$

  Mit Polynomdivision kann gezeigt werden, dass jede Nebenklasse einem Vertreter vom Grad $< n$ hat.

  $$\implies K = \{\overline{\sum_{i=0}^{n-1} a_i X^i} | a_i \in \mathbb{F}_p\}$$

  (b) Konstruktion als Körpererweiterung:

  Sei $\alpha$ Nullstelle von $f$ in einem Erweiterungskörper $\mathbb{F}_p(\alpha)$, dann gilt

  $$[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = n \qquad (III.3.3)$$

  Somit ist $\mathbb{F}_p(\alpha)$ ein $\mathbb{F}_p$-Vektorraum der Dimension $n$ und einer Basis $\{1, \alpha^1, \alpha^2, \ldots, \alpha^{n-1}\}$.

  $$\implies \mathbb{F}_p(\alpha) = \{\sum_{i=0}^{n-1} a_i \alpha^i | a_i \in \mathbb{F}_p\}$$

  Es gilt $\mathbb{F}_p(\alpha) \cong_\varphi \mathbb{F}_p[X]/(f)$ mit

  $$\varphi : \sum_{i=0}^{n-1} a_i \alpha^i \mapsto \overline{\sum_{i=0}^{n-1} a_i X^i}$$

  Isomorphismus.

**Bemerkung.**

Zur Klassifikation der endlihen Körper könnte versucht werden, zu jedem $p \in \mathbb{P}, n \geq 2$ ein irreduzibles Polynom $f \in \mathbb{F}_p[X]$ vom Grad $n$ zu konstruieren.

**ABER:** schwer.

### III.4.2 Lemma

Ist $K$ ein Körper, $\#K = q$ und $L|K$ eine Körpererweiterung mit $[L : K] = d \in \mathbb{N}$, dann ist $L$ ein Zerfällungskörper des Polynoms

$$f(X) := X^{q^d} - X \in K[X]$$

**Beweis.**
$L^\times \cong C_{q^d-1} \quad (\#L^\times = q^d - 1)$

$$\begin{aligned}
&\implies \forall \alpha \in L^\times : \alpha^{(q^d-1)} = 1\\
&\implies \forall \alpha \in L^\times : \alpha^{(q^d)} - \alpha = 0\\
&\implies \forall \alpha \in L^\times : f(\alpha) = 0 \wedge f(0) = 0\\
&\implies \forall \alpha \in L : f(\alpha) = 0
\end{aligned}$$

Damit hat man $q^d$ Nullstellen gefunden, d.h.

$$f(X) = \prod_{\alpha \in L} (X - \alpha)$$

also zerfällt $f$ in $L$. Somit ist $L$ Zerfällungskörper von $f$.

### III.4.3 Definition

Die formale Ableitung eines Polynoms

$$f(X) := \sum_{i=0}^{n} a_i X^i \in F[X]$$

(mit $F$ Körper) ist das Polynom

$$f'(X) := \sum_{i=0}^{n} i \cdot a_i X^{i-1}$$

### III.4.4 Lemma

Für $f, g \in F[X]$ gelten

(a) $(f + g)' = f' + g'$

(b) $(fg)' = f'g + fg'$

**Beweis.** siehe Übung

### III.4.5 Lemma

Sei $f \in F[X]$ und $deg(f) = n$. Sei $E$ ein Zerfällungskörper von $f$.

Ist $1 \in ggT_F(f, f')$, dann hat $f$ $n$ paarweise verschiedene Nullstellen in $E$.

**Beweis.**

Sei $f = c \cdot \prod_{i=1}^{n}(X - \alpha_i)$, $E = F(\alpha_1, \dots, \alpha_n)$. Wäre $\alpha_i = \alpha_j$, dann $f = (X - \alpha_i)^2 \cdot g$ $(g \in E[X])$ und

$$f'(X) = 2(X - \alpha_i)f(X) + (X - \alpha_i)^2 g'(X)$$

$$\implies X - \alpha_i | ggT_E(f, f') \lightning$$

Dies wäre ein Widerspruch.

Beachte : $ggT_E(f, f') = ggT_F(f, f')$ (wird mit euklidischen Algorithmus berechnet $\implies$ nur Elemente in $F$)

### III.4.6 Definition

Sei $F$ ein Körper, $char(F) = p$.

Der Frobenius-Endomorphismus ist die Abbildung

$$\phi_p : \begin{cases} F \to F \\ x \mapsto x^p \end{cases}$$

### III.4.7 Lemma

(a) $\phi_p \in END(F) = Hom(F, F)$

(b) Ist $F$ endlch, dann $\phi_p \in Aut(F)$

**Beweis.**

(a)

$$(xy)^p = x^p y^p$$
$$(x + y)^p = x^p + y^p$$

(Ü29)

(b) $\phi_p$ injektiv:

$$\begin{aligned} x^p = y^p &\implies x^p - y^p = 0 \\ &\implies (x - y)^p = 0 \\ &\implies x = y \end{aligned}$$

(Da $F$ nullteilerfrei)

Da $f$ endlich, ist $\phi_p$ auch surjektiv und damit eine Bijektion.

### III.4.8 Lemma

Für jedes $\sigma \in End(F)$ ($F$ Körper) ist

$$F^\sigma := \{x \in F | \sigma(x) = x\}$$

ein Körper, der Fixkörper von $\sigma$

**Beweis.**

Seien $x, y \in F^\sigma, 0 \neq u \in F^\sigma$. Dann gilt

- $\sigma(x \pm y) = \sigma(x) \pm \sigma(y) = x \pm y \implies x \pm y \in F^\sigma$

- $\sigma(xy) = \sigma(x)\sigma(y) = xy \implies xy \in F^\sigma$
- $\sigma(u^{-1}) = \sigma(u)^{-1} = u^{-1} \implies u^{-1} \in F^\sigma$
- $0, 1 \in F^\sigma$

### III.4.9 Theorem

Sei $K$ endlich, $\#K = q = p^n, p \in \mathbb{P}$. Zu jedem $d \in \mathbb{N}$ existiert bis auf Isomorphie genau eine Erweiterung $K_d|K$ mit $[K_d : K] = d$, nämlich der Zerfällungskörper von $f = X^{q^d} - X$.

**Beweis.**

- Eindeutigkeit: III.4.2 + III.3.2 + III.3.11
- Existenz:

  Sei $L$ Zerfällungskörper von $f$, d.h.

  - $f = \prod_{i=1}^{q^d}(X - \alpha_i)$
  - $L = K(\alpha_1, \dots, \alpha_{q^d})$

  Wähle $\sigma : L \to L$ mit

  $$\sigma := (\phi_p)^{dn} = (x \mapsto x^{p^{nd}})$$

  Da $L$ endlich, ist $\sigma$ Automorphismus.

  Es ist

  $$\begin{aligned} L^\sigma &= \{x \in L | x^{p^{nd}} = x\} \\ &= \{x \in L | x^{p^{nd}} - x = 0\} \\ &= \{x \in L | f(x) = 0\} \\ &= \{\alpha_1, \dots, \alpha_{q^d}\} \subset L \end{aligned}$$

  $L^\sigma = K \cup \{\alpha_1, \dots, \alpha_{q^d}\}$

  denn $\forall k \in K$:

  $$\sigma(k) = k^{p^{n^d}} = k^{q^d} = k$$

  weil $k^q = k$

  $\implies K(\alpha_1, \dots, \alpha_{q^d}) = L$ ist der kleinste Körper mit

  $$K \cup \{\alpha_1, \dots, \alpha_{q^d}\} \subset L$$

  $\implies L = L^\sigma = \{\alpha_1, \dots, \alpha_{q^d}\}$

  Außerdem sind die $\alpha_i$ paarweise verschieden, denn

  $$\begin{aligned} f' &= q^d X^{q^d - 1} - 1 \\ &= p^{n \cdot d} X^{q^d} - 1 \\ &= -1 \sim 1 \end{aligned}$$

  $\implies ggT(f, f') = 1$

Also $\#L = \#\{\alpha_1, \ldots, \alpha_{q^d}\} = q^d$
$\implies [L : K] = d$

### III.4.10 Korollar

Zu jeder Primpotenz $q = p^n$ gibt es bis auf Isomorphie genau einen Körper mit $q$ Elementen.

**Beweis.** III.4.9