# Lineare Algebra I

## Woche 07

28.11.2023 und 30.11.2023

Änderungen in KW51

- Montag, 18.12. um 14:15 Uhr Vorlesung statt Plenarübung
- Dienstag, 19.12. to be announced
- Montag, 08.01. Plenarübung wird geplant zur Woche 09

# Körper

## Definition

Ein **Körper** $(K, +, \cdot)$ ist eine Menge $K$ mit zwei Verknüpfungen $+$ und $\cdot$, die die folgenden Bedingungen erfüllen:

1. $(K, +)$ ist eine abelsche Gruppe mit Nullelement $0_K$.

wie beim Ring

2. $(K \setminus \{0_K\}, \cdot)$ ist eine abelsche Gruppe mit Einselement $1_K$.

(wegen $0_K \cdot a = 0_K$ für alle $a \in K$ ist $0_K$ nicht multiplikativ invertierbar.

3. Es gelten die **Distributivgesetze**

fasse zusammen

$$\begin{cases} a \cdot (b + c) = (a \cdot b) + (a \cdot c) \\ (a + b) \cdot c = (a \cdot c) + (b \cdot c) \end{cases}$$

Ein Körper ist ein spezieller kommutativer Ring mit Einselement $1_K$.

# Körper

## Beispiel

1. $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$ sind Körper.

   Nullelement ist 0.
   Einselement ist 1.

2. $(\mathbb{Z}_2, +_2, \cdot_2)$ ist ein kleinstmöglicher Körper. bis auf Isomorphie eindeutig

   $= \{\overline{0}, \overline{1}\}$

3. Der Restklassenring $(\mathbb{Z}/4\mathbb{Z}, \tilde{+}, \tilde{\cdot})$ mit dem Nullelement [0] und dem Einselement [1] ist *kein* Körper.

   Denn: $[2] \neq [0]$ hat keine multipl. Inverse!
   $[2] \tilde{\cdot} [a] \neq [1]$ für alle $a \in \mathbb{Z}$.

   Siehe Woche 06 Folie 22

# Funktionen mit Werten in einem Körper

Bisher: Eigenschaften einer Struktur betrachten
Jetzt auf Funktionen in die Struktur

**Beispiel**

Es sei $X$ eine Menge.

1. Ist $(H, +)$ eine Halbgruppe, dann ist auch $(H^X, +)$ Halbgruppe.
2. Ist $(M, +)$ ein Monoid, dann ist auch $(M^X, +)$ ein Monoid.
3. Ist $(G, +)$ eine Gruppe, dann ist auch $(G^X, +)$ eine Gruppe.
4. Ist $(R, +, \cdot)$ ein Ring, dann ist auch $(R^X, +, \cdot)$ ein Ring.
5. Ist $(K, +, \cdot)$ ein Körper, dann ist $(K^X, +, \cdot)$ i.A. kein Körper, denn $K^X \setminus \{0\}$ enthält bzgl. $\cdot$ nicht-invertierbare Elemente. (Nullfunktion) Folie 24 von Woche 06

Ausnahme: $\#X = 1$. Dann $K^X \cong K$

# Eigenschaften eines Körpers

## Lemma

Es sei $(K, +, \cdot)$ ein Körper mit dem Nullelement $0_K$ und dem Einselement $1_K$.

1. $0_K \neq 1_K$. Ein Körper hat mind. 2 Elemente
2. $(K, +, \cdot)$ ist ein kommutativer, nullteilerfreier Ring mit dem Einselement $1_K$ ungleich dem Nullring, also ein Integritätsring.
3. Es gelten die **Kürzungsregeln** in der Gruppe $(K \setminus \{0_K\}, \cdot)$

$$a \star b_1 = a \star b_2 \quad \Rightarrow \quad b_1 = b_2$$
$$b_1 \star a = b_2 \star a \quad \Rightarrow \quad b_1 = b_2$$

für $a, b_1, b_2 \in K$ mit $a \neq 0_K$.

# Charakteristik eines Körpers

## Definition

Es sei $(K, +, \cdot)$ ein Körper.

Wenn $n\,1_K = 0_K$ für ein $n \in \mathbb{N}$ gilt, dann heißt

$$\min\{n \in \mathbb{N} \mid n\,1_K = 0_K\}$$

die **Chakteristik** von $K$, kurz $\operatorname{char}(K)$. Andernfalls setzen wir $\operatorname{char}(K) = 0$.

Wegen $1_K \neq 0_K$ kann char(K) nicht 1 sein.

## Beispiel

1. $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$ haben Charakteristik 0.
2. $(\mathbb{Z}_2, +_2, \cdot_2)$ hat Charakteristik 2.

Fakt: char(K) ist Null oder Primzahl.

# Wann ist ein Ring ein Körper?

## Satz

Für eine Menge $(K, +, \cdot)$ mit zwei Verknüpfungen sind äquivalent:

1. $(K, +, \cdot)$ ist ein Körper, dessen Nullelement mit $0_K$ und dessen Einselement mit $1_K$ bezeichnet werden.
2. $(K, +, \cdot)$ ist ein kommutativer Ring mit dem Einselement $1_K$ und dem Nullelement $0_K \neq 1_K$, wobei zu jedem $a \in K \setminus \{0_K\}$ ein Inverses bzgl. $\cdot$ in $K$ existiert.

Beweis. ① ⇒ ②: Kommutatives Ring mit Einselement $1_K$. $0_K \neq 1_K$ wurde gezeigt (Folie 05). $(K \setminus \{0_K\}, \cdot)$ ist Gruppe, damit ex. die Inversen.

# Wann ist ein Ring ein Körper?

## Satz

Für eine Menge $(K, +, \cdot)$ mit zwei Verknüpfungen sind äquivalent:

1. $(K, +, \cdot)$ ist ein Körper, dessen Nullelement mit $0_K$ und dessen Einselement mit $1_K$ bezeichnet werden.
2. $(K, +, \cdot)$ ist ein kommutativer Ring mit dem Einselement $1_K$ und dem Nullelement $0_K \neq 1_K$, wobei zu jedem $a \in K \setminus \{0_K\}$ ein Inverses bzgl. $\cdot$ in $K$ existiert.

Beweis. ② ⇒ ① $(K, +)$ ist abelsche Gruppe ✓
Distributivgesetze ✓ Zu zeigen: $(K \setminus \{0_K\}, \cdot)$ ist abelsche Gruppe. Wir wissen $(K, \cdot)$ ist abelsches Monoid mit $1_K$.
$(K \setminus \{0_K\}, \cdot)$ ist abgeschlossen! denn $a \cdot b = 0_K$, $a \neq 0_K$
$\Rightarrow b = a^{-1} \cdot (a \cdot b) = a^{-1} \cdot 0_K = 0_K$. $\Rightarrow (K \setminus \{0_K\}, \cdot)$
ist abelsches Monoid, mit Invertierbarkeit Gruppe.

# endliche Integritätsringe sind Körper

## Satz

Es sei $(R, +, \cdot)$ ein Integritätsring mit endlich vielen Elementen.

Dann ist $(R, +, \cdot)$ ein Körper.

## Folgerung

Der

- Restklassenring modulo $m$ $(\mathbb{Z}\,/\,m\,\mathbb{Z}, \widetilde{+}, \widetilde{\cdot})$
- der zu ihm isomorphe Ring von $\mathbb{Z}$ modulo $m$ $(\mathbb{Z}_m, +_m, \cdot_m)$

sind Körper genau dann, wenn $m \in \mathbb{N}$ eine Primzahl ist.

Restklassenkörper modulo m, wenn m eine Primzahl ist.

# Unterkörper oder Teilkörper

## Definition

Es sei $(K, +, \cdot)$ ein Körper.

1. Eine bzgl. $+$ und $\cdot$ abgeschlossene Teilmenge $U \subseteq K$ heißt ein **Unterkörper** von $(K, +, \cdot)$, wenn $(U, +, \cdot)$ selbst wieder ein Körper ist.
   - $(U, +)$ ist Untergruppe von $(K, +)$.
   - $(U \setminus \{0\}, \cdot)$ ist Untergruppe von $(K \setminus \{0\}, \cdot)$.
2. Ein Unterkörper $(U, +, \cdot)$ von $(K, +, \cdot)$ heißt **echt**, wenn $U \subsetneq K$ gilt.

## Beispiel

1. $(\mathbb{Q}, +, \cdot)$ ist ein Unterkörper von $(\mathbb{R}, +, \cdot)$.
2. $(\mathbb{R}, +, \cdot)$ ist ein Unterkörper von $(\mathbb{C}, +, \cdot)$.

# Homomorphismus von Körpern

Es seien $(K_1, +_1, \cdot_1)$ und $(K_2, +_2, \cdot_2)$ zwei Körper.

## Definition

1. Eine Abbildung $f : K_1 \to K_2$ heißt **strukturverträglich** oder ein **Homomorphismus** von $(K_1, +_1, \cdot_1)$ in $(K_2, +_2, \cdot_2)$, wenn gilt:

$$\begin{aligned} f(a +_1 b) &= f(a) +_2 f(b) \quad \text{für alle } a, b \in K_1, \\ f(a \cdot_1 b) &= f(a) \cdot_2 f(b) \quad \text{für alle } a, b \in K_1, \\ f(1_{K_1}) &= 1_{K_2}. \end{aligned}$$

Bedingungen identisch zu Homom. zwischen Ringen mit Eins.

2. Ist zudem $f : H_1 \to H_2$ bijektiv, so heißt $f$ auch **strukturerhaltend** oder ein **Isomorphismus**.

# Körperhomomorphismen sind injektiv

**Lemma**

Es sei $f : (K_1, +_1, \cdot_1) \to (K_2, +_2, \cdot_2)$ ein Körperhomomorphismus.

Dann ist $f$ injektiv.

Beweis. Es sei $a \neq b$, aber $f(a) = f(b)$.

$$1_{K_2} = f(1_{K_1}) = f((a -_1 b)^{-1} \cdot_1 (a -_1 b))$$

$$= f((a -_1 b)^{-1}) \cdot_2 f(a -_1 b)$$

$$= f((a -_1 b)^{-1}) \cdot_2 [\underbrace{f(a) -_2 f(b)}_{= 0_{K_2}}]$$

$$= 0_{K_2} \quad \lightning.$$

# Polynom (Beispiel klasse von Ringen)

## Definition

Es sei $(R, +, \cdot)$ ein kommutativer Ring. (oft sogar ein Körper) (Koeffizientenring)

1. Ein **Polynom** über $R$ in der Variablen $t$ ist ein formaler Ausdruck der Gestalt ($n \in \mathbb{N}_0$)
$$a_n \cdot t^n + a_{n-1} \cdot t^{n-1} + \cdots + a_1 \cdot t^1 + a_0 \cdot t^0 \quad \text{oder} \quad \sum_{i=0}^{n} a_i \cdot t^i.$$
(Koeffizient $\in R$) (Terme mit Koeff. $0_R$ werden oft weggelassen.)
2. Die Menge aller Polynome in der Variablen $t$ über $R$ ist $R[t]$.
3. Ein **konstantes Polynom** hat $a_1 = a_2 = \cdots = 0_R$
4. Das **Nullpolynom** hat alle Koeff. $= 0_R$.
5. Ein **Monom** hat einen Koeff. $1_R$ (Ring mit Eins!) und alle anderen gleich $0_R$.
6. Das **Einspolynom** hat $a_0 = 1_R$ und $a_1 = a_2 = \cdots = 0_R$

Spezialfall

# Polynom

## Beispiel

1. $(R, t, \cdot) = (\mathbb{Q}, t, \cdot)$

   $p = \frac{3}{4} \cdot t^2 - 7t + \frac{1}{2} = \frac{1}{2} + \frac{3}{4} \cdot t^2 - 7 \cdot t \in \mathbb{Q}[t]$

2. $(R, t, \cdot) = (\mathbb{Z}_2, \tau_2, \cdot_2)$

   $p = 1 \cdot s^3 + 0 \cdot s^2 + 0 \cdot s + 1 = s^3 + 1 \in \mathbb{Z}_2[s]$

3. $(R, t, \cdot) = (\mathbb{Z}/4\mathbb{Z}, \tilde{+}, \tilde{\cdot})$

   $p = [1] \tilde{\cdot} X^3 \tilde{+} [3] \tilde{\cdot} X^2 \tilde{+} [2] \tilde{\cdot} X \in (\mathbb{Z}/4\mathbb{Z})[X]$

4. $(R, t, \cdot) = (\mathcal{P}(\{a, b\}), \Delta, \cap)$ $\quad \in \mathcal{P}(\{a, b\})[X]$

   $p = \{a, b\} \cap \underbrace{X^2}_{= X \cap X} \Delta \{a\} \cap \underbrace{X^1}_{= X} \Delta \emptyset \cap \underbrace{X^0}_{= \{a, b\}}$

# Addition von Polynomen

## Definition

Es sei $(R, +, \cdot)$ ein kommutativer Ring.

Die **Addition** der Polynome $p, q \in R[t]$

$$p = \sum_{i=0}^{n} a_i \cdot t^i \quad \text{und} \quad q = \sum_{j=0}^{m} b_j \cdot t^j$$

ist definiert als das Polynom

Koeffizienten addieren

$$p + q := \sum_{i=0}^{\max\{n,m\}} (a_i + b_i) \cdot t^i.$$

$p$ $q$ in $R$

Addition in $R[t]$ ist kommutativ.

# Addition von Polynomen

## Beispiel

Polynome in der Variable $X$ über dem Restklassenring $(\mathbb{Z}/4\mathbb{Z}, \tilde{+}, \tilde{\cdot})$:

$$p = [1] \tilde{\cdot} X^3 \quad \tilde{+} \quad [-3] \tilde{\cdot} X^2 \quad \tilde{+} \quad [2] \tilde{\cdot} X$$
$$q = [-1] \tilde{\cdot} X \quad \tilde{+} \quad [7]$$

$$p \tilde{+} q = [1] X^3 \tilde{+} [-3] X^2 \tilde{+} [2-1] X \tilde{+} [7]$$
$$= X^3 \tilde{+} X^2 \tilde{+} X \tilde{+} [3]$$

# Multiplikation von Polynomen

## Definition

Es sei $(R, +, \cdot)$ ein kommutativer Ring.

Die **Multiplikation** der Polynome $p, q \in R[t]$

$$p = \sum_{i=0}^{n} a_i \cdot t^i \quad \text{und} \quad q = \sum_{j=0}^{m} b_j \cdot t^j$$

ist definiert als das Polynom

ergibt sich durch Ausmultiplizieren und Sortieren nach Potenzen

$$p \cdot q := \sum_{k=0}^{n+m} c_k \cdot t^k \quad \text{mit} \quad c_k := \sum_{i=0}^{k} a_i \cdot b_{k-i}.$$

Multiplikation in $R[t]$ ist kommutativ.

# Multiplikation von Polynomen

## Beispiel

Polynome in der Variable $X$ über dem Restklassenring $(\mathbb{Z}/4\mathbb{Z}, \tilde{+}, \tilde{\cdot})$:

$$p = [1] \tilde{\cdot} X^3 \quad \tilde{+} \quad [-3] \tilde{\cdot} X^2 \quad \tilde{+} \quad [2] \tilde{\cdot} X$$

$$q = [-1] \tilde{\cdot} X \quad \tilde{+} \quad [7]$$

$$p \tilde{\cdot} q = ([-1]) X^4 \tilde{+} ([3] + [7]) X^3$$

$$\tilde{+} ([-2] + [-21]) X^2 \tilde{+} ([14]) X^1$$

$$= [3] X^4 \tilde{+} [2] X^3 + x^2 + [2] X$$

# Polynomring

## Definition

Es sei $(R, +, \cdot)$ ein kommutativer Ring.

Mit der Addition $+$ und Multiplikation $\cdot$ wird $(R[t], +, \cdot)$ zum **Polynomring in der Variablen $t$ über dem Koeffizientenring $R$.**

- $(R[t], +, \cdot)$ ist kommutativer Ring.
- Das Nullelement in $(R[t], +, \cdot)$ ist das Nullpolynom.
- Besitzt $(R, +, \cdot)$ das Einselement $1_R$, dann besitzt $(R[t], +, \cdot)$ das Einselement $1_R$ (Einspolynom).
- Der Koeffizientenring $(R, +, \cdot)$ ist der Unterring der konstanten Polynome in $(R[t], +, \cdot)$.

# Polynomring als Folgenring

Es sei $(R, +, \cdot)$ ein kommutativer Ring.

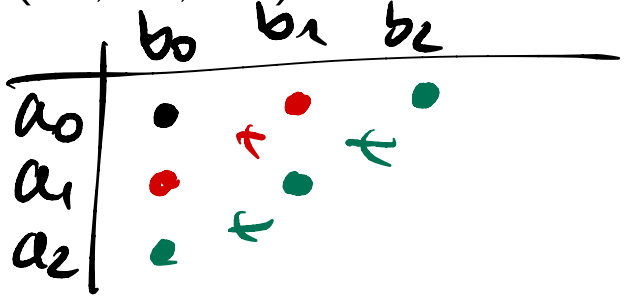
- Es besteht eine Bijektion

$$\begin{array}{ccc} p \in R[t] & \longleftrightarrow & (a_0, a_1, \ldots) \in (R^{\mathbb{N}_0})_{00} \\ \text{Polynom} & & \text{Koeffizientenfolge mit endlichem Träger} \end{array}$$

- Addition von Polynomen entspricht der gliedweisen Addition der Koeffizientenfolgen.

- Multiplikation von Polynomen entspricht der **Faltung** der Koeffizientenfolgen $(a_0, a_1, \ldots)$ und $(b_0, b_1, \ldots)$:

$$c_0 = a_0 \cdot b_0$$
$$c_1 = a_0 \cdot b_1 + a_1 \cdot b_0$$
$$c_2 = a_0 \cdot b_2 + a_1 \cdot b_1 + a_2 \cdot b_0$$



# Grad eines Polynoms

## Definition

Es sei $(R, +, \cdot)$ ein kommutativer Ring und $p = \sum_{j=0}^{n} a_j \cdot t^j$.

1. Der **Grad** von $p$ ist Welches ist der höchste Koeff. ungleich 0?

$$\deg(p) := \begin{cases} -\infty, & \text{falls alle } a_j = 0_R \text{ sind} \\ \max\{j \in \mathbb{N}_0 \mid a_j \neq 0_R\} & \text{sonst.} \end{cases}$$

2. Der **führende Koeffizient** von $p$ ist Was ist der Wert dieses Koeffizienten?

$$\ell(p) := \begin{cases} 0, & \text{falls alle } a_j = 0_R \text{ sind} \\ a_{\deg(p)} & \text{sonst.} \end{cases}$$

3. Hat $R$ das Einselement $1_R$ und gilt $\ell(p) = 1_R$, dann heißt das Polynom $p$ **normiert** oder **monisch**.

# Grad eines Polynoms

## Beispiel

Polynome in der Variable $X$ über dem Restklassenring $(\mathbb{Z}/4\mathbb{Z}, \tilde{+}, \tilde{\cdot})$:

$$p = [-2]\,X^3 \,\tilde{+}\, [-3]\,X^2 \,\tilde{+}\, [2]\,X \qquad \deg(p) = 3$$

$$q = [2]\,X \,\tilde{+}\, [7] \qquad \deg(q) = 1$$

Es gilt

$$p \,\tilde{+}\, q = [-2]\,X^3 \,\tilde{+}\, \cdots \qquad \deg(p \,\tilde{+}\, q) = 3$$

$$p \,\tilde{\cdot}\, q = [-4]\,X^4 \,\tilde{+}\, ([-14] \,\tilde{+}\, [-6])\,X^2 \,\tilde{+}\, ([-21] \,\tilde{+}\, [4])\,X^2 \,\tilde{+}\, \cdots \qquad \deg(p \,\tilde{\cdot}\, q) = 2$$

# Grad eines Polynoms

## Lemma

Es sei $R$ ein kommutativer Ring und $p, q \in R[t]$ zwei Polynome.

1. $\deg(p+q) \leqslant \max\{\deg(p), \deg(q)\}$.
2. $\deg(p \cdot q) \leqslant \deg(p) + \deg(q)$.
3. Ist $R$ nullteilerfrei, dann gilt sogar $\deg(p \cdot q) = \deg(p) + \deg(q)$.

Beweis. Übung

# Polynomdivision mit Rest

In einem Körper ist $\frac{p_1}{p_2} = p_1 \cdot p_2^{-1} \in K$ für $p_2 \neq 0$, d.h. $p_1 = (p_1 \cdot p_2^{-1}) p_2$

## Lemma

D.h. Jedes $p_2 \neq 0$ ist Teiler von jedem $p_1$.

Der Polynomring $R[t]$ ist niemals ein Körper.

## Definition

Es seien $K$ ein Körper und $p_1, p_2 \in K[t]$ zwei Polynome.

$p_2$ heißt ein **Teiler** von $p_1$ (kurz: $p_2 \mid p_1$), wenn es ein $q \in K[t]$ gibt, sodass gilt:

$$p_1 = q \cdot p_2.$$

## Satz

vgl. $13 = 3 \cdot 4 + 1$

Rest $b$

Es seien $K$ ein Körper und $p_1, p_2 \in K[t]$ zwei Polynome.

Ist $p_2 \neq 0_K$, dann gibt es eindeutig bestimmte Polynome $q, r \in K[t]$, sodass gilt:

$$p_1 = q \cdot p_2 + r \quad \text{und} \quad \deg(r) < \deg(p_2).$$

# Polynomdivision mit Rest

## Beispiel

Was ist $(3t^3 + 2t + 1) : (t^2 - 4t)$ in $\mathbb{R}[t]$?

$$(3t^3 + 2t + 1) = (3t + 12)(t^2 - 4t) + 50t + 1$$

$q$ $p_2$ $r$

$$\begin{array}{r} 3t^3 + 2t + 1 \\ -(3t^3 - 12t^2) \\ \hline 12t^2 + 2t + 1 \\ -(12t^2 - 48t) \\ \hline 50t + 1 \end{array}$$

# Polynomfunktion

## Definition

Es sei $R$ ein kommutativer Ring.

Zu jedem Polynom $p = \sum_{j=0}^{n} a_j \cdot t^j$ gehört eine **Polynomfunktion**

$r$ wird für $t$ eingesetzt!

$$\widetilde{p}\colon R \to R, \quad r \mapsto \widetilde{p}(r) := \sum_{j=0}^{n} a_j \, r^j.$$

Die Abbildung

Bild $\Phi$ = Untermenge der Polynomfunktionen

$$\Phi\colon \underbrace{(R[t], +, \cdot)}_{\text{Ring}} \ni p \quad \longmapsto \quad \widetilde{p} \in \underbrace{(R^R, +, \cdot)}_{\text{Ring}}$$

(Polynom / Polynomfunktion)

ist ein Ringhomomorphismus zwischen zwei kommutativen Ringen.

Wenn $R$ das Einselement $1_R$ hat, dann wird $1 \in R[t]$ durch $\Phi$ auf $1_R \in R^R$ (Einsfunktion) abgebildet.

# Polynomfunktion

## Beispiel

Polynome in der Variable $t$ über dem Ring von $\mathbb{Z}$ modulo 2 $(\mathbb{Z}_2, +_2, \cdot_2)$:

$$p = t^2 + t \qquad (0,1,1,0,\dots)$$

$$q = 0 \qquad (0,0,\dots)$$

$\tilde{p}(0) = 0 \cdot_2 0 +_2 0 = 0$ $\qquad$ $\tilde{q}(0) = 0$

$\tilde{p}(1) = 1 \cdot_2 1 +_2 1 = 0$ $\qquad$ $\tilde{q}(1) = 0$

Der Homomorphismus $\Phi : \mathbb{Z}_2[t] \to \mathbb{Z}_2^{\mathbb{Z}_2}$ ist also i.A. nicht injektiv!

# Nullstelle eines Polynoms

## Definition

Es sei $R$ ein kommutativer Ring, $p \in R[t]$ ein Polynom und $\widetilde{p}\colon R \to R$ die zugehörige Polynomfunktion.

$\lambda \in R$ heißt eine **Nullstelle** von $p$ in $R$, wenn $\widetilde{p}(\lambda) = 0_R$ gilt.

- Wieviele Nullstellen kann ein Polynom besitzen?
- Was sagen die Nullstellen über ein Polynom aus?

# Nullstelle eines Polynoms

## Beispiel

Aufgabe ist wesentlich

1. $p = t^2 + 1 \in \mathbb{R}[t]$ besitzt keine Nullstelle, weil für die Polynomfunktion $\widetilde{p}\colon \mathbb{R} \to \mathbb{R}$ gilt: $\widetilde{p}(t) = t^2 + 1 \geqslant 1$ für alle $t \in \mathbb{R}$.

$(-i)^2 = i^2 = -1$

2. $p = t^2 + 1 \in \mathbb{C}[t]$ besitzt genau die beiden Nullstellen $i$ und $-i$.

3. $p = t^2 + 1 \in \mathbb{Z}_5[t]$ besitzt genau die beiden Nullstellen 2 und 3:

$$\widetilde{p}(0) = 0 \cdot_5 0 +_5 1 = 1 \qquad \widetilde{p}(3) = 3 \cdot_5 3 +_5 1 = 0$$
$$\widetilde{p}(1) = 1 \cdot_5 1 +_5 1 = 2 \qquad \widetilde{p}(4) = 4 \cdot_5 4 +_5 1 = 2$$
$$\widetilde{p}(2) = 2 \cdot_5 2 +_5 1 = 0$$

Alle des Koeffizientenringe $\mathbb{R}, \mathbb{C}, \mathbb{Z}_5$ sind Körper.

# Nullstellen und Teiler

## Lemma

Es seien $K$ ein Körper und $p \in K[t]$ ein Polynom. Dann sind äquivalent:

1. $\lambda \in K$ ist eine Nullstelle von $p$. d.h. $\tilde{p}(\lambda) = 0_K$.
2. Das Polynom $t - \lambda \in K[t]$ ist ein Teiler von $p$. $= 1 \cdot t^1 - \lambda \cdot t^0$ $\deg(t-\lambda) = 1$

In diesem Fall gilt für das eindeutige $q \in K[t]$ mit $p = q \cdot (t - \lambda)$ die Beziehung $\deg(q) = \deg(p) - 1$.

Nachtrag nach der Vorlesung

Beweis. (1) $\Rightarrow$ (2) Wir führen Polynomdivision mit Rest (Folie 24) durch: $p = q \cdot \underbrace{(t-\lambda)}_{\text{nicht das Nullpolynom}} + r$ mit $\deg(r) < \deg(t-\lambda) = 1$,

also ist $r$ konstantes Polynom. Um $r$ zu bestimmen, müssen wir die Polynomfkt. $\tilde{r}$ nur an einer Stelle kennen: $\tilde{r}(\lambda) = \tilde{p}(\lambda) - \tilde{q}(\lambda) \cdot (\lambda - \lambda) = \tilde{p}(\lambda) = 0_K \Rightarrow r = 0$.

$\uparrow$ $\Phi$ ist Ringhomomorphismus

# Nullstellen und Teiler

## Lemma

Es seien $K$ ein Körper und $p \in K[t]$ ein Polynom. Dann sind äquivalent:

1. $\lambda \in K$ ist eine Nullstelle von $p$.
2. Das Polynom $t - \lambda \in K[t]$ ist ein Teiler von $p$.

In diesem Fall gilt für das eindeutige $q \in K[t]$ mit $p = q \cdot (t - \lambda)$ die Beziehung $\deg(q) = \deg(p) - 1$.

Nachtrag nach der Vorlesung

Beweis. ② ⇒ ①: Nach Voraussetzung: $t-\lambda \mid p$, also existiert $q \in K[t]$ mit $p = q \cdot (t-\lambda)$.

$\Rightarrow \tilde{p}(\lambda) = \tilde{q}(\lambda) \cdot (\lambda - \lambda) = 0$, also ist $\lambda$ eine Nullstelle von $p$.

↑ $\tilde{\cdot}$ ist Ringhomomorphismus

Folie 23: $\deg(p) = \deg(q \cdot (t-\lambda)) = \deg(q) + 1$.

↑ $K$ ist als Körper nullteilerfrei

# Zerlegung eines Polynoms

## Satz

Es seien $K$ ein Körper und $p \in K[t]$ ein Polynom, $p \neq 0_K$.

1. Es existieren $s \in \mathbb{N}_0$, paarweise verschiedene Zahlen $\lambda_1, \ldots, \lambda_s \in K$ sowie Exponenten $n_1, \ldots, n_s \in \mathbb{N}$ und $q \in K[t]$ ohne Nullstelle in $K$, sodass gilt:

$$p = \underbrace{(t-\lambda_1)^{n_1} \cdot \ldots \cdot (t-\lambda_s)^{n_s}}_{\text{Linearfaktoren}} \cdot q.$$

Die Darst. ist i.W. eindeutig.

$\deg(q) = \deg(p) - n_1 - \ldots - n_s$

2. Die Nullstellen von $p$ sind genau die Zahlen $\lambda_1, \ldots, \lambda_s \in K$.

## Beispiel

$$2t^5 - 5t^3 - 4t^2 - 3t - 2 = (t-2)^1 (t+1)^2 \underbrace{(2t^2+1)}_{q} \quad \text{in } \mathbb{R}[t]$$

2 ist einfache Nullstelle

$-1$ ist doppelte "

# Zerlegung eines Polynoms

## Folgerung

Es seien $K$ ein Körper und $p \in K[t]$ ein Polynom, $p \neq 0_K$.

1. $p$ hat höchstens $\deg(p) \in \mathbb{N}_0$ viele verschiedene Nullstellen:

$$s \leqslant \deg(p)$$

2. $p$ hat höchstens $\deg(p) \in \mathbb{N}_0$ viele Nullstellen, entsprechend ihrer Vielfachheit gezählt:

$$\sum_{i=1}^{s} n_i \leqslant \deg(p)$$

# Polynome über unendlichen Körpern

## Folgerung

Es sei $K$ ein unendlicher Körper.

Dann ist die Abbildung $\Phi\colon R[t] \to R^R$ injektiv.

Nachtrag nach der Vorlesung

**Beweis.** Es seien $p_1, p_2 \in K[t]$ mit $\tilde{p_1} = \tilde{p_2}$.
Zu zeigen ist $p_1 = p_2$. Setze $q := p_1 - p_2$.
Dann ist $\tilde{q} = \Phi(q) = \Phi(p_1 - p_2) = \tilde{p_1} - \tilde{p_2} = 0_K$.
($0_K$: Nullfkt.; $\Phi$ ist Ringhomomorphismus)
Also hat $q$ unendlich viele Nullstellen, nämlich alle Elemente von $K$. Nach Folie 33 muss also $q = 0_K$ sein, d.h. $p_1 = p_2$.

# Fundamentalsatz der Algebra

## Satz

Jedes Polynom $p \in \mathbb{C}[t]$ mit $\deg(p) > 0$ hat mindestens eine Nullstelle.

## Folgerung

Jedes nicht-konstante Polynom $p \in \mathbb{C}[t]$ zerfällt vollständig in Linearfaktoren:

$$p = (t - \lambda_1)^{n_1} \cdot \ldots \cdot (t - \lambda_s)^{n_s} \cdot q$$

$q \in \mathbb{C} \setminus \{0\}$