Lineare Algebra I

Woche 07

28.11.2023 und 30.11.2023

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.
2. $(K \setminus \{0_K\}, \cdot)$ ist eine abelsche Gruppe mit Einselement 1_K.
3. Es gelten die **Distributivgesetze**

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$
$$(a + b) \cdot c = (a \cdot c) + (b \cdot c)$$

Beispiel

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

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

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

Funktionen mit Werten in einem Körper

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 $(K^X, +, \cdot)$

Eigenschaften eines Körpers

Lemma

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

1. $0_K \neq 1_K$.

2. $(K, +, \cdot)$ ist ein kommutativer, nullteilerfreier Ring mit dem Einselement 1_K ungleich dem Nullring, also ein Integritätsring.

3. Es gelten die **Kürzungsregeln**

$$\begin{aligned} a \star b_1 = a \star b_2 \quad &\Rightarrow \quad b_1 = b_2 \\ b_1 \star a = b_2 \star a \quad &\Rightarrow \quad b_1 = b_2 \end{aligned}$$

   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 $\operatorname{char}(K) = 0$.

Beispiel

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

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.

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.

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 $(\mathbb{Z} / m\mathbb{Z}, \tilde{+}, \tilde{\cdot})$
- 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.

Unterkörper

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

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

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

Körperhomomorphismen sind injektiv

Lemma

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

Dann ist f injektiv.

Beweis.

Polynom

Definition

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

1. Ein **Polynom** über R in der Variablen t ist ein formaler Ausdruck der Gestalt ($n \in \mathbb{N}_0$)
$$a_n \cdot t^n + a_{n-1} \cdot t^{n-1} + \cdots + a_1 \cdot t + a_0 \quad \text{oder} \quad \sum_{i=0}^{n} a_i \cdot t^i.$$
2. Die Menge aller Polynome in der Variablen t über R ist $R[t]$.
3. Ein **konstantes Polynom**
4. Das **Nullpolynom**
5. Ein **Monom**
6. Das **Einspolynom**

Polynom

Beispiel

1.
2.
3.
4.

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

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

Addition von Polynomen

Beispiel

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

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

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

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

Multiplikation von Polynomen

Beispiel

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

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

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
- Das Nullelement in $(R[t], +, \cdot)$ ist
- Besitzt $(R, +, \cdot)$ das Einselement 1_R, dann besitzt $(R[t], +, \cdot)$
- Der Koeffizientenring $(R, +, \cdot)$ ist der

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
$$\deg(p) := \begin{cases} -\infty, & \text{falls alle } a_j = 0_R \text{ sind} \\ \max\{j \in \mathbb{N}_0 \mid a_j \neq 0_R\} & \text{sonst.} \end{cases}$$
2. Der **führende Koeffizient** von p ist
$$\ell(p) := \begin{cases} 0, & \text{falls alle } a_j = 0_R \text{ sind} \\ a_{\deg(p)} & \text{sonst.} \end{cases}$$
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 $(\mathbb{Z} / 4\,\mathbb{Z}, \tilde{+}, \tilde{\cdot})$:

$$\begin{aligned} p &= [-2]\,X^3 \tilde{+} [-3]\,X^2 \tilde{+} [2]\,X \\ q &= [2]\,X \tilde{+} [7] \end{aligned}$$

Es gilt

$$p \tilde{+} q =$$

$$p \tilde{\cdot} q =$$

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

Lemma

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

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 $\mathbb{R}[t]$?

Polynomfunktion

Definition

Es sei R ein kommutativer Ring.

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

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

Die Abbildung

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

ist ein Ringhomomorphismus zwischen zwei kommutativen Ringen.

Polynomfunktion

Beispiel

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

$$p = t^2 + t$$
$$q = 0$$

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

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 $t \in \mathbb{R}$.

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:

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

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 $\deg(q) = \deg(p) - 1$.

Beweis.

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 $\deg(q) = \deg(p) - 1$.

Beweis.

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 $\lambda_1, \dots, \lambda_s \in K$ sowie Exponenten $n_1, \dots, n_s \in \mathbb{N}$ und $q \in K[t]$ ohne Nullstelle in K, sodass gilt:

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

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

Beispiel

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

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.

Beweis.

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:

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