Übersicht
Vorlesungswoche 1

Ulrich Görtz

Lineare Algebra 2, SS 21

Essen Seminar for Algebraic Geometry and Arithmetic

UNIVERSITÄT DUISBURG ESSEN

Ausgangssituation

K Körper, V ein (endlichdimensionaler) K-Vektorraum.

$f\colon V \to V$ ein Endomorphismus ($\leftrightsquigarrow$ A darstellende Matrix)

Eigenwerte, Eigenräume, Diagonalisierbarkeit.

Ziele für dieses Semester

- genauer verstehen: Wann ist $f \in \mathrm{End}_K(V)$ diagonalisierbar?

  Welche Arten von "Normalformen" für $M_{\mathcal{B}}^{\mathcal{B}}(f)$ existieren sonst?

  ... charakteristisches Polynom, Minimalpolynom von f ...

  ... Jordansche Normalform.

  Vorbereitung: "Polynomring"

- Quotientenvektorraum $U \subseteq V$ UVR $\rightsquigarrow$ konstruiere VR V/U

  + surj. VR-Homom $\pi : V \to V/U$ mit $\mathrm{Ker}(\pi) = U$.

- Euklidische, unitäre Vektorräume $/\mathbb{C}$

  $\mathbb{R}$-VR mit "Skalarprodukt" $\rightsquigarrow$ Abstände, Länge eines Vektors, Winkel

Ringe

Ring $\left[\begin{array}{lll} R, & + : R \times R \to R, & \text{s.d. } (R,+) \text{ komm. Gruppe} \\ & \cdot : R \times R \to R, & \text{assoziativ, neutr. Elem. } 1 \in R, \\ & & \text{Distributivgesetz.} \end{array} \right.$

Der Polynomring

K Körper

$\rightsquigarrow$ Polynomring $K[X] = \left\{ \sum_{i=0}^{n} a_i X^i \; ; \; n \in \mathbb{N}, \quad a_i \in K \right\}$

$\ni$

Polynom $\rightarrow$ $f = \sum_{i=0}^{n} a_i X^i$

$x \in K$

$\rightsquigarrow$ $f(x) = \sum_{i=0}^{n} a_i x^i \in K$

$\rightsquigarrow$ $K \longrightarrow K$, $x \longmapsto f(x)$ Polynomfunktion zu f.

Ringe - Definition und Beispiele
Vorlesungswoche 1

Ulrich Görtz

Lineare Algebra 2, SS 21

Essen Seminar for Algebraic Geometry and Arithmetic

UNIVERSITÄT DUISBURG ESSEN

Definition: Ring

Definition (1) Ein <u>Ring</u> ist eine Menge R zusammen mit zwei Verknüpfungen

$$+ : R \times R \to R \quad \text{(Addition)}, \qquad \cdot : R \times R \to R \quad \text{(Multiplikation)}$$

so dass (a) $(R, +)$ ist eine kommutative Gruppe (mit neutr. Elem 0)

(b) die Multiplikation ist assoziativ: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.

(c) es gelten die Distributivgesetze: $a(b+c) = ab + ac$

$(a+b)c = ac + bc$

für alle $a, b, c \in R$.

In dieser Vorlesung heißt <u>Ring</u> immer: Ring mit Eins.

(2) Wenn die Multiplikation auf R ein neutrales Elem. hat, dann heißt R ein Ring mit Eins.

(3) Wenn die Multiplikation von R kommutativ ist, dann nennt man R einen kommutativen Ring.

Bemerkungen: R sei ein Ring, $a \in R$

- Addition: 0 neutrales Elem., $-a$ Inverses von a, $a - b := a + (-b)$
- Multiplikation: 1 neutrales Element, falls mult. Inverses von a ex.: a^{-1}
- Punkt- vor Strichrechnung

Einheiten

Sei R ein Ring.

Def Ein Element $a \in R$ heißt Einheit, wenn $b \in R$ existiert mit

$$ab = 1 = ba.$$

Die Menge $R^\times$ aller Einheiten von R bildet eine Gruppe bezüglich der Multiplikation von R, die sogenannte Einheitengruppe oder multiplikative Gruppe von R.

Quiz

Finden Sie möglichst viele Beispiele von Ringen, die Sie in der LA1 kennengelernt haben!

Quiz

Finden Sie möglichst viele Beispiele von Ringen, die Sie in der LA1 kennengelernt haben!

- $\mathbb{Z}$ ganze Zahlen mit üblicher Add., Mult. ist komm. Ring, $\mathbb{Z}^\times = \{1, -1\}$
- $\mathbb{Z}/n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$ Rechnen "modulo n" ist komm. Ring

  $(\mathbb{Z}/n)^\times = \{\bar{m} \; ; \; m, n \text{ teilerfremd}\}$
- Jeder Körper K ist ein komm. Ring, $K^\times = K \setminus \{0\}$.
- K Kp., $n \in \mathbb{N}$. Dann ist $M_n(K)$ mit Add. und Produkt von Matrizen ein Ring (falls $n \geq 2$: nicht kommutativ), $M_n(K)^\times = GL_n(K)$
- K Kp., V ein K-VR. Dann ist $\mathrm{End}_K(V)$ mit Addition und Verkettung von Abb. als Multiplikation ein Ring, $\mathrm{End}_K(V)^\times = \mathrm{Aut}_K(V)$.

- der Nullring $\{0\}$

- Produkt von Ringen: R_1, R_2 Ringe $\longrightarrow$ $R_1 \times R_2$ ist Ring mit komponentenweise Add., Mult.

$$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2)$$
$$(x_1, x_2) \cdot (y_1, y_2) = (x_1 y_1, x_2 y_2).$$

Analog: $R_1 \times \ldots \times R_n$, $\prod_{i \in I} R_i$.

- X Menge, R Ring. Dann ist $\mathrm{Abb}(X, R)$ mit Add. / Mult. von Abbildungen ein Ring:

$$(f+g)(x) = f(x) + g(x), \quad (f \cdot g)(x) = f(x) \cdot g(x),$$
$$f, g \in \mathrm{Abb}(X, R), \quad x \in X.$$

$$\left(\mathrm{Abb}(X, R) = R^X = \prod_{x \in X} R. \right)$$

Quiz

Welche der folgenden Mengen sind mit den beiden angegebenen Verknüpfungen als Addition und Multiplikation ein Ring?

$\mathbb{Q}$ mit Addition $+$ und Multiplikation $+$

$\mathrm{Hom}(V, K)$ mit Addition $+$ und Multiplikation $\cdot$
(Addition/Multiplikation von Abbildungen, K Körper, V endlichdim. K-Vektorraum)

$\{f\colon K \to K;\ f \text{ Polynomfunktion}\}$
mit Addition $+$ und Multiplikation $\cdot$ (Addition/Multiplikation von Abbildungen)

Quiz

Welche der folgenden Mengen sind mit den beiden angegebenen Verknüpfungen als Addition und Multiplikation ein Ring?

- $\mathbb{Q}$ mit Addition $+$ und Multiplikation $+$ Distributivgesetz nicht erfüllt
- $\mathrm{Hom}(V, K)$ mit Addition $+$ und Multiplikation $\cdot$ Produkt linearer Abb. ist im allg. nicht linear $\rightsquigarrow$ keine Verknüpfung
  (Addition/Multiplikation von Abbildungen, K Körper, V endlichdim. K-Vektorraum)
- $\{f\colon K \to K;\ f \text{ Polynomfunktion}\}$ $f(x) = \sum_{i=0}^{n} a_i x^i, \quad a_i \in K.$
  mit Addition $+$ und Multiplikation $\cdot$ (Addition/Multiplikation von Abbildungen)

Rechenregeln

R Ring

- $0 \cdot a = 0 = a \cdot 0$ für alle $a \in R$ $\quad (0 \cdot a = (0+0) \cdot a = \dots)$
- $(-1) \cdot a = -a = a \cdot (-1)$

im allg. <u>nicht</u> $\quad \left.\begin{array}{l} ab = ac \\ a \neq 0 \end{array}\right\} \Rightarrow b = c$

$ab = 0 \Rightarrow a = 0$ oder $b = 0$

Ringhomomorphismen
Vorlesungswoche 1

Ulrich Görtz

Lineare Algebra 2, SS 21

Essen Seminar for Algebraic Geometry and Arithmetic

UNIVERSITÄT DUISBURG ESSEN

Definition: Ringhomomorphismus

Def. Seien R, S Ringe. Eine Abbildung $f: R \to S$ heißt Ringhomomorphismus, wenn für alle $x, y \in R$:

(a) $f(x+y) = f(x) + f(y)$ (f Gruppenhom. bzgl $+$)

(b) $f(xy) = f(x)\, f(y)$

(c) $f(1) = 1$.

Konsequenzen: Sei $f: R \to S$ ein Ringhomomorphismus.

- f Gruppenhomomorphismus (bezüglich $+$)

  also $f(0) = 0$, $f(-x) = -f(x)$

- f induziert Gruppenhomomorphismus $R^\times \to S^\times$

  $(ab = ba = 1 \Rightarrow f(a)f(b) = f(ab) = f(1) = 1, \quad f(b)f(a) = 1$

  $\Rightarrow f(a) \in S^\times)$

<u>Bemerkung</u>

- Die Verkettung von Ringhomom. ist wieder ein Ringhomomorphismus.

- Die identische Abbildung $id_R : R \to R$ ist ein Ringhomomorphismus.

Quiz

Finden Sie Beispiele von Ringhomomorphismen, die Sie in der LA1 kennengelernt haben!

Quiz

Finden Sie Beispiele von Ringhomomorphismen, die Sie in der LA1 kennengelernt haben!

- $n \in \mathbb{N}_{>1}$, $\mathbb{Z}/n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$

  Die "kanonische Projektion" $\boxed{\mathbb{Z} \to \mathbb{Z}/n}$, $x \mapsto \bar{x}$ ← Rest von x bei Division durch n

  ist ein surjektiver Ringhomomorphismus.

- K Körper, V endlichdim'l K-VR mit Basis $\mathcal{B}$

  $\rightsquigarrow$ $\mathrm{End}_K(V) \to M_n(K)$, $f \mapsto M_{\mathcal{B}}^{\mathcal{B}}(f)$,

  ist Ringhomomorphismus, sogar bijektiv

Isomorphismen

Def. Ein Ringhomom. $f: R \to S$ heißt <u>Isomorphismus</u>, wenn ein Ringhomom. $g: S \to R$ ex., so dass $g \circ f = id_R$, $f \circ g = id_S$ gilt.

<u>Lemma</u> Sei f ein Ringhomom. Dann gilt:

$$f \text{ Isomorphismus} \iff f \text{ bijektiv.}$$

Quiz

Welche der Abbildungen sind Ringhomomorphismen/-isomorphismen? (K ein Körper)

$$\mathbb{C} \to \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} ;\ a, b \in \mathbb{R} \right\}, \quad a + ib \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

$\det\colon M_n(K) \to K \quad$ (für $n > 1$)

$M_n(K) \to M_n(K),\ A \mapsto A^t.$

$M_n(K) \to M_n(K),\ A \mapsto SAS^{-1} \quad$ (für eine fixierte Matrix $S \in GL_n(K)$)

$K \to M_n(K),\ a \mapsto aE_n$

Quiz

Welche der Abbildungen sind Ringhomomorphismen/-isomorphismen? (K ein Körper)

- $\mathbb{C} \to \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} ;\ a, b \in \mathbb{R} \right\}, \quad a + ib \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$

Isomorphismus

$(a+ib)(c+id) = (ac-bd) + i(ad+bc)$.

$\begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} c & -d \\ d & c \end{pmatrix} = \begin{pmatrix} ac-bd & -ad-bc \\ bc+ad & -bd+ac \end{pmatrix}$

- $\det\colon M_n(K) \to K \quad$ (für $n > 1$)
- $M_n(K) \to M_n(K),\ A \mapsto A^t$.
- $M_n(K) \to M_n(K),\ A \mapsto SAS^{-1} \quad$ (für eine fixierte Matrix $S \in GL_n(K)$)
- $K \to M_n(K),\ a \mapsto aE_n$

Quiz

Welche der Abbildungen sind Ringhomomorphismen/-isomorphismen? (K ein Körper)

$$\mathbb{C} \to \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} ;\ a, b \in \mathbb{R} \right\}, \quad a + ib \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix}$$

$\det\colon M_n(K) \to K \quad (\text{für } n > 1)$ — kein Ringhomomorphismus (im allg.: $\det(A+B) \neq \det(A) + \det(B)$)

$M_n(K) \to M_n(K),\ A \mapsto A^t.$ — kein Ringhomom.: im allg. $(AB)^t \neq A^t B^t$ $= B^t A^t$

$M_n(K) \to M_n(K),\ A \mapsto SAS^{-1} \quad (\text{für eine fixierte Matrix } S \in GL_n(K))$ — Ringisomorphismus (Umkehrabb.: $A \mapsto S^{-1}AS$)

$K \to M_n(K),\ a \mapsto aE_n$ — Ringhomomorphismus, für $n \geq 2$ kein Isomorphismus

Unterringe

Def. Sei S ein Ring. Eine Teilmenge $R \subseteq S$ heißt <u>Unterring</u>, wenn

(a) $R \subseteq S$ eine Untergruppe ist bzgl. $+$

(b) für alle $x, y \in R$ gilt $xy \in R$

(c) $1 \in R$.

Bsp.

- $\mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$
- $\{a \cdot E_n \,;\, a \in K\} \subseteq M_n(K)$ (K Körper).

Kern und Bild eines Ringhomomorphismus

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

Wir definieren

$$\ker(f) = \{ x \in R ; \quad f(x) = 0 \} \subseteq R \qquad \underline{\text{Kern}} \text{ von } f$$

$$\operatorname{Im}(f) = \{ y \in S ; \quad \text{es gibt } x \in R \text{ mit } f(x) = y \} \subseteq S \qquad \underline{\text{Bild}} \text{ von } f.$$

<u>Bem.</u> $\operatorname{Im}(f) \subseteq S$ ist ein Unterring.

Ideale

Def. Sei R ein Ring. Eine Teilmenge $\mathfrak{a} \subseteq R$ heißt <u>Ideal</u>,

wenn (1) $\mathfrak{a} \subseteq R$ Untergruppe bzgl. $+$

(2) für alle $a \in \mathfrak{a}$, $x \in R$: $xa \in \mathfrak{a}$, $ax \in \mathfrak{a}$

<u>Schreibweise</u> $\mathfrak{a}$ $\mathfrak{b}$ $\mathfrak{c}$ $\mathfrak{m}$ $\mathfrak{n}$ $\mathfrak{p}$ $\mathfrak{q}$

a b c m n p q

<u>Beispiele</u>

- $\{0\}$ Nullideal, R "Einsideal"
- Ist $\mathfrak{a} \subseteq R$ ein Ideal, das eine Einheit von R enthält $(x \in R^\times,\ x \in \mathfrak{a})$ $\Rightarrow$ $1 = x^{-1}x \in \mathfrak{a}$ $\Rightarrow$ $\mathfrak{a} = R$

- Insbes.: Ist K ein Körper, so sind $\{0\}$ und K die einzigen Ideale.

- Ist $f: R \to S$ ein Ringhomomorphismus, so ist $\operatorname{Ker}(f) \subseteq R$ ein Ideal

  - Untergruppe ✓
  - $a \in \operatorname{Ker}(f)$, $x \in R$ $\Rightarrow$ $f(xa) = f(x) \underbrace{f(a)}_{=0} = 0 \Rightarrow xa \in \operatorname{Ker} f$

    analog: $ax \in \operatorname{Ker} f$.

Das von einer Teilmenge erzeugte Ideal

Der Durchschnitt von Idealen ist Ideal.

<u>Def.</u> Sei R ein Ring, $M \subseteq R$ eine Teilmenge. Dann ist

$$(M) := \bigcap_{\substack{\mathfrak{a} \subseteq R \text{ Ideal} \\ M \subseteq \mathfrak{a}}} \mathfrak{a} \subseteq R$$

das kleinste Ideal, das M enthält.

Wir nennen (M) das <u>von M erzeugte Ideal</u>.

Schreibweise: $(x_1, \ldots, x_n)$ statt $(\underbrace{\{x_1, \ldots, x_n\}}_{M})$,

z.B. R kommutativ

$$(x) = \{ yx \,;\, y \in R \}$$

Quiz

Berechnen Sie $(4, 14) \subseteq \mathbb{Z}$.

Seien K ein Körper und $n \in \mathbb{N}_{>1}$. Ist $\{A \in M_n(K);\ \mathrm{rg}(A) \leq 1\}$ ein Ideal in $M_n(K)$?

Zeigen Sie: Ein kommutativer Ring R ist genau dann ein Körper, wenn $\{0\}$ und R die einzigen Ideale von R sind.

Quiz

Berechnen Sie $(4, 14) \subseteq \mathbb{Z}$.

Beh. $(4, 14) = (2) = \{2x;\ x \in \mathbb{Z}\}$ ← alle geraden ganzen Zahlen

Begr. "$\supseteq$" $2 = 14 - 3 \cdot 4 \in (4, 14)$

"$\subseteq$" (2) ist ein Ideal und $\{4, 14\} \subseteq (2)$, also $(4, 14) \subseteq (2)$.

Seien K ein Körper und $n \in \mathbb{N}_{>1}$. Ist $\{A \in M_n(K);\ \mathrm{rg}(A) \leq 1\}$ ein Ideal in $M_n(K)$?

Nein, zum Beispiel $\mathrm{rg}\Big(\underbrace{\mathrm{diag}(1, 0, \ldots, 0)}_{\mathrm{rg}=1} + \underbrace{\mathrm{diag}(0, \ldots, 0, 1)}_{\mathrm{rg}=1}\Big) = 2$

Zeigen Sie: Ein kommutativer Ring R ist genau dann ein Körper, wenn $\{0\}$ und R die einzigen Ideale von R sind.

- K Körper, $\mathfrak{a} \subseteq K$ Ideal, $\mathfrak{a} \neq 0$

  $\Rightarrow$ es ex. $a \in \mathfrak{a} \setminus \{0\}$, also $1 = a^{-1} a \in \mathfrak{a}$, also $\mathfrak{a} = K$.

- zz: $R^\times = R \setminus \{0\}$. Sei $x \in R \setminus \{0\}$ $\Rightarrow$ $\underset{\{yx;\ y \in R\}}{\underset{\parallel}{(x)}} = R \ni 1$ $\Rightarrow$ es ex. $y \in R$: $yx = 1$.

Der Polynomring
Vorlesungswoche 1

Ulrich Görtz

Lineare Algebra 2, SS 21

Essen Seminar for Algebraic Geometry and Arithmetic

UNIVERSITÄT DUISBURG ESSEN

Erinnerung: Polynomfunktionen

K Körper (oder ein kommutativer Ring)

Eine Polynomfunktion ist eine Abbildung $K \to K$

der Form $x \mapsto \sum_{i=0}^{n} a_i x^i$, $n \in \mathbb{N}$, $a_i \in K$

$\rightsquigarrow$ Ring $\mathrm{Pol}(K)$ der Polynomfunktionen

Allerdings: Wenn K ein endlicher Körper ist, dann hat der Ring $\mathrm{Pol}(K)$ "nicht so gute Eigenschaften". (Es ex. $f, g \neq 0$ mit $f \cdot g = 0$.)

Definition des Polynomrings

Sei R ein kommutativer Ring.

Ziel $\quad R[X] = \left\{ \overbrace{\sum_{i=0}^{n} a_i X^i}^{\text{"formaler Ausdruck"}} \; ; \; \begin{array}{l} n \in \mathbb{N} \\ a_i \in R \end{array} \right\}$

Polynomring über R in X

"Unbestimmte"

$$\sum_{i=0}^{n} a_i X^i = \sum_{i=0}^{n} b_i X^i \iff \forall i = 0, \dots, n : a_i = b_i.$$

Def. Sei R ein kommutativer Ring.

Wir definieren $R[X] := \left\{ (a_0, a_1, a_2, \dots) = (a_i)_{i \in \mathbb{N}} \; ; \; \begin{array}{l} a_i \in R \\ \text{höchstens endlich} \\ \text{viele } a_i \text{ sind} \\ \neq 0 \end{array} \right\}$

mit Addition $(a_i)_i + (b_i)_i = (a_i + b_i)_i$

$\cap$

$R[X]$

$$\text{"} \sum a_i X^i + \sum b_i X^i = \sum (a_i + b_i) X^i \text{"}$$

und Multiplikation

$$(a_i)_i \cdot (b_i)_i = \left(\sum_{\substack{j,k \geq 0 \\ j+k=i}} a_j b_k \right)_i \in R[X]$$

$$X^i \cdot X^j = X^{i+j}$$

+ Distributivgesetz

$$\rightsquigarrow \left(\sum a_i X^i\right)\left(\sum b_i X^i\right) = \sum_i \left(\sum_{j+k=i} a_j b_k \right) X^i$$

Dies definiert einen kommutativen Ring $R[X]$, den wir den Polynomring über R (in der Unbestimmten X) nennen.

Nullelement $0 = (0,0,0,\dots)$

Einselement $1 = (1,0,0,\dots)$

Wir definieren dann $X = (0,1,0,0,\dots) \in R[X]$

$$\boxed{(a_i)_i \mathrel{\hat{=}} \sum_i a_i X^i}$$

Dann rechnet man nach: $(a_i)_i = \sum_{i \geq 0} a_i X^i \in R[X]$

Zwischenschritt: $X^i = (0,\dots,0,\underset{i}{1},0,\dots)$

$$R[X] = \left\{ \sum_{i=0}^{n} a_i X^i \; ; \; n \in \mathbb{N}, \; a_i \in R \right\}$$ "R adjungiert X".

$$\rightsquigarrow \quad R \longrightarrow R[X], \quad a \longmapsto (a, 0, 0 \ldots) = a \cdot \underbrace{X^0}_{1}$$

injektiver Ringhomomorphismus

Elemente von $R[X]$ nennen wir <u>Polynome</u>.

Polynome der Form a, $a \in R$, heißen konstante Polynome.

Varianten

- andere Name für Unbestimmte: $R[Y]$, $R[T]$, ...

$$= \left\{ \sum_{i=0}^{n} a_i Y^i \right\}$$

- mehr als eine Unbestimmte

$$R[X, Y] = \left\{ \sum_{i,j \geq 0} a_{ij} X^i Y^j \; ; \; a_{ij} \in R, \text{ nur endl. viele } a_{ij} \text{ sind } \neq 0 \right\}$$

$R[X_1, \ldots, X_n]$, $R[X_i, i \in I]$ (in jedem einzelnen Polynom treten nur endlich viele Unbestimmte auf)

Der Einsetzungshomomorphismus
Vorlesungswoche 1

Ulrich Görtz

Lineare Algebra 2, SS 21

Essen Seminar for Algebraic Geometry and Arithmetic

UNIVERSITÄT DUISBURG ESSEN

Der Einsetzungshomomorphismus

R kommutativer Ring

Können in Polynom $f = \sum_{i=0}^{n} a_i X^i$ Elemente von R einsetzen:

$$x \in R \rightsquigarrow f(x) := \sum_{i=0}^{n} a_i x^i \in R$$

Dabei

- erhalte Homomorphismus ($R[X] \longrightarrow R$, für festes $x \in R$)

$$(f+g)(x) = f(x) + g(x)$$
$$(f \cdot g)(x) = f(x)\, g(x)$$
$$f = 1 \Rightarrow f(x) = 1.$$

- können "manchmal" auch Elemente anderer Ringe einsetzen:

zB: $f = X^2 + 3 \in \mathbb{Z}[X]$, können auch Elem. von $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$.

Satz / Def. Sei R ein kommutativer Ring, $\varphi : R \to S$ ein Ringhomom., $x \in S$.

Dann existiert ein eindeutig bestimmter Ringhomom.

$$\Phi : R[X] \longrightarrow S \quad \text{so dass} \quad \begin{aligned} \Phi(a) &= \varphi(a) \quad \text{für alle } a \in R \\ \Phi(X) &= x, \end{aligned}$$

nämlich
$$\Phi\left(\sum_{i=0}^{n} a_i X^i\right) = \sum_{i=0}^{n} \varphi(a_i)\, x^i. \qquad (*)$$

Dieser Ringhomom. heißt der Einsetzungshomomorphismus, und wir schreiben $f(x) = \Phi(f)$ für $f \in R[X]$.

Beweis Definiere die Abb. Φ durch $(*)$. zz: Dies ist ein Ringhomom.

- $\Phi(1) = 1$ ✓
- $\Phi(f+g) = \Phi(f) + \Phi(g)$ (einfach)

- $\phi(f \cdot g) = \phi(f) \cdot \phi(g)$. Schreibe $f = \sum a_i X^i$, $g = \sum b_i X^i$

Dann $\phi(f \cdot g) = \phi\left(\left(\sum a_i X^i\right)\left(\sum b_i X^i\right)\right) = \phi\left(\sum_i \left(\sum_{j+k=i} a_j b_k\right) X^i\right)$

$$= \sum_i \varphi\left(\sum_{j+k=i} a_j b_k\right) x^i$$

$$= \sum_i \left(\sum_{j+k=i} \varphi(a_j)\, \varphi(b_k)\right) x^i = \left(\sum_i \varphi(a_i) x^i\right)\left(\sum_i b_i x^i\right)$$

φ Ringhomom

$$= \phi(f) \cdot \phi(g).$$

<u>Bem.</u> In den meisten Fällen ist "klar", was die Abb. φ ist, zum Beispiel

- $R = S$, $\varphi = \mathrm{id}_R$
- $R \subseteq S$ Unterring, $\varphi : R \to S$ Inklusion
- K ein Körper, $R = K$, $S = M_n(K)$, $R \to S$, $a \mapsto a E_n$.

$$\begin{tikzcd}
a \arrow[d, mapsto] & R \arrow[r, "\varphi"] \arrow[d] & S \ni x \\
a & R[X] \arrow[ur, dashed, "\phi"] & X \arrow[u, mapsto, "x"']
\end{tikzcd}$$

Quiz

Sei $\mathbb{Z} \to \mathbb{F}_7$ die kanonische Projektion und $f(X) = X^2 - 3 \in \mathbb{Z}[X]$. Berechnen Sie $f(\bar{4}) \in \mathbb{F}_7$.

Sei $\mathbb{R} \to M_2(\mathbb{R})$ der Ringhomomorphismus mit $a \mapsto aE_2$. Berechnen Sie $f(A) \in M_2(\mathbb{R})$ für $f = X^2 + 2X - 3$ und $A = \begin{pmatrix} -1 & 2 \\ 2 & -1 \end{pmatrix}$.

Quiz

Sei $\overset{\pi}{\boxed{\mathbb{Z} \to \mathbb{F}_7}}$ die kanonische Projektion und $f(X) = X^2 - 3 \in \mathbb{Z}[X]$. Berechnen Sie $f(\overline{4}) \in \mathbb{F}_7$.

$$f(\overline{4}) = \overline{4}^2 - \overline{3} = \pi(16-3) = \overline{6}.$$

Sei $\mathbb{R} \to M_2(\mathbb{R})$ der Ringhomomorphismus mit $a \mapsto aE_2$. Berechnen Sie $f(A) \in M_2(\mathbb{R})$ für $f = X^2 + 2X - 3$ und $A = \begin{pmatrix} -1 & 2 \\ 2 & -1 \end{pmatrix}$.

$$f(A) = A^2 + \underset{\substack{\parallel \\ (2E_2 A)}}{2A} - 3E_2 = \begin{pmatrix} 5 & -4 \\ -4 & 5 \end{pmatrix} + \begin{pmatrix} -2 & 4 \\ 4 & -2 \end{pmatrix} + \begin{pmatrix} -3 & 0 \\ 0 & -3 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Grad, Absolutkoeffizient, Leitkoeffizient, normierte Polynome

Sei R ein kommutativer Ring. Sei $f = \sum_{i=0}^{n} a_i X^i \in R[X]$ mit $a_n \neq 0$.

Dann heißt n der <u>Grad</u> des Polynoms f, wir schreiben $\deg(f)$.

Für $f \neq 0$ erhalten so $\deg(f) \in \mathbb{N}$. Wir setzen formal $\deg(0) = -\infty$.

Der Koeffizient a_n eines Polynoms vom Grad n heißt der <u>Leitkoeffizient</u>.

Ein Polynom heißt <u>normiert</u>, wenn der Leitkoeffizient gleich 1 ist.

Der Koeffizient a_0 von X^0 $(=1)$ heißt der Absolutkoeffizient. $(= f(0))$.

Polynome und Polynomfunktionen
Vorlesungswoche 1

Ulrich Görtz

Lineare Algebra 2, SS 21

Essen Seminar for Algebraic Geometry and Arithmetic

UNIVERSITÄT DUISBURG ESSEN

Polynomfunktionen

R kommutativer Ring

Def. Eine Abbildung $f: R \to R$ der Form $f(x) = \boxed{\sum_{i=0}^{n} a_i x^i}$ mit $n \in \mathbb{N}$, $a_i \in R$, heißt <u>Polynomfunktion</u>.

Die Menge $\mathrm{Pol}(R)$ $(\subseteq \mathrm{Abb}(R,R))$ bildet einen Ring bzgl. der Add. und Mult. von Funktionen.

$$(f+g)(x) = f(x) + g(x)$$

$$(f \cdot g)(x) = f(x) \cdot g(x)$$

(Einselement: $x \mapsto 1$)

Haben konstruiert: Polynomring $R[X] = \left\{ \sum_{i=0}^{n} a_i X^i \right\} \ni f = \sum_{i=0}^{n} b_i X^i$

$\rightsquigarrow$ $R \to R$, $x \mapsto f(x) := \sum_{i=0}^{n} b_i x^i$ Polynomfkt.

Erhalte <u>surjektiven Ringhomom.</u> $R[X] \longrightarrow \mathrm{Pol}(R)$

… für einen unendlichen Körper K

<u>Satz</u> Sei K ein Körper mit unendlich vielen Elementen.

Dann ist die Abb. $K[X] \xrightarrow{\alpha} \mathrm{Pol}(K)$ ein Homomorphismus.

<u>Beweis</u> zu: ist injektiv.

Wir wissen aber: ist $f = \sum_{i=0}^{n} a_i X^i \in K[X]$ mit $f(x) = 0$ für alle $x \in K$,

so sind alle $a_i = 0$, d.h. $f = 0 \in K[X]$.

Also $\mathrm{Ker}(\alpha) = \{0\}$, d.h., dass α injektiv ist.

… für einen endlichen Körper K

Sei K ein endlicher Körper, etwa $K = \{x_1, \dots, x_q\}$.

Dann ist der Ringhomom. $\alpha : K[X] \to \mathrm{Pol}(K)$ nicht injektiv.

Sei $$f := \prod_{i=1}^{q} (X - x_i) = X^q - (x_1 + \dots + x_q) X^{q-1} \dots + (-1)^q x_1 \cdots x_q \in K[X]$$

Dann gilt $f(x) = 0$ für alle $x \in K$

(denn x ist eines der x_i)

Weil der Koeffizient von X^q in f gleich 1 ist, ist $f \neq 0 \in K[X]$.

Quiz

Geben Sie Polynomfunktionen $f, g \colon \mathbb{F}_2 \to \mathbb{F}_2$ an, die beide von der Nullfunktion verschieden sind, aber so dass das Produkt fg die Nullfunktion ist.

Quiz

$\{0, 1\}$
$\parallel$

Geben Sie Polynomfunktionen $f, g \colon \mathbb{F}_2 \to \mathbb{F}_2$ an, die beide von der Nullfunktion verschieden sind, aber so dass das Produkt fg die Nullfunktion ist.

- $f : \mathbb{F}_2 \to \mathbb{F}_2, \quad x \mapsto x \qquad (f(1) = 1 \neq 0)$
- $g : \mathbb{F}_2 \to \mathbb{F}_2, \quad x \mapsto x - 1 \qquad (g(0) = 1 \neq 0)$

$$\rightsquigarrow \quad (f \cdot g)(x) = x(x-1) = \begin{cases} 0 & x = 0 \\ 0 & x = 1 \end{cases}$$