Kapitel 1: Polynomring

Anweisung:

- Wiederholen Sie Begriffe aus LAI: Gruppe, Ring, Körper, Vektorraum, Untervektorraum, lineare Abbildung, injektiv, surjektiv, bijektiv, Konstruktion von $\mathbb{Z}_n$, komplexe Zahlen, vollständige Induktion
- Lesen Sie das Kapitel durch, und machen Sie sich Notizen, was Sie nicht verstehen. Schlagen Sie Begriffe nach, die Sie vergessen haben. Arbeiten Sie nun sorgfältig das Kapitel durch. Nehmen Sie sich hierzu Teilabschnitte vor, die inhaltlich zusammenhängen. Versuchen Sie nun die Lücken im Skript zu schließen. Einige der Lücken sind Wiederholungsaufgaben. Versuchen Sie diese erst selbstständig zu lösen, bevor Sie diese nachschlagen.
- Im Forum in Ilias können Sie über den Text und insbesondere die Lücken diskutieren. Versuchen Sie anderen Hilfestellung zu geben, ohne die Lösung zu verraten. Viel Spaß!

Literaturhinweis: Lesen Sie zur Ergänzung

- Klopsch, Lineare Algebra I, Abschnitt 13.
- Stix, Lineare Algebra, Abschnitt 13.

§1 Der Polynomring $K[X]$

Sei K ein Körper, $\underset{S}{R}$ ein kommut. Ring mit 1, "

1.1 Def: Ein Ringhomomorphismus, kurz Homomorphismus, zwischen Ringen R und S ist eine Abbildung $\varphi: R \longrightarrow S$ mit

(R1) $\varphi(1_R) = 1_S$,

(R2) $\varphi(a+b) = \varphi(a) + \varphi(b)$

(R3) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$,

für alle $a, b \in R$.

Abbildung φ heißt Isomorphismus, falls φ zusätzlich bijektiv.

Zwei Ringe R und S heißen isomorph, geschrieben $R \simeq S$, falls es einen Isomorph. $\varphi: R \to S$ gibt

1.2 Bsp:

(a) Sei $n \in \mathbb{N}$. Dann ist $\mathbb{Z} \longrightarrow \mathbb{Z}_n$, $a \longmapsto a + n\mathbb{Z}$ ein Ringhomomorphismus.

(R1) Das Einselement von $\mathbb{Z}$ ist _____.
Das Einselement von $\mathbb{Z}_n$ ist _____.

Es gilt $\varphi(\_\_) = \_\_\_$, also gilt (R1).

Weiterhin gelten (R2) und (R3):

Für alle $a, b \in R$ gilt:

$\varphi(a+b) =$

$\varphi(a \cdot b) =$

Also ist φ Ringhomomorphismus.

Ist φ injektiv? Ist φ surjektiv?

(b) Inklusion von Ringen ist ein Ringhomomorphismus,
z.B. $\mathbb{Z} \xhookrightarrow{\varphi} \mathbb{Q}$, $a \mapsto a$ ist —"— .
Die Inklusion ist injektiv.

(c) Ist die Abb. $\varphi: \mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{C}$, $(x,y) \longmapsto x+yi$
ein Ringisomorphismus? Begründung?

(d) Sei $\varphi: R \longrightarrow S$ ein Ringisomorphismus. Dann ist φ bijektiv, also existiert eine Abbildung $\varphi^{-1}: S \longrightarrow R$, (die natürlich auch bijektiv ist, nach LA I).
Die Abb. φ^{-1} ist ein Homomorphismus:
Seien $a, b \in S$. Dann ist

$$\varphi^{-1}(a+b) = \varphi^{-1}\left(\varphi(\varphi^{-1}(a)) + \varphi(\varphi^{-1}(b))\right)$$

$$\overset{\varphi \text{ Homom.}}{=} \varphi^{-1}\left(\underline{\qquad\qquad\qquad\qquad}\right)$$

$$= \varphi^{-1}(a) + \varphi^{-1}(b),$$

und analog gilt

$$\varphi^{-1}(a \cdot b) =$$

$$= \varphi^{-1}(a) \cdot \varphi^{-1}(b).$$

1.3 Bem: Ein Element $a \in R$ heißt <u>invertierbar</u> oder <u>Einheit in R</u>, falls es $b \in R$ gibt mit $ab = 1 = ba$.
Definiere $R^\times = \{r \in R \mid r \text{ invertierbar}\}$
Dann ist $(R^\times, \cdot)$ eine Gruppe, die Einheitengruppe von Ring R. Siehe LA I.

1.4 Bsp: $\mathbb{Z}^\times = \{+1, -1\}$
$\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$
$K^\times = K \setminus \{0\}$
$\mathbb{Z}_{15}^\times = \{\bar{1}, \bar{2}, \_\_\_\_\_\}$ Warum?

Übung: Zeigen Sie: $\bar{a} \in \mathbb{Z}_n^\times \iff ggT(a, n) = 1$.

Aus der Schule und aus Analysis kennen Sie Polynomfunktionen vom Typ $\mathbb{R} \to \mathbb{R}$ oder $\mathbb{C} \to \mathbb{C}$. Wir lassen auch andere Grundkörper zu:

1.5 Def: Sei R ein Ring oder Körper.
Der Polynomring $R[X]$ in einer Variablen X besteht aus formalen Summen

$$p := \sum_{i=0}^{n} a_i X^i, \quad n \in \mathbb{N}_0, \; a_i \in R, \; 0 \le i \le n.$$

Wir nennen p ein Polynom und schreiben

$$p = \sum_{i \ge 0} a_i X^i \text{ mit } a_i = 0 \text{ für } i \ge n+1.$$

Definiere Addition und Multiplikation von Polynomen durch:

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

und $$\left(\sum_{i \ge 0} a_i X^i\right) \cdot \left(\sum_{i \ge 0} b_i X^i\right) = \sum_{i \ge 0} c_i X^i$$

mit $$c_i := \sum_{t=0}^{i} a_t b_{i-t} = \sum_{s+t=i} a_s b_t$$

z.B. $$p = (X^3 - 2X)(X^2 + 1) = X^5 + X^3 - 2X^3 - 2X$$
$$= X^5 - X^3 - 2X,$$

wie Sie das aus der Schule gewohnt sind.

1.6. Bem:

(a) Die Ringaxiome von R implizieren die Ringaxiome von $R[X]$:

z.B. (i) Kommutativgesetz für Addition gilt, denn:

$$\sum_{i\geq 0} a_i X^i + \sum b_i X^i \overset{\text{Def}}{=} \overset{\text{Kommutativgesetz in } R}{=} \overset{\text{Def}}{=} \sum_{i\geq 0} b_i X^i + \sum_{i\geq 0} a_i X^i$$

(ii) Assoziativgesetz für Multiplikation:

Seien $f = \sum a_i X^i$, $g = \sum b_i X^i$, $h = \sum d_i X^i$ in $R[X]$.

Der i-te Summand von $(f\cdot g)\cdot h$ ist

$$\sum_{p=0}^{i} c_p d_{i-p} \overset{\text{Def von } c_p \text{ wie in 1.5}}{=} \sum_{p=0}^{i} \left(\sum_{q=0}^{p} a_q b_{p-q} \right) d_{i-p}$$

$$\overset{\text{Warum?}}{=} \sum_{p=0}^{i} \sum_{q=0}^{p} a_q b_{p-q} d_{i-p} \qquad (1)$$

$$\overset{\text{Warum?}}{=} \sum_{r+s+t=i} a_r b_s d_t \qquad (2)$$

und dies entspricht auch dem i-ten Summanden von $f(g\cdot h)$.

Bei (1) benutzen wir:

Bei (2) benutzen wir:

Einfachheitshalber spezialisieren wir und arbeiten ab jetzt mit $R = K$ Körper.

1.7 Bem: Der Polynomring $K[X]$ ist auch ein K-Vektorraum und nach 1.6 (b) auch ein Untervektorraum des K-Vektorraumes der folgen. (Warum?) Eine Basis von $K[X]$ ist durch die Potenzen von X gegeben: $1, X, X^2, \ldots$

1.8 Def: Wir definieren die Auswertungsabbildung für $x \in K$ als die Abbildung

$$\mathrm{ev}_x : K[X] \longrightarrow K$$

$$p = \sum_{i \geq 0} a_i X^i \longmapsto \sum_{i \geq 0} a_i x^i$$

Beachten Sie die Notation:

X Großbuchstabe – ist Variable,

x Kleinbuchstabe – ist Element aus Körper K.

1.9 Prop: Sei K ein Körper und $x \in K$. Die Auswertungsabbildung für $x \in K$ ist ein Ringhomomorphismus.

Beweis: (Übung)

(b) Formal gesehen sind Polynome Folgen $(a_i)_{i \in \mathbb{N}_0}$ mit $a_i \in R$, wobei nur endlich viele a_i ungleich Null sind. Setze $X := (0,1,0,0,\dots)$. Dann folgt mit obiger Multiplikationsformel

$$X^2 = X \cdot X = (0,1,0,0,\dots) \cdot (0,1,0,0,\dots)$$
$$= (0,0,1,0,\dots)$$

Etc.
Induktiv ist also $X^j = (b_i)$ mit $b_i = \begin{cases} 1 & \text{für } i=j \\ 0 & \text{für } i \neq j \end{cases}$

Für $a \in R$, definiere $a \cdot (b_i) := (a \cdot b_i)$. Dann entspricht die Folge (a_i) genau der formalen Summe $\sum_{i \geq 0} a_i X^i$ aus Definition 1.5.

(c) Sei $n \geq 2$. Definiere induktiv

$$R[X_1, \dots, X_n] := R[X_1, \dots, X_{n-1}][X_n],$$

den Polynomring über R in n Unbestimmten $X_1, X_2, \dots, X_n$.

1.10 Bem: (Polynom versus Polynomfunktion)

(a) Die Menge $Abb(k,k) = \{f : K \to k\}$ aller Abbildungen von K nach K ist ein K-Vektorraum und trägt auch die Struktur eines Ringes. Die Operation Addition, Skalarmultiplikation bzw Multiplikation (im Ring) sind gegeben durch

$$(f+g)(x) := f(x) + g(x)$$
$$(\lambda f)(x) := \lambda \cdot f(x)$$
$$(f \cdot g)(x) := f(x) \cdot g(x),$$

für alle $f, g \in Abb(k,k)$ und $\lambda \in K$.

(b)(i) Wir unterscheiden zwischen Polynomen und ihren zugehörigen Polynomfunktionen: Jedes Polynom $p = \sum a_i X^i \in K[X]$ definiert eine Polynomfunktion f_p durch $f_p : K \longrightarrow K$, $x \longmapsto \sum a_i x^i =: f_p(x)$

Statt $f_p(x)$ schreiben wir üblicherweise $p(x)$.

(ii) Die resultierende Abbildung $f : K[X] \longrightarrow Abb(k,k)$, $p \longmapsto f_p$

die einem Polynom p die zugehörige Polynomfunktion f_p zuordnet ist ein Ringhomomorphismus, sowie eine K-lineare Abbildung (dh. ein Vektorraumhomomorphismus). Das Bild von f, also $im(f)$, entspricht dem Unterraum der Polynomfunktionen im K-$Abb(K,K)$. Abbildung f ist im Allgemeinen also nicht surjektiv.

Vektorraum?

(c) Ein Ring R, der gleichzeitig ein K-VR ist, so daß Skalare mit allem kommutieren, nennt man eine K-Algebra. Sowohl $K[X]$ als auch $Abb(K,K)$ sind Beispiele von K-Algebren. Die in (b) erwähnte Abbildung ist ein K-Algebrenhomomorphismus.

(d) Aus der formalen Definition von Polynomen in 1.5(b) folgt: Zwei Polynome $p = \sum a_i X^i$, $q = \sum b_i X^i$ sind gleich, genau dann, wenn $a_i = b_i$ $\forall i$. Insbesondere sind dann auch die zugehörigen Polynomfunktionen f_p und f_q gleich. Die Umkehrung gilt im Allgemeinen nicht:
Sei z.B. $K = \mathbb{Z}_2$. Seien p = Nullpolynom und sei $q = X^2 + X$ in $\mathbb{Z}_2[X]$. Dann ist $p \neq q$ als Polynom. Die zugehörigen Polynomfunktionen sind aber gleich: $f_p = f_q$, denn $q(0) = \_\_\_\_$,
$q(1) = \_\_\_\_$.
Insbesondere ist der ~~Homomorphismus~~ f aus (b) nicht notwendigerweise injektiv.

Übung: Beweisen Sie die Aussagen in (b):