Universität Konstanz
Fachbereich Mathematik und Statistik
Prof. Dr. Markus Schweighofer
Aaron Kunert / Sven Wagner

Wintersemester 2009/2010
Übungsblatt 6
23.11.2009

Lineare Algebra I

Aufgabe 6.1: (Polynomdivision mit Rest)

Seien K ein Körper und $K[X]$ der Polynomring über K in der Unbestimmten X.

(a) Seien $p, q \in K[X]$. Zeigen Sie:

$$\deg(p+q) \leq \max\{\deg(p), \deg(q)\}, \tag{1}$$

$$\deg(p+q) = \max\{\deg(p), \deg(q)\}, \text{ falls } \deg(p) \neq \deg(q), \text{ und} \tag{2}$$

$$\deg(pq) = \deg(p) + \deg(q) \tag{3}$$

In diesem Zusammenhang gelte $-\infty + d := -\infty =: d + (-\infty)$ für alle $d \in \mathbb{N}_0 \cup \{-\infty\}$ und $-\infty < d$ für alle $d \in \mathbb{N}_0$.

(b) Seien $p, q \in K[X]$. Zeigen Sie, dass aus $pq = 0$ stets $p = 0$ oder $q = 0$ folgt.

(c) Sei $g \in K[X]$, und sei $(g) = \{pg \mid p \in K[X]\}$ das davon erzeugt Hauptideal in $K[X]$. Es bezeichne $\equiv_{(g)}$ die dazugehörige Kongruenzrelation auf $K[X]$, das heißt $p \equiv_{(g)} q \iff p - q \in (g)$ für alle $p, q \in K[X]$. Zeigen Sie: Sind $p, q \in K[X]$ mit $\deg(p) < \deg(g) > \deg(q)$ und $p \equiv_{(g)} q$, so gilt $p = q$.

(d) Sei $g \in K[X]$ und $g \neq 0$. Sei $f \in K[X]$ mit $\deg(g) \leq \deg(f)$. Zeigen Sie, dass es ein $r \in K[X]$ mit $f \equiv_{(g)} r$ und $\deg(r) < \deg(f)$ gibt.

(e) Seien $f, g \in K[X]$ und $g \neq 0$. Zeigen Sie, dass es genau ein $r \in K[X]$ mit $f \equiv_{(g)} r$ und $\deg(r) < \deg(g)$ gibt.
(Hinweis: Verwenden Sie (a) und (c) für die Eindeutigkeit und (d) für die Existenz.)

(f) Seien $f, g \in K[X]$ und $g \neq 0$. Zeigen Sie, dass es genau ein Paar $(q, r) \in K[X] \times K[X]$ mit $f = qg + r$ und $\deg(r) < \deg(g)$ gibt.
(Hinweis: Verwenden Sie (b) und (e).)
Es heißt $f \operatorname{div} g := q$ der **Quotient** und $f \bmod g := r$ der **Rest** bei **(Polynom-) Division** von f durch g.

(g) Seien $f, g \in K[X]$ und $g \neq 0$. Zeigen Sie, dass das Polynom r aus (e) der Rest der Polynomdivision von f durch g ist.

(h) Berechnen Sie unter Benutzung eines Quotientenrings $K[X]/(g)$ (vgl. Beispiel in der Vorlesung in $\mathbb{Z}/(10)$) folgende Reste von Polynomdivisionen in $K[X]$:
- $(2X^3 + 2X^2 - 1)^{100} \bmod X^2 - 2$ für $K = \mathbb{F}_5$.
- $(64X^6 + 144X^4 + 108X^2 + 27)^{473} \bmod 16X^4 + 24X^2 + 10$ für $K = \mathbb{R}$.
- $\prod_{i=1}^{6} (X^i - \frac{1}{i}) \bmod X^7$ für $K = \mathbb{F}_7$.

Aufgabe 6.2:

(a) Sei $\mathbb{F}_2 = \mathbb{Z}/(2) = \{0, 1\}$ der Körper mit zwei Elementen, und sei $\mathbb{F}_2[X]$ der Polynomring in einer Unbestimmten über $\mathbb{F}_2$. Sei $g := X^2 + X + 1 \in \mathbb{F}_2[X]$. Zeigen Sie:

(i) $\mathbb{F}_4 := \mathbb{F}_2[X]/(g) = \{\overline{0}, \overline{1}, \overline{X}, \overline{X+1}\}$.

Bitte wenden.

(ii) $\mathbb{F}_4$ ist ein Körper mit vier Elementen. Stellen Sie dafür auch die Additions- und Multiplikationstabelle auf, wobei Sie $\overline{0}$ mit 0, $\overline{1}$ mit 1, $\overline{X}$ mit a und $\overline{X+1}$ mit b bezeichnen.

(b) Sei nun K ein beliebiger Körper mit vier Elementen. Zeigen Sie, dass K isomorph zu $\mathbb{F}_4$ ist. Gehen Sie dabei wie folgt vor:

- Nehmen Sie an, das Universum von K ist die Menge $\{0, 1, a, b\}$.
- Welche abelsche Gruppen kommen für die additive abelsche Gruppe $(K, +)$ überhaupt in Frage?
- Welche abelsche Gruppen kommen für die multiplikative abelsche Gruppe $K^\times$ in Frage?
- Wie müssen die Additions- und Multiplikationstabelle von K aussehen?
- K ist als kommutativer Ring isomorph zu $\mathbb{F}_4$.

Aufgabe 6.3:

Sei $\mathbb{F}$ ein endlicher Körper mit genau m Elementen.

(a) Zeigen Sie, dass $\sum_{i=1}^{m} a = 0$ für alle $a \in \mathbb{F}$.
(Hinweis: Versuchen Sie zuerst, für ein beliebiges $a \in \mathbb{F}$ die Existenz eines $k \in \mathbb{N}$ mit $\sum_{i=1}^{k} a = 0$ zu beweisen, und betrachten Sie dafür die von a erzeugte Untergruppe der abelschen Gruppe $(\mathbb{F}, +)$.)

(b) Zeigen Sie, dass $a^{m-1} = 1$ für alle $a \in \mathbb{F} \setminus \{0\}$.

(c) Zeigen Sie, dass die Polynome $\prod\limits_{a \in \mathbb{F}^\times} (X - a)$ und $X^{m-1} - 1$ übereinstimmen.

(d) Finden Sie ein Polynom $f \in \mathbb{F}[X] \setminus \{0\}$ mit $f(a) = 0$ für alle $a \in \mathbb{F}$.

Aufgabe 6.4:

Schreiben Sie die folgenden komplexen Zahlen in der Form: $a + b\mathring{\imath}$ mit $a, b \in \mathbb{R}$.

(i) $(2 + 3\mathring{\imath})(1 - 5\mathring{\imath})$

(ii) $\dfrac{1}{\mathring{\imath}}$

(iii) $\dfrac{1}{1 + \mathring{\imath}}$

(iv) $\dfrac{1 + \mathring{\imath}}{1 - \mathring{\imath}}$

(v) $(1 + \mathring{\imath})^{16}$

Abgabe bis Montag, den 30. November, 10 Uhr in die Briefkästen neben F411.