TECHNISCHE UNIVERSITÄT DRESDEN

Fakultät Mathematik und Naturwissenschaften Fachrichtung Mathematik, Institut für Algebra

Prof. Dr. A. Fehm, Dr. C. Zschalig

Algebra und Zahlentheorie (Modul ALGZTH), Sommersemester 2017

7. Übungsblatt für die Übungen vom 26.6.-30.6.2017

Ringe von Brüchen, irreduzible Polynome, Körper

Hinweis: Wir betrachten in der Übung - wie in der Vorlesung - ausschließlich **kommutative Ringe mit Einselement**.

V57. **Vorbereitungsaufgabe: Bitte bereiten Sie diese Aufgabe zur Übung vor.**

(a) Zeigen Sie, dass das Polynom $X^2 + X + 1$ irreduzibel in $\mathbb{F}_2[X]$ ist.

(b) Stellen Sie die Verknüpfungstafeln für Addition und Multiplikation im Körper $\mathbb{L} := \mathbb{F}_2[X]/(X^2 + X + 1)$ auf.

(c) Lösen Sie im Körper $\mathbb{L}$ die folgenden linearen Gleichungssysteme in den Unbekannten $x_1, x_2 \in \mathbb{L}$ (zu $f(X) \in \mathbb{F}_2[X]$ sei $\overline{f(X)} := f(X) + (X^2 + X + 1) \in \mathbb{L}$).

(i)
$$\begin{array}{rl} \overline{1} \cdot x_1 + \overline{X} \cdot x_2 & = \overline{1} \\ \overline{(X+1)} \cdot x_1 + \overline{1} \cdot x_2 & = \overline{X} \end{array}$$

(ii)
$$\begin{array}{rl} \overline{X} \cdot x_1 + \overline{X} \cdot x_2 & = \overline{1} \\ \overline{(X+1)} \cdot x_1 + \overline{1} \cdot x_2 & = \overline{1} \end{array}$$

Ü58. (a) Bestimmen Sie den Inhalt des Polynoms $f(X) = 84X^3 + \frac{24}{5}X^2 + \frac{60}{7}X + \frac{36}{7}$, wenn

- $f(X)$ als Polynom mit Koeffizienten aus $K = \mathbb{Q}$ als Quotientenkörper von $R = \mathbb{Z}$
- $f(X)$ als Polynom mit Koeffizienten aus $K = R = \mathbb{Q}$

aufgefasst wird.

(b) Es seien $f(X), g(X) \in \mathbb{Q}[X]$ Polynome mit rationalen Koeffizienten. Formulieren Sie eine notwendige und hinreichende Bedingung an die Koeffizienten von $f(X)$ und $g(X)$, so dass $f(X) \cdot g(X) \in \mathbb{Z}[X]$.

Ü59. Zeigen Sie die Irreduzibilität folgender Polynome in $\mathbb{Z}[X]$ bzw. $\mathbb{Q}[X]$. Nutzen Sie dazu die Kriterien, die Sie in VL II.10. kennengelernt haben.

(a) $X^3 + 6X^2 - 17X + 8$,
(b) $X^4 + 2X^3 + X^2 + 2X + 1$
(c) $X^4 + 2X + 2$,
(d) $X^4 + 2X + 4$
(e) $3X^4 + 5X^3 - 10X^2 - 5X + 15$,
(f) $7X^3 - 8X^2 + 17X - 135$

Ü60. Es sei $S = \{2^m \mid m \in \mathbb{N}_0\}$. Die Menge $S^{-1}\mathbb{Z} := \{\frac{g}{2^m} \mid g \in \mathbb{Z}, m \in \mathbb{N}_0\} \subseteq \mathbb{Q}$ bildet zusammen mit der üblichen Addition und Multiplikation (s. VL II.8.4) einen Ring ohne Nullteiler. Beweisen Sie das!

(a) Zeigen Sie, dass für alle ungeraden g gilt: $\frac{g}{2^m} \mid \frac{h}{2^n}$ in $S^{-1}\mathbb{Z} \iff g|h$ in $\mathbb{Z}$

(b) Geben Sie die Einheiten von $S^{-1}\mathbb{Z}$ an.

(c) Geben Sie ein vollständiges Vertretersystem der Klassen assoziierter Elemente von $S^{-1}\mathbb{Z}$ an.

(d) Sind 2 und 6 Primelemente von $S^{-1}\mathbb{Z}$?

A61. **Hausaufgabe nur für Lehramtsstudierende,**
bitte bis zum 5.7.2017, 12:00 Uhr im entsprechenden Briefkasten im C-Flügel unter Angabe von Name, Matrikelnr. und Übungsgruppe abgeben.

(a) Bestimmen Sie alle irreduziblen Polynome $\varphi \in \mathbb{F}_2[X]$ mit $\deg(\varphi) = 4$.

(b) Zerlegen Sie das Polynom $\varphi = X^7 - 1$ in $\mathbb{F}_2[X]$ in irreduzible Faktoren.

A62. **Hausaufgabe für Bachelor- und Lehramts-Studierende,**
bitte bis zum 5.7.2017, 12:00 Uhr im entsprechenden Briefkasten im C-Flügel unter Angabe von Name, Matrikelnr. und Übungsgruppe abgeben.
Es sei $\varphi(X) = X^4 + 1$.

(a) Zeigen Sie: $\varphi(X)$ ist irreduzibel in $\mathbb{Z}[X]$.

(b) Zeigen Sie: $\varphi(X)$ ist reduzibel in $\mathbb{F}_2[X]$, $\mathbb{F}_3[X]$ und $\mathbb{F}_5[X]$.

(c) Zeigen Sie: $\varphi(X)$ ist reduzibel in $\mathbb{F}_p[X]$ für jede Primzahl p mit $p \equiv 1 \pmod 4$.
Hinweis: Sie können z.B. $a, b \in \mathbb{F}_p$ suchen, die die Gleichung $X^4 + 1 = (X^2 + a)(X^2 + b)$ erfüllen.

(d)* [Zusatzaufgabe - wird nicht bewertet]
Zeigen Sie: $\varphi(X)$ ist reduzibel in $\mathbb{F}_p[X]$ für jede Primzahl p mit $p \equiv 3 \pmod 4$.
Hinweis: Wählen Sie den Ansatz $X^4+1 = (X^2+aX+b)(X^2+cX+d)$ und zeigen Sie, dass es geeignete $a, b, c, d \in \mathbb{F}_p[X]$ gibt, die diese Gleichung erfüllen. Sie benötigen dazu Eigenschaften des *Legendre-Symbols*, das nicht in der VL behandelt wurde.

A63. **Hausaufgabe nur für Bachelor-Studierende,**
bitte bis zum 5.7.2017, 12:00 Uhr im entsprechenden Briefkasten im C-Flügel unter Angabe von Name, Matrikelnr. und Übungsgruppe abgeben.
Zeigen Sie: Ist $f(X) \in \mathbb{Z}[X]$ ein Polynom mit $2 \nmid f(0)$ und $2 \nmid f(1)$, dann besitzt $f(X)$ keine ganzzahlige Nullstelle. Beweisen Sie, dass darüber hinaus $f(X)$ keine rationale Nullstelle besitzt, wenn der Leitkoeffizient ungerade ist.

H64. Welche der beiden Faktorringe $\mathbb{F}_2[X]/(X^2+1)$ und $\mathbb{F}_3[X]/(X^2+1)$ sind Körper? Begründen Sie. Stellen Sie jeweils Verknüpfungstafeln für Addition und Multiplikation auf.

H65. Zeigen Sie: Ist R faktoriell und $f(X), g(X) \in R[X]$ teilerfremd, dann ist $f(X)+g(X)\cdot Y \in R[X,Y]$ ein Primelement.

H66. Es seien

$$f(X) = X^5 - X^4 - 2X^3 + 2X^2 - 3X + 3 \quad \text{und} \quad g(X) = X^4 + X^3 - 2X^2 - 3X + 3$$

Polynome aus $\mathbb{Q}[X]$.

(a) Zerlegen Sie $f(X)$ und $g(X)$ in irreduzible Faktoren in $\mathbb{Q}[X]$, in $\mathbb{R}[X]$ und in $\mathbb{C}[X]$. Daraus kann $\mathrm{ggT}(f(X), g(X))$ abgelesen werden.

(b) Bestimmen Sie $\mathrm{ggT}(f(X), g(X))$ mit dem erweiterten Euklidischen Algorithmus.

(c) Begründen Sie: Ist $L|K$ eine Körpererweiterung, dann gilt für alle Polynome $f(X), g(X) \in K[X]$: $\mathrm{ggT}_K(f(X), g(X)) = \mathrm{ggT}_L(f(X), g(X))$.