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

8. Übungsblatt für die Übungen vom 10.7.-14.7.2017

Körper

V67. **Vorbereitungsaufgabe: Bitte bereiten Sie diese Aufgabe zur Übung vor.**

(a) Wir wissen aus der Vorlesung, dass die Menge $\mathbb{Q}[\sqrt{2}] := \{s + t \cdot \sqrt{2} \mid s,t \in \mathbb{Q}\} \subseteq \mathbb{R}$ einen Körper bildet, es gilt also $\mathbb{Q}[\sqrt{2}] = \mathbb{Q}(\sqrt{2})$. Geben Sie das Inverse eines Elements $s + t\sqrt{2}$ explizit an.

(b) Zeigen Sie die paarweise Nichtisomorphie der folgenden Ringe:
$(\mathbb{F}_2)^2 = \mathbb{F}_2 \times \mathbb{F}_2, \qquad \mathbb{F}_{2^2}, \qquad \mathbb{Z}/2^2\mathbb{Z}.$

Ü68. Es sei $f = X^6 - 5X - 10$.

(a) Beweisen Sie, dass f irreduzibel in $\mathbb{Q}[X]$ ist.

(b) Es sei α eine Nullstelle von f (in einem Erweiterungskörper, z.B. $\mathbb{R}$ oder $\mathbb{C}$). Welchen Grad hat die Körpererweiterung $\mathbb{Q}(\alpha) \mid \mathbb{Q}$?

(c) Geben Sie eine Basis des $\mathbb{Q}$-Vektorraumes $\mathbb{Q}(\alpha)$ an.

(d) Drücken Sie die Elemente α^6, α^8 und α^{16} als Linearkombination dieser Basiselemente aus.

Ü69. Bestimmen Sie die Minimalpolynome von $\sqrt[4]{2}+1$, von $\sqrt[3]{2}+1$ und von $\alpha = \sqrt{2}+\sqrt{3}$ über $\mathbb{Q}$ und über $\mathbb{Q}(\sqrt{2})$.

Ü70. Beweisen Sie Lemma III.4.4: Für $f, g \in F[X]$ gelten:

(a) $(f+g)' = f' + g'$

(b) $(fg)' = f' \cdot g + f \cdot g'$

Hinweis: Die folgenden Hausaufgaben sind vorrangig für diejenigen Studierenden gedacht, die noch nicht genügend Punkte zum Erreichen der PVL haben. Beachten Sie das Abgabedatum!

A71. **Hausaufgabe, bitte bis zum 14.7.2017, 12:00 Uhr im entsprechenden Briefkasten im C-Flügel unter Angabe von Name, Matrikelnr. und Übungsgruppe abgeben.**
Wie viele Elemente hat der Zerfällungskörper des Polynoms

$$\varphi(X) = (X^2 + 2X + 2)(X^3 + 2X + 1) \in \mathbb{F}_3[X]\,?$$

Lösen Sie das Problem in folgenden Schritten:

(a) Finden Sie einen irreduziblen Faktor ψ_0 von φ vom Grad > 1. Ist einer der angegebenen Faktoren schon irreduzibel?

(b) Erweitern Sie $\mathbb{F}_3$ durch Übergang zum Körper $E_1 := \mathbb{F}_3[X]/(\psi_0)$.

(c) Finden Sie einen nichttrivialen Faktor ψ_1 von φ, der über dem Erweiterungskörper E_1 irreduzibel ist.

(d) Wie viele Elemente hat der Körper $E_2 := E_1[X]/(\psi_1)$, den man durch erneute Erweiterung erhält?

(e) Zerfällt φ über diesem Körper in Linearfaktoren, oder muss der Vorgang wiederholt werden?

A72. **Hausaufgabe, bitte bis zum 14.7.2017, 12:00 Uhr im entsprechenden Briefkasten im C-Flügel unter Angabe von Name, Matrikelnr. und Übungsgruppe abgeben.**

Das Polynom $f(X) := X^{16} - X$ aus $\mathbb{F}_2[X]$ lässt sich schreiben in der Form

$$f(X) = X \cdot (X + 1) \cdot q(X).$$

(a) Bestimmen Sie $q(X)$.

(b) Es sei α eine Primitivwurzel von $\mathbb{F}_{16}$ und $\beta := \alpha^3$. Was sind die Ordnungen von α und β in $\mathbb{F}_{16}^{\times}$?

Hinweis: Eine *Primitivwurzel* in einem (endlichen) Körper F ist ein Element $\alpha \in F$ mit $\langle\alpha\rangle = F^{\times}$. Der Körper $\mathbb{F}_{16}$ kann aus $\mathbb{F}_2[X]$ durch Faktorisierung nach dem Hauptideal eines irreduziblen Polynoms $f \in \mathbb{F}_2[X]$ vom Grad 4 konstruiert werden.

(c) Was ist der kleinste Grad eines nichttrivialen Polynoms aus $\mathbb{F}_2[X]$, welches β als Nullstelle hat?

(Hinweis: Jedes Polynom aus $\mathbb{F}_2[X]$, das β zur Nullstelle hat, hat auch β^2 als Nullstelle, etc.)

A73. **Hausaufgabe, bitte bis zum 14.7.2017, 12:00 Uhr im entsprechenden Briefkasten im C-Flügel unter Angabe von Name, Matrikelnr. und Übungsgruppe abgeben.**

Verifizieren Sie „$\mathbb{F}_{2^4} \cong \mathbb{F}_{4^2}$“.

Hinweis: Natürlich gilt obige Isomorphie nach dem Klassifikationssatz. Ziel der Aufgabe ist es, dass Sie $\mathbb{F}_2[X]/(f(X))$ und $\mathbb{F}_4[X]/(g(X))$ mit irreduziblen Polynomen $f(X) \in \mathbb{F}_2[X]$ und $g(X) \in \mathbb{F}_4[X]$ vom Grad 4 bzw. 2 konstruieren und dann einen Isomorphismus konkret angeben.