TECHNISCHE UNIVERSITÄT DRESDEN

Bereich Mathematik und Naturwissenschaften Fakultat Mathematik, Institut fur Algebra

Jun.-Prof. Martin Schneider, Dr. C. Zschalig

Algebra und Zahlentheorie für Lehramt (Modul ALGZTH), Sommersemester 2019

12. Übungsblatt für die Übungen vom 24.6.-28.6.2019

Polynomringe, endliche Körper

N12.1 **Hausaufgabe (Nachbereitung) Abgabe vor Übungsbeginn**
Die Summe aus erster und letzter Ziffer Ihrer Matrikelnummer sei die Zahl a, die Summe aus zweiter und vorletzter Ziffer sei die Zahl b.

Bestimmen Sie mit Hilfe des erweiterten Euklidischen Algorithmus das Element $d := \mathrm{ggT}(a+bi, 2+4i)$ im Ring $\underline{\mathbb{Z}}[i]$ der Gaußschen Zahlen und stellen Sie es als Linearkombination $d = c_1 \cdot (a+bi) + c_2 \cdot (2+4i)$ mit $c_1, c_2 \in \mathbb{Z}[i]$ dar. Machen Sie eine Probe!

Hinweis: Diese Aufgabe ist von jedem Mitglied Ihrer Gruppe separat zu lösen.

V12.2 **Hausaufgabe (Vorbereitung) Abgabe vor Übungsbeginn**

(a) Führen Sie die folgenden Polynomdivisionen mit Rest über den jeweiligen Körpern aus:

(i) $(X^9 + X^8 + X^7 + X^5) : (X^3 + X)$ über $\mathbb{Q}$

(ii) $(-X^5 + 4X^2 + 5) : (X^3 + X^2)$ über $\mathbb{Z}_{11}$

(iii) $(-X^5 + 4X^2 + 5) : (X^3 + X^2)$ über $\mathbb{Z}_5$

(b) Beweisen Sie, dass für alle $n \in \mathbb{N}$ das Polynom $X^n - 1 \in \mathbb{R}[X]$ ohne Rest durch $(X-1)$ teilbar ist. Geben Sie (in Abhängigkeit von n) den Quotienten an.

Ü12.3 Bestimmen Sie mit Hilfe des (erweiterten) Euklidischen Algorithmus die multiplikativen Inversen von

$$X^2 + 1 \text{ in } \mathbb{Z}_2[X]/X^4 + X + 1 \quad \text{und} \quad 2X^3 + 1 \text{ in } \mathbb{Z}_5[X]/X^5 + 4X + 2.$$

Ü12.4 Zeigen Sie die paarweise Nichtisomorphie der folgenden Ringe.

$(\mathbb{Z}_2)^2 = \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_2[X]/X^2 + X + 1$, $\mathbb{Z}_4$.

Finden Sie weitere, zu den genannten nichtisomorphe Ringe mit 4 Elementen.

Ü12.5 (a) Zeigen Sie, dass das Polynom $X^3 + X + 1$ irreduzibel im Polynomring $\mathbb{Z}_2[X]$ ist.

(b) Bestimmen Sie alle irreduziblen Polynome vom Grad 3 in $\mathbb{Z}_2[X]$.

(c) Geben Sie ein irreduzibles Polynom vom Grad 5 in $\mathbb{Z}_2[X]$ an. Geben Sie ein Polynom vom Grad 5 in $\mathbb{Z}_2[X]$ an, das nicht irreduzibel ist, aber keine Nullstellen besitzt.

Ü12.6 Betrachtet wird der Körper $K := \mathbb{Z}_2[X]/X^3 + X^2 + 1$.

(a) Stellen Sie die Verknüpfungstafeln für die Addition und die Multiplikation in K auf.

(b) Geben Sie zu jedem Element von K das inverse Element bezüglich der Addition und bezüglich der Multiplikation an, falls es existiert.

(c) Ermitteln Sie für K die Ordnungen aller Elemente in der additiven Gruppe und in der multiplikativen Gruppe.

Die folgenden Selbststudiumsaufgaben dienen der Festigung und Vertiefung des Stoffes in der Nachbereitung der Lehrveranstaltung. Sie müssen nicht abgegeben werden.

H12.7 Zeigen Sie: Hat das ganzzahlige Polynom $p(x) = x^2 + a_1x + a_0$ (d.h. es gilt $a_1, a_0 \in \mathbb{Z}$) die rationalen Nullstellen c_1 und c_2, dann sind c_1 und c_2 ganze Zahlen. Wählen Sie dazu $c_1 = \frac{e}{f}$ mit $\mathrm{ggT}(e, f) = 1$ (d.h. der Bruch ist vollständig gekürzt) und beweisen Sie $f = 1$.

Hinweis: Das bedeutet, dass c_1 und c_2 entweder irrational oder Teiler von a_0 sind. Diese Aussage lässt sich auf Basis des Satzes von Gauß auf Polynome beliebigen Grades erweitern und hilft u.U. enorm bei der Nullstellensuche.

H12.8 In dieser Aufgabe betrachten wir den Ring $R = \mathbb{Z}_3[X]/p(X)$ mit $p(X) := X^2 + 2X + 1$.

(a) Zeigen Sie: $p(X)$ ist reduzibel in $\mathbb{Z}_3[X]$.

(b) Berechnen Sie folgende Ausdrücke in R:

(i) $X^3 + X^2$, (ii) $X^{-3} + X^{-2}$

(c) Geben Sie alle Einheiten und alle Nullteiler in R an. Ist R ein Körper?

(d) Finden Sie einen Unterring in R, der ein Körper ist.

H12.9 Berechnen Sie das Produkt und den größten gemeinsamen Teiler für die folgenden Polynome sowohl in $\mathbb{Q}[X]$ als auch in $\mathbb{Z}_2[X]$:

(a) $p_1(X) = 1 + X^4 + X^5$ und $p_2(X) = 1 + X^2 + X^3 + X^4$,

(b) $p_3(X) = 1 + X^3 + X^5 + X^7$ und $p_4(X) = 1 + X + X^4 + X^5$.

Bestimmen Sie in $\mathbb{Z}_2[X]$ außerdem $p_1(X) \cdot p_2(X) \pmod{X^4 + X + 1}$ und $p_3(X) \cdot p_4(X) \pmod{X^4 + X + 1}$.