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

4. Übungsblatt für die Übungen vom 16.5.-20.5.2017

Ringe, Polynomringe, Teilbarkeit

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

V27. **Vorbereitungsaufgabe: Bitte bereiten Sie diese Aufgabe zur Übung vor.**
Wir betrachten in dieser Aufgabe, für eine natürliche Zahl $n \in \mathbb{N}$, die Menge

$$R_n = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} \;\middle|\; a, b \in \mathbb{Z}_n \right\}$$

zusammen mit der üblichen Matrizenaddition und -multiplikation in $\mathbb{Z}_n$.

(a) Zeigen Sie, dass (für alle $n \in \mathbb{N}$) $(R_n, +, \cdot)$ ein Ring ist. Wie viele Elemente besitzt R_n?

(b) Geben Sie, für $n = 3$ und für $n = 4$, alle Nullteiler und alle Einheiten von R_n an.

(c) Finden Sie einen nichttrivialen Unterring (d.h. mit mehr als zwei und weniger als $\#R_n$ Elementen) von R_n.

Ü28. Berechnen Sie die Menge der 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 $p_4(x) = 1 + x + x^4 + x^5$.

Hinweis: Der ggT zweier Polynome kann - analog zur Berechnung des ggT zweier natürlicher Zahlen - mit dem Euklidischen Algorithmus durch fortgesetzte Division mit Rest (s. VL II.2.7) gefunden werden.

Ü29. (a) Sei R ein endlicher Ring. Zeigen Sie, dass jedes von Null verschiedene Element von R entweder Nullteiler oder Einheit ist. Folgern Sie, dass jeder endliche nullteilerfreie Ring bereits ein Körper ist.

(b) Es sei R ein Ring der Charakteristik $p \in \mathbb{P}$. Zeigen Sie, dass dann für alle $a, b \in R$ gilt

$$(a + b)^p = a^p + b^p.$$

Folgern Sie: Die Abbildung $x \mapsto x^p$ ist ein Ringendomorphismus von R.

Ü30. (a) Zeigen Sie, dass die Menge der Gaußschen Zahlen $\mathbb{Z}[\mathrm{i}] = \{a + \mathrm{i}b \mid a, b \in \mathbb{Z}\}$ mit der üblichen Addition und Multiplikation einen Unterring von $\mathbb{C}$ bildet.

(b) Bestimmen Sie alle Nullteiler und alle Einheiten von $\mathbb{Z}[\mathrm{i}]$.

Hinweis: Sie können zur Bestimmung der Einheiten das Quadrat der Norm $|a + bi|^2 = a^2 + b^2$ verwenden.

(c) Zeigen Sie: $7 \in \mathbb{Z}[i]$ ist irreduzibel, aber $5 \in \mathbb{Z}[i]$ ist reduzibel.

(d) Zeigen Sie: Gilt $a^2 + b^2 = p$ für eine Primzahl p, dann ist $a + bi$ irreduzibel.

(e) Zeigen Sie: $1 + i | a + bi \iff a \equiv b \pmod 2$.

Hinweis: Damit ist „jede zweite“ Zahl in $\mathbb{Z}[i]$ ein Vielfaches von $1 + i$.

Bitte wählen Sie 2 der folgenden 3 Hausaufgaben zur Abgabe aus.

A31. **Hausaufgabe, bitte bis zum 24.5.2017, 12:00 Uhr im entsprechenden Briefkasten im C-Flügel unter Angabe von Name, Matrikelnr. und Übungsgruppe abgeben.**

Betrachtet wird die Potenzmenge $R := \mathfrak{P}(M)$ der dreielementigen Menge $M = \{a, b, c\}$. Zeigen Sie, dass R mit den Operationen

$$A + B := A \triangle B = (A \cup B) \setminus (A \cap B), \quad A \cdot B := A \cap B \qquad \text{für alle } A, B \in R$$

einen endlichen kommutativen Ring bildet. Geben Sie das Einselement an. Bestimmen Sie alle Einheiten und alle Nullteiler in diesem Ring.

A32. **Hausaufgabe, bitte bis zum 24.5.2017, 12:00 Uhr im entsprechenden Briefkasten im C-Flügel unter Angabe von Name, Matrikelnr. und Übungsgruppe abgeben.**

(a) Beweisen Sie Bemerkung II.2.2 aus der Vorlesung: Ist R ein Ring, dann ist auch $R[X]$ ein Ring (der Polynomring über R).

(b) Beweisen Sie Beispiel II.2.12 aus der Vorlesung: $R[X_1, X_2] \cong (R[X_1])[X_2]$.

A33. **Hausaufgabe, bitte bis zum 24.5.2017, 12:00 Uhr im entsprechenden Briefkasten im C-Flügel unter Angabe von Name, Matrikelnr. und Übungsgruppe abgeben.**

Sei R ein Ring und $f \in R[X]$, dann bezeichnen wir mit $\tilde{f} : R \to R$, $r \mapsto f(r)$ die übliche Polynomfunktion zu f.

(a) Zeigen Sie: Ist R nullteilerfrei und unendlich, dann ist die Abbildung $\Phi : R[X] \to Abb(R, R) : f \mapsto \tilde{f}$ injektiv.

(b) Finden Sie ein Gegenbeispiel über $\mathbb{F}_p$, d.h. finden Sie zwei Polynome $f \neq g \in \mathbb{F}_p[X]$ mit $\tilde{f} = \tilde{g}$.

(c)* Finden Sie ein Gegenbeispiel über einem nullteilerbehafteten und unendlichen Ring.

H34. Es sei $\mathbb{K}$ ein Körper. Beweisen Sie, dass in $\mathbb{K}[X]$ gilt: $x^m - 1 | x^n - 1 \iff m | n$. Schlussfolgern Sie, dass für jede natürliche Zahl $a > 1$ gilt: $a^m - 1 | a^n - 1 \iff m | n$

H35. Beweisen Sie Lemma II.1.11 aus der Vorlesung:

Sind $f : R \to S$ und $g : S \to T$ Ringhomomorphismen, dann ist auch $g \circ f : R \to T$ ein Ringhomomorphismus. Ist $f : R \to S$ ein Ringisomorphismus, dann ist auch $f^{-1} : S \to R$ ein Ringisomorphismus.

H36*. (a) Beweisen Sie das *allgemeine Assoziativitätsgesetz*: Die Produkte von $n \geq 3$ Elementen in einer Gruppe hängen nicht von der Wahl der Klammerung ab.

(b) Beweisen Sie das *allgemeine Kommutativitätsgesetz*: Sind die Elemente $a_1, \dots, a_n$ einer Gruppe $(H, \cdot)$ paarweise vertauschbar, so gilt

$$a_1 \cdot a_2 \cdot \ldots \cdot a_n = a_{\pi(1)} \cdot a_{\pi(2)} \cdot \ldots \cdot a_{\pi(n)}$$

für jede Permutation $\pi \in S_n := S_{\{1,\dots,n\}}$.