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

6. Übungsblatt für die Übungen vom 12.6.-16.6.2017

faktorielle Ringe, Hauptidealringe, Euklidische Ringe

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

V47. **Vorbereitungsaufgabe: Bitte bereiten Sie diese Aufgabe zur Übung vor.**
Zeigen Sie, dass die Elemente $2, 3, 1+\sqrt{-5}, 1-\sqrt{-5}$ irreduzibel im Ring $\mathbb{Z}[\sqrt{-5}]$ (siehe Aufgabe Ü38) sind und dass keine zwei von ihnen assoziiert sind. Ist $\mathbb{Z}[\sqrt{-5}]$ ein faktorieller Ring?

Ü48. Betrachtet wird der Ring der Gaußschen Zahlen (siehe Ü30) $\mathbb{Z}[\mathrm{i}] = \{a + \mathrm{i}b \mid a, b \in \mathbb{Z}\}$.

(a) Bestimmen Sie alle Primteiler der Zahl $p = 2$ in $\mathbb{Z}[\mathrm{i}]$.

(b) Berechnen Sie alle größten gemeinsamen Teiler von $a = 1 + 3\mathrm{i}$ und $b = 3 + 4\mathrm{i}$ in $\mathbb{Z}[\mathrm{i}]$.

(c) Zeigen Sie, dass $\mathbb{Z}[i]$ (bzgl. des Normquadrats $\delta(z) = |z|^2$) ein Euklidischer Ring ist.

Ü49. Zeigen Sie, dass $\mathbb{Z}[X]$ kein Hauptidealring ist, indem Sie zeigen, dass das Ideal $(X, 2) \trianglelefteq \mathbb{Z}[X]$ nicht von einem Element erzeugt wird.

Ü50. (a) Berechnen Sie den größten gemeinsamen Teiler $h(X)$ der Polynome

$$f(X) = X^5 + X^4 + X^3 + 1 \text{ und } g(X) = X^4 + X^2 + 1$$

in $\mathbb{F}_2[X]$ und stellen Sie diesen als Linearkombination von $f(X)$ und $g(X)$ dar.

(b) Es sei $I := (X^4 + X^3 + 1)$ ein Ideal im Polynomring $\mathbb{F}_2[X]$. Bestimmen Sie im Faktorring $\mathbb{F}_2[X]/I$ das multiplikative Inverse, falls existent, zum Element $a(X) + I$ mit $a(X) = X^6 + X + 1$.

A51. **Hausaufgabe nur für Lehramtsstudierende,**
bitte bis zum 21.6.2017, 12:00 Uhr im entsprechenden Briefkasten im C-Flügel unter Angabe von Name, Matrikelnr. und Übungsgruppe abgeben.
Berechnen Sie, falls existent, das multiplikative Inverse zu $2X+1+(X^3-2)$ im Faktorring $K[X]/(X^3-2)$ für die Fälle $K = \mathbb{Q}$, $K = \mathbb{F}_5$ und $K = \mathbb{F}_7$

A52. **Hausaufgabe für Bachelor- und Lehramts-Studierende,**
bitte bis zum 21.6.2017, 12:00 Uhr im entsprechenden Briefkasten im C-Flügel unter Angabe von Name, Matrikelnr. und Übungsgruppe abgeben.

(a) Sei R ein faktorieller Ring. Zeigen Sie die folgenden Aussagen:

(i) Für je zwei Elemente aus R existiert ein ggT.

(ii) Für je zwei Elemente aus R existiert ein kgV.

(b) Beweisen Sie: In einem nullteilerfreien Ring R gilt $k = \mathrm{kgV}(a, b) \iff Ra \cap Rb = Rk$.

A53. **Hausaufgabe nur für Bachelor-Studierende,**
bitte bis zum 21.6.2017, 12:00 Uhr im entsprechenden Briefkasten im C-Flügel unter Angabe von Name, Matrikelnr. und Übungsgruppe abgeben.
Für eine Primzahl p sei $\mathbb{Z}_{(p)} := \{\frac{a}{b} \mid p \nmid b\} \subseteq \mathbb{Q}$ (siehe Vorlesung II.8.8) die Menge der rationalen Zahlen, in deren Bruchdarstellung der Nenner nicht durch p teilbar ist.

(a) Bestimmen Sie die Einheiten und Primelemente von $\mathbb{Z}_{(p)}$.

(b) Zeigen Sie, dass $\mathbb{Z}_{(p)}$ ein faktorieller Ring ist.

(c) Zeigen Sie, dass $\mathbb{Z}_{(p)}$ ein Euklidischer Ring ist.

H54. Der Ring $\mathbb{Z}[\sqrt{-5}]$ ist nach Ü38 kein Hauptidealring. Zeigen Sie, dass aber jedes Ideal durch 2 Elemente erzeugt wird.

H55. Es sei K ein Körper. Zeigen Sie, dass der Ring $K[X, Y]$ aller Polynome über X und Y mit Koeffizienten aus K kein Hauptidealring ist.

H56*. Diese Aufgabe führt durch den Beweis eines Satzes von Fermat, der sagt:

Eine ungerade Primzahl p ist genau dann Summe zweier Quadrate, also $p = a^2 + b^2$, wenn sie von der Form $p = 4n + 1$ ist. (a, b, n sind natürliche Zahlen).

Zeigen Sie dazu die folgenden Aussagen:

(a) Ist $p = 4n + 3$, dann existiert keine Darstellung $p = a^2 + b^2$.

(b) Erinnern Sie sich daran, dass (siehe Ü48) der Ring der Gaußschen Zahlen $\mathbb{Z}[i]$ Euklidisch ist.

(c) Gilt $cp = a^2 + b^2$ für $a, b, c, p \in \mathbb{Z}$ und p prim und $p \nmid c$, dann ist p reduzibel in $\mathbb{Z}[i]$. Schließen Sie, dass p die Summe zweier Quadrate ist.

(d) Gilt $p = 4n + 1$ mit $n \in \mathbb{Z}$ und p prim, dann existieren (siehe H44) $a, b, c \in \mathbb{Z}$ mit $cp = a^2 + b^2$. Schlussfolgern Sie das Theorem.