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

5. Übungsblatt für die Übungen vom 29.5.-2.6.2017

Ideale, Einheitengruppen

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

V37. **Vorbereitungsaufgabe: Bitte bereiten Sie diese Aufgabe zur Übung vor.**

(a) Berechnen Sie zu den folgenden natürlichen Zahlen n den Wert $\varphi(n)$ der Eulerschen Funktion.

(i) $n = 30$, (ii) $n = 60$, (iii) $n = 100$, (iv) $n = 2520$.

(b) Beweisen Sie: Gilt $n = pq$ für zwei Primzahlen $p \neq q$, dann folgt $\phi(n) = (p-1)(q-1)$.

(c) Finden Sie alle natürlichen Zahlen $n \in \mathbb{N}$, für die gilt:

(i) $\varphi(n) = 2$, (ii) $\varphi(n) = 3$, (iii) $\varphi(n) = 4$, (iv) $\varphi(n) = 6$.

(d) Berechnen Sie die folgenden Potenzen. Benutzen Sie den Satz von Euler, falls möglich:

(i) $19^{289} \pmod{21}$, (ii) $13^{54} \pmod{32}$, (iii) $7^{27} \pmod{36}$, (iv) $15^{13} \pmod{18}$.

Ü38. (a) Geben Sie das von 10 und 14 erzeugte Ideal I des Ringes $\mathbb{Z}$ an. Ist I ein Hauptideal (wenn ja, von welchem Element wird es erzeugt)? Ist der zugehörige Faktorring $\mathbb{Z}/I$ isomorph zum Ring $\mathbb{Z}_n$ für ein geeignetes n? Wenn ja, begründen Sie warum und geben Sie dieses n an.

(b) Bestimmen Sie im Ring $\mathbb{Z}[\sqrt{-5}\,] := \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ das kleinste Ideal J, das die Zahlen 2 und $1 + \sqrt{-5}$ enthält.

Erwartet wird Angabe $J = \{x + y\sqrt{-5} \mid \text{...Bedingung für } x, y\text{...}\}$ und Begründung.

(c) Zeigen Sie, dass J kein Hauptideal von $\mathbb{Z}[\sqrt{-5}\,]$ ist und beschreiben Sie den Faktorring $\mathbb{Z}[\sqrt{-5}\,]/J$.

Ü39. Lösen Sie folgende Systeme von Kongruenzen:

(a)
$$\begin{aligned} x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 2 \pmod{7} \end{aligned}$$

(b)
$$\begin{aligned} x &\equiv 4 \pmod{5} \\ x &\equiv 6 \pmod{7} \\ x &\equiv 9 \pmod{11} \end{aligned}$$

Führen Sie jeweils die Probe durch!

Ü40. (a) Verifizieren Sie, dass die Gruppe $(\mathbb{Z}/15\mathbb{Z})^\times$ nicht zyklisch ist.

(b) Zeigen Sie: Sind $p \neq q$ ungerade Primzahlen, dann ist $(\mathbb{Z}/pq\mathbb{Z})^\times$ nicht zyklisch.

(c) Bestimmen Sie alle n, für die $(\mathbb{Z}/n\mathbb{Z})^\times$ zyklisch ist.

A41. **Hausaufgabe nur für Lehramtsstudierende,**
bitte bis zum 7.6.2017, 12:00 Uhr im entsprechenden Briefkasten im C-Flügel unter Angabe von Name, Matrikelnr. und Übungsgruppe abgeben.
Schreiben Sie Ihre Matrikelnummer auf. Die (von links gelesen) 5. Ziffer sei die Zahl a, die 6. Ziffer b und die 7. Ziffer c.

Bestimmen Sie die Lösungen des Kongruenzensystems

$$\begin{aligned} x &\equiv a \pmod 5 \\ x &\equiv b \pmod 6 \\ x &\equiv c \pmod 7 \end{aligned}$$

A42. **Hausaufgabe für Bachelor- und Lehramts-Studierende,**
bitte bis zum 7.6.2017, 12:00 Uhr im entsprechenden Briefkasten im C-Flügel unter Angabe von Name, Matrikelnr. und Übungsgruppe abgeben.
Betrachten Sie den Ring $\mathbb{Q}[X]$. Beweisen Sie, dass für $S \subseteq \mathbb{C}$ die Menge

$$I(S) \ := \ \{f \in \mathbb{Q}[X] \mid \forall x \in S : \ f(x) = 0\}$$

ein Ideal ist.

Für welche der folgenden Mengen S_i ist $I(S_i)$ ein Primideal?

- $S_1 \ := \ \{3, 7\}$
- $S_2 \ := \ \{7 + 3i, 7 - 3i\}$
- $S_3 \ := \ \{\sqrt[3]{2}, -\sqrt[3]{2}\}$
- $S_4 \ := \ \{\sqrt{2}, -\sqrt{2}\}$

A43. **Hausaufgabe nur für Bachelor-Studierende,**
bitte bis zum 7.6.2017, 12:00 Uhr im entsprechenden Briefkasten im C-Flügel unter Angabe von Name, Matrikelnr. und Übungsgruppe abgeben.
Es seien $a, b \in \mathbb{N}$ und $p > 3$ eine Primzahl. Zeigen Sie, dass das Kongruenzensystem

$$\begin{aligned} x &\equiv a \pmod{2p} \\ x &\equiv b \pmod{3p} \end{aligned}$$

genau dann eine Lösung hat, wenn $a \equiv b \pmod p$ gilt. Finden Sie (in Abhängigkeit von a, b, p) die Lösungsmenge dieses Systems.

H44. Zeigen Sie: Ist p eine ungerade Primzahl, dann ist die Gleichung $x^2 \equiv -1 \pmod p$ genau dann lösbar, wenn $p \equiv 1 \pmod 4$ gilt.

H45. (a) Es sei $\mathbb{F}_3$ der Körper mit drei Elementen. Betrachten Sie $\mathbb{F}_3^2$ als ringtheoretisches Produkt sowie als $\mathbb{F}_3$-Vektorraum. Bestimmen Sie alle Ideale, Unterringe und Untervektorräume.

(b) Es sei nun K ein beliebiger Körper. Betrachten Sie $K^2 = K \times K$ als ringtheoretisches Produkt sowie als K-Vektorraum. Vergleichen Sie die Begriffe Ideal, Unterring und Untervektorraum in diesem Ring.

H46. Für fast alle natürlichen Zahlen $n > 1$ gilt $\phi(n) \geq \sqrt{n}$. Beweisen Sie diese Aussage und finden Sie die beiden Ausnahmen.

Hinweis: Betrachten Sie die Aussage zunächst für quadratfreie Zahlen, d.h. für solche Zahlen $n \in \mathbb{N}$, die nicht durch ein Quadrat $m^2 \in \mathbb{N} \setminus \{1\}$ teilbar sind.