

## Übungsaufgaben zur Linearen Algebra IIa

- (1+1+3 Punkte) Im folgenden können Sie den Begriff eines Integritätsrings (mit oder ohne Einselement) und die Begriffe *Ideal* und *Hauptideal* als bekannt voraussetzen.
  - Definieren Sie, was ein *Euklidischer Ring* ist.
  - Definieren Sie, was ein *Hauptidealring* ist.
  - Beweisen Sie, dass jeder Euklidische Ring ein Hauptidealring ist.

- (2 Punkte) Nach Definition ist  $\mathbb{Z}_m^* = \{a \in \mathbb{Z}_m \mid \exists b \in \mathbb{Z}_m \text{ mit } a \cdot_m b = 1\}$ . Beweisen Sie

$$\mathbb{Z}_m^* = \{a \in \mathbb{Z}_m \mid \text{ggT}(a, m) = 1\}.$$

Hinweis: Sie dürfen ohne Beweis benutzen, dass es für  $b, c \in \mathbb{Z}$  Zahlen  $\lambda_1, \lambda_2 \in \mathbb{Z}$  mit  $\text{ggT}(b, c) = \lambda_1 b + \lambda_2 c$  gibt. (Es folgt elegant mit dem Euklidischen Algorithmus. Es folgt noch eleganter daraus, dass  $\mathbb{Z}$  ein Hauptidealring ist.)

- (2+1,5+1,5 Punkte) Die *Eulersche  $\varphi$ -Funktion*  $\varphi : \mathbb{N} \rightarrow \mathbb{N}$  ist durch

$$\varphi(m) := |\mathbb{Z}_m^*|$$

definiert.

- Sei  $p$  eine Primzahl, und sei  $l \in \mathbb{N}$ . Zeigen Sie

$$\varphi(p^l) = (p-1)p^{l-1}.$$

Hinweis: Man kann die Menge  $\mathbb{Z}_{p^l} - \mathbb{Z}_{p^l}^*$  anders charakterisieren, so dass die Behauptung praktisch sofort daraus folgt. Wie?

- Bemerkung (Beweis später): Bei  $a, b \in \mathbb{N}$  mit  $\text{ggT}(a, b) = 1$  gilt

$$\varphi(ab) = \varphi(a)\varphi(b).$$

Daraus und aus (a) und mit der (eindeutigen) Primfaktorzerlegung für natürliche Zahlen kann man  $\varphi(n)$  für nicht zu großes  $n$  leicht berechnen. Geben Sie in einer Tabelle für

$$n \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20\}$$

die Werte  $n$  und  $\varphi(n)$  an. Begründungen sind nicht nötig (Kopfrechnen!).

- Bemerkung:  $\mathbb{Z}_m^*$  ist mit der Multiplikation eine Gruppe (Lemma 10.7 (a)). Listen Sie in einer Tabelle die Elemente der Gruppe  $\mathbb{Z}_{28}^*$  und ihre Inversen auf.

4. (4 Punkte) **Definition:** Sei  $m \in \mathbb{N}$ . Das  $m$ -te Kreisteilungspolynom  $\Phi_m(x)$  ist definiert durch

$$\Phi_m = \Phi_m(x) := \prod_{a \in \mathbb{Z}_m^*} (x - e^{2\pi ia/m}) \in \mathbb{C}[x].$$

**Satz:**

(a)  $\deg \Phi_m = \varphi(m)$ , und  $\Phi_m$  ist unitär.

(b)

$$x^m - 1 = \prod_{d \in \mathbb{N}: d|m} \Phi_d.$$

(c)  $\Phi_m \in \mathbb{Z}[x]$ .

(d)  $\Phi_m$  ist in  $\mathbb{Z}[x]$  und in  $\mathbb{Q}[x]$  irreduzibel.

(a) ist klar. (b) ist ziemlich klar. (c) folgt relativ leicht mit dem folgenden Satz. (d) ist schwer. Sie sollen (b) und den folgenden Satz im Fall  $R = \mathbb{Z}$  anwenden, um einige Kreisteilungspolynome auszurechnen. Diese Rechnungen werden Ihnen eine Idee geben, wie man (induktiv) (c) beweist. Aber der Beweis von (c) ist nicht Teil der Aufgabe.

**Satz:** Sei  $R$  ein Integritätsring mit 1, und seien  $f(x)$  und  $g(x)$  in  $R[x] - \{0\}$  mit  $g(x)$  unitär (d.h. Leitkoeffizient = 1). Dann gibt es eindeutige  $q(x), r(x) \in R[x]$  mit  $\deg r(x) < \deg g(x)$  und  $f(x) = q(x) \cdot g(x) + r(x)$ . (Gegenüber der Division mit Rest in  $K[x]$  ist hier nur neu, dass die Koeffizienten in  $R$  bleiben und man nie dividieren muss. Das liegt daran, dass  $g(x)$  unitär ist.)

**Beispiele:** (i)  $m = 3$ :  $x^3 - 1 = \Phi_1 \cdot \Phi_3$ . Offenbar ist  $\Phi_1 = x - 1$ . Daher ist

$$\Phi_3 = \frac{x^3 - 1}{x - 1} = x^2 + x + 1.$$

(ii)  $m = 9$ :  $x^9 - 1 = \Phi_1 \cdot \Phi_3 \cdot \Phi_9 = (x^3 - 1) \cdot \Phi_9$ . Daher und wegen (i) ist

$$\Phi_9 = \frac{x^9 - 1}{x^3 - 1} = x^6 + x^3 + 1.$$

Hier ist es offenbar besser, durch  $x^3 - 1 = \Phi_1 \cdot \Phi_3$  zu teilen, statt hintereinander durch  $\Phi_1$  und  $\Phi_3$ .

Berechnen Sie in ähnlicher Weise

$$\Phi_2, \Phi_4, \Phi_8, \Phi_{27}, \Phi_5, \Phi_{15}, \Phi_6, \Phi_{12}.$$

(Die Berechnung von  $\Phi_{15}$  ist am schwersten.)

**Abgabe bis Montag, den 24. Februar 2020, um 11:50 Uhr im Kasten Ihrer Gruppe im Eingangsbereich des C-Teils des Gebäudes in A5**