8. Übung zur Algebra

Prof. M. Geck, Dr. L. Iancu, WiSe 2023/2024

Aufgabe 1. (V) Sei $m \geq 2$ und $G = (\mathbb{Z}/m\mathbb{Z})^\times$ die Einheitengruppe des Ringes $\mathbb{Z}/m\mathbb{Z}$. Nach dem Hauptsatz über endliche abelsche Gruppe (Satz 10.7) ist also G isomorph zu einem direkten Produkt von zyklischen Gruppen von Primzahlpotenzordnung. Zum Beispiel ist $G = \langle \bar{2} \rangle \cong \mathbb{Z}/2\mathbb{Z}$ für $m = 3$ und $G = \langle \bar{3} \rangle \cong \mathbb{Z}/2\mathbb{Z}$ für $m = 4$. Finden Sie drei verschiedene Werte für m, so dass G nicht zyklisch ist.

Aufgabe 2. (V) Sei $(R, +, \cdot)$ ein kommutativer Ring mit 1; es gelte $R \neq \{0\}$. Zeigen Sie:

(a) Ist R ein Integritätsring und $|R| < \infty$, so ist R ein Körper.
(*Hinweis:* Für $0 \neq a \in R$ betrachte die Abbildung $f\colon R \to R$, $x \mapsto ax$.)

(b) R ist ein Körper $\iff$ $\{0\}$ und R sind die einzigen Ideale von R.

Aufgabe 3. (V) Sei $(R, +, \cdot)$ ein kommutativer Ring mit 1.

(a) Sei $n \in \mathbb{N}$ und $a_1, \ldots, a_n \in R$; zeigen Sie dass die Teilmenge

$$I = (a_1, \ldots, a_n) := \{r_1 \cdot a_1 + \ldots + r_n \cdot a_n \mid r_j \in R \text{ für alle } j\} \subseteq R$$

ein Ideal von R ist ; es gilt $a_j \in I$ für alle j. (Im Fall $n = 1$ ist $I = (a_1)$ ein Hauptideal.)

(b) Sei $R = \mathbb{Z}[i\sqrt{5}] = \{n + mi\sqrt{5} \mid n, m \in \mathbb{Z}\} \subseteq \mathbb{C}$ und sei $I = (2, 1 + i\sqrt{5}) \subseteq R$ (nach (a) ist I ein Ideal). Zeigen Sie : Es gilt

$$I = \{n + mi\sqrt{5} \mid n, m \in \mathbb{Z} \text{ mit } n \equiv m \bmod 2\} \subsetneqq R \qquad \text{und} \qquad |R/I| = 2\,;$$

geben Sie explizit Repräsentanten für die beiden Elemente in R/I an. Ist I ein Hauptideal?

Aufgabe 4. (V) Sei R kommutativer Ring mit 1. Ein Ideal $I \neq R$ heißt Primideal, wenn folgende Bedingung für alle $a, b \in R$ gilt: Ist $ab \in I$, so gilt $a \in I$ oder $b \in I$.

(a) Zeigen Sie: I ist ein Primideal genau dann, wenn R/I ein Integritätsing ist.

(b) Die Primideale von $\mathbb{Z}$ sind: $\{0\}$ und die Ideale (p) mit p Primzahl.

(c) Wir betrachten den Ring $R = \mathbb{Z}[X]$. Zeigen Sie:

(i) Ist $p \in \mathbb{Z}$ eine Primzahl, so ist das Hauptideal $(p) = \{fp \mid f \in \mathbb{Z}[X]\}$ auch ein Primideal in $\mathbb{Z}[X]$.
(ii) Das Ideal $(2, X)$ ist ein Primideal in $\mathbb{Z}[X]$, aber kein Hauptideal.
(iii) Das Ideal $(2, X^2 + 1)$ ist kein Primideal in $\mathbb{Z}[X]$.

Aufgabe 5. (Schriftlich, 15=3+3+3+2+2+2 Punkte)
Wir betrachten den Gaußschen Zahlring $\mathbb{Z}[i] = \{n + mi \mid n, m \in \mathbb{Z}\} \subseteq \mathbb{C}$.

(a) Zeigen Sie, dass $\mathbb{Z}[i]$ ein Euklidischer Ring ist mit zugehöriger Funktion $\delta\colon \mathbb{Z}[i] \to \mathbb{N}_0$ gegeben durch $\delta(n + mi) = (n + mi)(n - mi) = n^2 + m^2$ für $x, y \in \mathbb{Z}$.

[*Hinweis:* Seien $\alpha, \beta \in \mathbb{Z}[i]$ mit $\beta \neq 0$. Um $q, r \in \mathbb{Z}[i]$ zu finden mit $\alpha = q\beta + r$, schreibe $\alpha\beta^{-1} \in \mathbb{C}$ als $a + ib$ mit $a, b \in \mathbb{Q}$. Dann setze $q := n + mi$ wobei n, m die ganzen Zahlen sind, die am nächsten an a bzw. b liegen, d.h., $|a - n| \leq 1/2$ und $|b - m| \leq 1/2$. Schließlich setze $r := \alpha - q\beta$.]

(b) Finden Sie in $\mathbb{Z}[i]$ einen größten gemeinsamen Teiler von 45 und $11 - 2i$.

(c) Zeigen Sie: Ist $\delta(z) \in \mathbb{N}$ eine Primzahl, so ist z irreduzibel in $\mathbb{Z}[i]$. Zum Beispiel ist $z = 1 - i$ irreduzibel.

(d) Sei $p \in \mathbb{N}$ eine Primzahl. Zeigen Sie: p ist reduzibel in $\mathbb{Z}[i] \Leftrightarrow p = a^2 + b^2$ mit $a, b \in \mathbb{Z}$.

(e) Zeigen Sie: Ist p eine Primzahl und $p \equiv 3 \bmod 4$, so ist p irreduzibel in $\mathbb{Z}[i]$.

(f) Finden Sie in $\mathbb{Z}[i]$ eine Zerlegung von $z = 356440$ in irreduzible Faktoren.

Aufgabe 6. (Z) In der Vorlesung wird gezeigt (Satz 12.2), dass der Polynomring über einem Körper ein Euklidischer Ring ist, und damit auch ein Hauptidealring. Ziel dieser Aufgabe ist, eine Umkehrung dieser Aussage zu zeigen. Sei also R ein Integritätsring und $R[X]$ der Polynomring über R.

(a) Sei $0 \neq a \in R$ und betrachten Sie das Ideal $I_a := \{af + Xg \mid f, g \in R[X]\} \subseteq R[X]$. Zeigen Sie: Ist I_a ein Hauptideal, so ist $a \in R^\times$ und $I_a = R[X]$.

(*Hinweis*: Sei $I_a = (d)$ mit einem $d \in R[X]$. Nun ist $a \in I_a$, also $d \mid a$; außerdem $X \in I_a$, also $d \mid X$.)

(b) Zeigen Sie: Ist $R[X]$ ein Hauptidealring, so muss R ein Körper sein. — Insbesondere zeigt dies noch einmal, dass $\mathbb{Z}[X]$ kein Hauptidealring ist.

Abgabe der schriftlichen Aufgaben: Am 11./12. Dezember, vor den Übungsgruppen.