8. Übung zur Algebra

Dr. L. Iancu, WiSe 2020

Aufgabe 1. Betrachten Sie den Gaußschen Zahlring

$$\mathbb{Z}[i] = \{x + yi \mid x, y \in \mathbb{Z}\}.$$

(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 $\delta(x + yi) = (x + yi)(x - yi) = x^2 + y^2$ 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 $q := x + iy$ wobei x, y die ganzen Zahlen sind, die am nächsten an a bzw. b liegen, d.h., $|a - x| \leq 1/2$ und $|b - y| \leq 1/2$. Schließlich setze $r := \alpha - q\beta$.]

(b) Finden Sie in $\mathbb{Z}[i]$ einen größten gemeinsamen Teiler von 60 und $8 + i$. Wenden Sie dazu auf $a = 60$ und $b = 8 + i$ eine analoge Version des erweiterten Euklidischen Algorithmus an (siehe Beweis von Bézouts Lemma).

(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.

Zum Selbststudium:

(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 $z = 5940$ in irreduzible Faktoren.

Aufgabe 2. (Schriftlich 6 Punkte) Sei 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 $I_a = R[X]$.

(b) Zeigen Sie: Ist $R[X]$ ein Hauptidealring, so ist R ein Körper.

Aufgabe 3. (Schriftlich, 9 Punkte) Für eine Primzahl p sei $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ der Körper mit p Elementen. Sei $\mathbb{F}_p[X]$ der Polynomring über $\mathbb{F}_p$.

(a) Zeigen Sie: Es gibt genau $\frac{1}{2}p(p-1)$ normierte, irreduzible Polynome $f \in \mathbb{F}_p[X]$ vom Grad 2.

(b) Für $p = 2, 3$, bestimmen Sie alle irreduziblen Polynome in $\mathbb{F}_p[X]$ vom Grad ≤ 4.

Bemerkung: Wir werden später in der Vorlesung zeigen, dass es zu jedem $n \geq 1$ mindestens ein irreduzibles Polynom $f \in \mathbb{F}_p[X]$ mit $\mathrm{Grad}(f) = n$ gibt. (Dies ist nicht selbstverständlich!)

Aufgabe 4. Sei R ein kommutativer Ring mit 1. Ein Ideal $I \trianglelefteq R$ heißt **maximales Ideal**, wenn $I \neq R$ gilt und es kein Ideal $J \trianglelefteq R$ mit $I \subsetneqq J \subsetneqq R$ gibt.

(a) Sei $I \trianglelefteq R$ ein Ideal. Zeigen Sie: I ist ein maximales Ideal $\Leftrightarrow$ R/I ist ein Körper.

(b) Bestimmen Sie alle maximalen Ideale in $R = \mathbb{Z}$.

(c) Sei $R = \mathbb{Z}[X]$ und $p \in \mathbb{N}$ eine Primzahl. Zeigen Sie, dass $I = \{pf + Xg \mid f, g \in \mathbb{Z}[X]\}$ ein maximales Ideal ist mit $\mathbb{Z}[X]/I \cong \mathbb{Z}/p\mathbb{Z}$.

(d) **(Selbststudium)** Bestimmen Sie alle maximalen Ideale in $R = \mathbb{Z}[X]$.

Abgabe der schriftlichen Aufgaben: Bis Mittwoch, den 13.01., vor den Übungsgruppen.