

Blatt 10

Aufgabe 40 (6 Punkte). Sei $f(X) \in \mathbf{Z}[X]$ irreduzibel und von Grad ≥ 1 , und sei $\alpha \in \mathbf{C}$ mit $f(\alpha) = 0$ gegeben.

- (1) Zeige, daß $\mathbf{Q}[X]/(f(X)) \simeq \text{Quot}(\mathbf{Z}[X]/(f(X)))$.
- (2) Zeige, daß $\mathbf{Q}[X]/(f(X)) \simeq \mathbf{Q}[\alpha] = \mathbf{Q}(\alpha)$.
- (3) Zeige, daß $\mathbf{Z}[X]/(f(X)) \simeq \mathbf{Z}[\alpha]$.

Aufgabe 41 (9 Punkte). Entscheide, ob R ein Hauptidealbereich ist. Entscheide, ob R faktoriell ist.

- (1) $R = \mathbf{Z}[i]$. (Hinweis: $\delta(a + bi) = a^2 + b^2$.)
- (2) $R = \mathbf{Z}[\zeta_3]$ mit $\zeta_3 := -\frac{1}{2} + \frac{i}{2}\sqrt{3}$.
- (3) $R = \mathbf{Z}[\sqrt{-13}]$.

Aufgabe 42 (4 Punkte). Sei R ein Hauptidealbereich. Zeige, daß für jedes Primideal \mathfrak{p} in $R[X]$ eine der Aussagen (i), (ii) oder (iii) zutrifft. Falls R unendlich viele Primideale enthält, entscheide, welchenfalls \mathfrak{p} ein maximales Ideal ist.

- (i) Es ist $\boxed{\mathfrak{p} = 0}$.
- (ii) Es gibt ein Primelement $g(X) \in R[X] \setminus \{0\}$ mit $\boxed{\mathfrak{p} = (g(X))}$.
- (iii) Es gibt ein Primelement $p \in R \setminus \{0\}$ und ein $h(X) \in R[X]$ normiert von Grad ≥ 1 , welches ein irreduzibles Bild in $(R/(p))[X]$ hat, derart, daß $\boxed{\mathfrak{p} = (p, h(X))}$.

(Hinweis: Sei $(a_m) := \{a \in R \mid \text{es gibt ein Polynom in } \mathfrak{p} \setminus \{0\} \text{ von Grad } m \text{ mit Leitkoeffizient } a\} \cup \{0\}$. Sei n der minimale in $\mathfrak{p} \setminus \{0\}$ auftretende Grad, und $g_n(X) \in \mathfrak{p} \setminus \{0\}$ von Grad n mit Leitkoeffizient a_n . Falls \mathfrak{p} kein Primelement aus $R \setminus \{0\}$ enthält, so zeige zunächst $g_n(X)$ irreduzibel, und dann $\mathfrak{p} = (g_n(X))$.)

Aufgabe 43 (10 Punkte). Entscheide, welche der folgenden Ideale prim sind.

- (1) $(X^{12} + 55X^7 + 125X^3 - 505X + 5) \subseteq \mathbf{Z}[X]$.
- (2) $(X^2 + 30X + 125) \subseteq \mathbf{Z}[X]$.
- (3) $(X^5 - X^4 + X^3 + X^2 + 2X + 1) \subseteq \mathbf{Z}[X]$ (Hinweis: Substitution, dann Eisenstein für $p = 3$).
- (4) $(X^2 - Y, X - Y^2) \subseteq \mathbf{Q}[X, Y]$.
- (5) $(X^2 - Y, X - Y^2 - 1) \subseteq \mathbf{Q}[X, Y]$.

Aufgabe 44 (6 Punkte). Zeige oder widerlege.

- (1) Sei R ein faktorieller Ring, und seien $x, y \in R \setminus \{0\}$. Es ist $(\text{ggT}(x, y)) = (x, y)$.
- (2) Sei $f(X) \in \mathbf{Z}[X]$ normiert, und sei $p \in \mathbf{Z}_{>0}$ prim. Ist sein Bild $\overline{f(X)} \in \mathbf{F}_p[X]$ irreduzibel, so auch $f(X)$ selbst.
- (3) Sei $f(X) = aX^k + \dots + b \in \mathbf{Z}[X]$, wobei $a \neq 0$, $k \geq 1$, und sei $\frac{m}{n} \in \mathbf{Q}$ mit $f(\frac{m}{n}) = 0$, wobei $m, n \in \mathbf{Z}$ teilerfremd seien. Dann gilt $n|a$ und $m|b$.
- (4) Sei R ein Hauptidealbereich, aber kein Körper, und sei $g(X) \in R[X]$ irreduzibel. Es ist $R[X]/(g(X))$ kein Körper.
- (5) Sei $f(X) \in \mathbf{Z}[X]$ irreduzibel. Es ist $\mathbf{Z}[X]/(f(X)) \longrightarrow \mathbf{Q}[X]/(f(X))$, $\bar{X} \longmapsto \bar{X}$ injektiv.
- (6) Sei $p \geq 3$ prim. Es gibt ein $a \in \mathbf{Z}$ mit $a^{(p-1)/2} \equiv_p -1$.