Lösung 5

Faktorielle Ringe, Primelemente

1. (**SAGE**): Plotten Sie alle Primelemente p in $\mathbb{Z}[i]$ mit $p = a + ib$, $-20 \leqslant a, b \leqslant 20$.

   Hinweis: Nutzen Sie Symmetrien aus. Schlagen Sie die Befehle

   ```
   QuadraticField(n), .maximal_order()
   ```

   im Sage-Handbuch nach. Sie müssen den zweiten Befehl nicht wirklich verstehen. Das folgende Code-Snippet könnte hilfreich sein.

   ```
   K.<i>=QuadraticField(-1)
   R=K.maximal_order()
   R(5).is_prime()
   ```

2. Sei R ein Hauptidealring. Zeigen Sie, dass $a, b \in R \setminus \{0\}$ koprim als Elemente von R sind, genau dann, wenn $(a), (b)$ koprim als Ideale von R sind.

3. Sei K ein Körper. Zeigen Sie, dass $R = K[X^2, X^3] \subset K[X]$ ein Integritätsbereich, aber nicht faktoriell ist.

4. Sei R ein Integritätsbereich und seien $a, b \in R$. Wir nennen $d \in R$ ein *kleinstes gemeinsames Vielfaches* von a und b und schreiben $d \sim \mathrm{kgV}(a, b)$, falls

   $$a|d \quad \wedge \quad b|d \quad \wedge \quad \forall c \in R : (a|c \wedge b|c \;\Rightarrow\; d|c)$$

   gilt. Zeige:

   (a) Falls $\mathrm{kgV}(a, b)$ existiert, ist es bis auf Einheiten eindeutig bestimmt.

   (b) Existiert $\mathrm{kgV}(a, b)$, so existiert auch $\mathrm{kgV}(ac, bc)$ für jedes $c \in R$ und es gilt

   $$\mathrm{kgV}(ac, bc) \sim c \cdot \mathrm{kgV}(a, b).$$

   (c) Falls R faktoriell ist, existiert $\mathrm{kgV}(a, b)$ und es gilt

   $$\mathrm{ggT}(a, b) \cdot \mathrm{kgV}(a, b) \sim a \cdot b.$$

   (d) Ist R ein Hauptidealring, dann gilt $(a) \cap (b) = (d)$, wobei $d \sim \mathrm{kgV}(a, b)$.

5. Seien K ein Körper und $f \in K[X]$ ein Polynom von ungeradem Grad. Zeigen Sie, dass
$$Y^2 + Y + f \in K[X, Y]$$
irreduzibel ist.

Hinweis: Betrachten Sie $Y^2 + Y + f$ als Element von $R[Y]$ für $R := K[X]$.

Lösung: Wir betrachten $p := Y^2 + Y + f$ als Element von $R[Y]$ für $R := K[X]$. Nimm an, es gebe eine Faktorzerlegung $p = a \cdot b$ mit Nicht-Einheiten $a, b \in R[Y]$. Schreibe
$$a = \alpha Y^i + \text{ kleinere Terme in } Y,$$
$$b = \beta Y^j + \text{ kleinere Terme in } Y$$
mit $\alpha, \beta \in R \setminus \{0\}$. Dann gilt $\alpha\beta Y^{i+j} = Y^2$, also $\alpha\beta = 1$ und $i + j = 2$. Somit sind $\alpha, \beta \in R^\times = K[X]^\times = K^\times$, siehe Aufgabe 3 in Serie 2. Wegen $a, b \notin R[Y]^\times = R^\times$ (da $R = K[X]$ Integritätsbereich) müssen dann $i, j > 0$ sein, also $i = j = 1$. Schreibe $a = \alpha Y + \gamma$ mit $\gamma \in R$ und setze $\delta := -\alpha^{-1}\gamma \in R$. Dann ist δ eine Nullstelle von a. Somit ist es auch eine Nullstelle von p, das heisst, es gilt $\delta^2 + \delta + f = 0$. Also ist $\deg_X(f) = \deg_X(-\delta^2 - \delta) = 2 \cdot \deg_X(\delta)$ gerade, im Widerspruch zur Annahme.

6. Sei R ein kommutativer Ring. Zeigen Sie, dass jedes Ideal in R endlich erzeugt ist, genau dann, wenn jede aufsteigende Kette $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ von Idealen in R stationär wird, d.h. es existiert $n_0 \in \mathbb{N}$ mit $I_n = I_{n_0}$ für alle $n \geqslant n_0$.

Lösung: Wir zeigen zuerst, wenn jedes Ideal in R endlich erzeugt ist, dann wird jede aufsteigende Kette von Idealen in R stationär. Sei dazu $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ eine aufsteigende Ketten von Idealen in R. Dann ist $J := \bigcup_{k=1}^{\infty} I_k$ ein Ideal in R (siehe Vorlesung). Nach Voraussetzung ist J endlich erzeugt, das heisst es existieren $b_1, \ldots, b_l \in J$ such that $J = (b_1, \ldots, b_l)$. Nun ist J nach Konstruktion die Vereinigung der I_k, das heisst es existiert $n_0 \in \mathbb{N}$ so dass $\{b_1, \ldots, b_l\} \subset I_{n_0}$. Es folgt, dass $I_{n_0} = (b_1, \ldots, b_l)$ und damit auch $I_n = I_{n_0}$ für alle $n \geqslant n_0$, was zu zeigen war.

Sei umgekehrt J ein Ideal in R und wir nehmen an, dass J nicht endlich erzeugt ist. Für jede endliche Teilmenge $\{a_1, \ldots, a_n\} \subset J$ für $n \in \mathbb{N}$ ist das davon erzeugte Ideal nicht gleich J. Sei nun a_1 in J beliebig. Da $(a_1) \neq J$ (J ist nicht endlich erzeugt) gibt es $a_2 \in J \setminus (a_1)$. Nun ist auch $(a_1, a_2) \neq J$ und wir finden $a_3 \in J \setminus (a_1, a_2)$. Diesen Prozess können wir iterieren und wir erhalten eine aufsteigende Kette von Idealen in R
$$(a_1) \subseteq (a_1, a_2) \subseteq (a_1, a_2, a_3) \subseteq \ldots$$
die nicht stationär wird (J hat unendlich viele Elemente). Dies ist ein Widerspruch.