Serie 6

Irreduzibilität in Polynomringe, Elementarteiler, Moduln

Erinnerung: ** bedeutet: Geht über den Standardstoff hinaus. Besprechen Sie Ihre Lösung mit Prof. Pink.

1. Zeige, dass die folgenden Polynome irreduzibel sind:

   (a) $\frac{1}{3}X^3 + \frac{5}{2}X^2 + 3X - 1 \in \mathbb{Q}[X]$

   (b) $X^3 + 8iX^2 - 6X - 1 + 3i \in \mathbb{Z}[i][X]$

   Hinweis: Benutze Serie 5, Aufgabe 1. (c).

   (c) $X^\ell + Y^m + Z^n \in \mathbb{C}[X, Y, Z]$ für beliebige $\ell, m, n \geqslant 1$.

2. (a) *Lagrange-Interpolation:* Sei K ein Körper und seien $a_0, \ldots, a_m \in K$ paarweise verschieden. Zeige, dass es für alle $b_0, \ldots, b_m \in K$ genau ein Polynom $f \in K[X]$ vom Grad $\leqslant m$ mit $f(a_i) = b_i$ für alle $0 \leqslant i \leqslant m$ gibt.

   Hinweis: Benutze die Vandermondsche Determinante oder betrachte für $0 \leqslant i \leqslant m$ die Polynome
   $$\prod_{\substack{j=0 \\ j\neq i}}^{m} \frac{X - a_j}{a_i - a_j}.$$

   (b) Zerlege $X^5 + X^4 + 1 \in \mathbb{Z}[X]$ in Primfaktoren mit folgendem Verfahren.

   Explizite Primfaktorzerlegung nach Kronecker: Sei $f \in \mathbb{Z}[X]$ ein primitives Polynom vom Grad n. Wir nehmen an, f habe eine (noch unbekannte) Faktorisierung $f = g \cdot h$ mit $g, h \in \mathbb{Z}[X]$ und $m := \deg(g) \leqslant \frac{n}{2}$. Um diese zu finden, wählen wir irgendwelche paarweise verschiedene $a_0, \ldots, a_m \in \mathbb{Z}$. Dann muss $g(a_i) | f(a_i)$ in $\mathbb{Z}$ für alle i gelten. Falls $f(a_i) = 0$ für ein i ist, kann $X - a_i$ von f abgespaltet werden und mit $\frac{f}{X - a_i}$ weiter gearbeitet werden. Andernfalls hat $f(a_i)$ für jedes i nur endlich viele Teiler in $\mathbb{Z}$. Für jedes System von Teilern $b_i | f(a_i)$ liefert (a) höchstens einen Kandidaten für g in $\mathbb{Z}[X]$ mit $g(a_i) = b_i$, für den man testet, ob er f teilt.

   *(c) Beschreibe einen analogen Algorithmus für Polynome in beliebig vielen Variablen über $\mathbb{Z}$.

3. Finde die Elementarteiler und die zugehörigen Matrizen U, V für die Matrix
$$A := \begin{pmatrix} 4 & 7 \\ 5 & 8 \\ 6 & 9 \end{pmatrix} \in \mathbb{Z}^{3\times 2}.$$

4. Für jede natürliche Zahl ℓ und jede $(m \times n)$-Matrix A über einem Hauptidealring R sei $d_\ell(A)$ der grösste gemeinsame Teiler aller $(\ell \times \ell)$-Unterdeterminanten von A. Zeige, dass für alle Matrizen $U \in \mathrm{GL}_m(R)$ und $V \in \mathrm{GL}_n(R)$ gilt $d_\ell(UAV) \sim d_\ell(A)$. Folgere, dass die Elementarteiler von A bis auf Assoziiertheit eindeutig bestimmt sind.

5. Zeige: Für alle $n \geqslant 1$ und $a_1, \ldots, a_n$ in einem Hauptidealring R sind äquivalent:
   (a) $\mathrm{ggT}(a_1, \ldots, a_n) \sim 1$.
   (b) Es existiert eine Matrix in $\mathrm{GL}_n(R)$ mit erster Spalte $(a_1, \ldots, a_n)^T$.

**6. Zeige oder widerlege für jedes n: Jede Matrix in $\mathrm{GL}_n(\mathbb{Z})$ ist ein Produkt von Matrizen der Form
   (a) Diagonalmatrizen mit Diagonaleinträgen ± 1,
   (b) Permutationsmatrizen, oder
   (c) Dreiecksmatrizen mit Diagonaleinträgen 1, einem weiteren Eintrag ± 1, und allen übrigen Einträgen 0.

7. Beweise: Für jeden Homomorphismus $\varphi\colon M \to N$ von Moduln über einem Ring R gilt:
   (a) $\mathrm{Kern}(\varphi) := \{m \in M \mid \varphi(m) = 0\}$ ist ein Untermodul von M.
   (b) $\mathrm{Bild}(\varphi)$ ist ein Untermodul von N.
   (c) φ ist injektiv genau dann, wenn $\mathrm{Kern}(\varphi) = 0$ ist.
   (d) φ ist surjektiv genau dann, wenn $\mathrm{Bild}(\varphi) = N$ ist.
   (e) Beweise den Homomorphiesatz für Moduln: Jeder Homomorphismus $\varphi\colon M \to N$ von R-Moduln induziert einen Isomorphismus von R-Moduln
$$M/\mathrm{Kern}(\varphi) \xrightarrow{\sim} \mathrm{Bild}(\varphi),\ m + \mathrm{Kern}(\varphi) \mapsto \varphi(m).$$

**8. Sei R ein Ring. Zeige:
   (a) $(\mathbb{Z}/m\mathbb{Z}) \otimes_{\mathbb{Z}} (\mathbb{Z}/n\mathbb{Z}) \cong (\mathbb{Z}/\mathrm{ggT}(m,n)\mathbb{Z})$ für alle $m, n \in \mathbb{Z}^{\geqslant 0}$.
   (b) Seien M und N freie R-Moduln vom Rang r bzw. s. Dann ist $M \otimes_R N$ ein freier Modul vom Rang rs.
   (c) Sei $n \in \mathbb{Z}^{\geqslant 0}$. Dann gilt:
$$\mathbb{Z}/n\mathbb{Z} \otimes_{\mathbb{Z}} \mathbb{Q} \cong \begin{cases} 0, & \text{wenn } n \neq 0 \text{ ist,} \\ \mathbb{Q}, & \text{wenn } n = 0 \text{ ist.} \end{cases}$$