D-MATH Algebra I HS 2022
Prof. Richard Pink

Serie 14

Polynomringe, Irreduzibilitätskriterien

1. Bestimme den verallgemeinerten Inhalt der folgenden Polynome:
   (a) $f(X) := \frac{1}{2}X^3 - 3X^2 + 2X - \frac{1}{3} \in \mathbb{Q}[X]$ bezüglich $R = \mathbb{Z}$.
   (b) $g(X) := \frac{1}{4}X^3 - \frac{1}{7}X^2 + \frac{1}{6}X - \frac{1}{2} \in \mathbb{Q}[X]$ bezüglich $R = \mathbb{Z}$.
   (c) $h(X) := (Y^2 + 3)^2X + Y^4 - 9 \in \mathbb{Q}(Y)[X]$ bezüglich $R = \mathbb{Q}(Y)$.

2. Sei R ein faktorieller Ring mit Quotientenkörper K. Zeige: Ist $f \in K[X]$ normiert, so ist $I(f) \sim \frac{1}{r}$ für ein $r \in R \smallsetminus \{0\}$.

3. Bestimme alle irreduziblen Polynome vom Grad $\leqslant 5$ in $\mathbb{F}_2[X]$.

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

5. Zeige, dass die folgenden Polynome irreduzibel sind:
   (a) $f(X) := X^3 - 3X^2 + 2X - 3 \in \mathbb{Q}[X]$
   (b) $g(X) := 7X^3 - X^2 + 4X - 2 \in \mathbb{Q}[X]$
   (c) $h(X) := X^5 + 4X^2 + 14X + 40 \in \mathbb{Q}[X]$

6. 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) $X^3 + 8iX^2 - 6X - 1 + 3i \in \mathbb{Z}[i][X]$. (Benutze Aufgabe 2 von Serie 13.)
   (c) $X^\ell + Y^m + Z^n \in \mathbb{C}[X, Y, Z]$ für beliebige $\ell, m, n \geqslant 1$.

7. (a) *Lagrange-Interpolation:* Sei K ein Körper, seien $a_0, \ldots, a_m \in K$ paarweise verschieden, und seien $b_0, \ldots, b_m \in K$ beliebig. Zeige, dass es genau ein Polynom $f \in K[X]$ vom Grad $\leqslant m$ gibt mit $f(a_i) = b_i$ für alle $0 \leqslant i \leqslant m$.
   Hinweis: Benutze die Vandermondesche Determinante oder betrachte für alle $0 \leqslant i \leqslant m$ 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 $\mathbb{Z}$.