D-MATH Algebra I HS20
Prof. Manfred Einsiedler

Serie 7

Irreduzibilität

1. Sei R ein faktorieller Ring und $f, g \in R[X]$, $f, g \neq 0$. Zeigen Sie, dass $f \mid g$ in $R[X]$ genau dann, wenn $I(f) \mid I(g)$ und $f \mid g$ in $K[X]$, wobei $K = \mathrm{Quot}(R)$.

2. Zeigen Sie, 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: Schreiben Sie $-1 + 3i$ als Produkt von Primelementen aus $\mathbb{Z}[i]$.

3. Faktorisieren Sie die folgenden Polynome in irreduzible Faktoren.

   (a) $X^3 + X + 1$ in $\mathbb{F}_p[X]$, für $p = 2, 3, 5$

   (b) $X^3 + 2X^2 - 3X - 3$ in $\mathbb{Q}[X]$

   (c) $X^4 + X + 1$ in $\mathbb{Q}[X]$

4. Zeigen Sie, dass die folgenden Polynome irreduzibel sind.

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

   (b) $7X^3 - X^2 + 4X - 2 \in \mathbb{Q}[X]$

   (c) $X^5 + 4X^2 + 14X + 40 \in \mathbb{Q}[X]$

   Hinweis: Sie dürfen SAGE verwenden, um geeignete Primzahlen und Faktorisierungen in $\mathbb{F}_p[X]$ zu finden. Ihren Beweis müssen Sie aber ohne SAGE formulieren.

5. Zeigen Sie, dass das Polynom $X^4 + 1 \in \mathbb{Z}[X]$ irreduzibel in $\mathbb{Z}[X]$, aber reduzibel in $\mathbb{F}_p[X]$ für alle Primzahlen $p \in \mathbb{N}$ ist.

   Hinweis: Sie dürfen ohne Beweis die folgenden zwei Aussagen benutzen:

   - -1 ist ein Quadrat in $\mathbb{F}_p$ genau dann, wenn $p = 2$ oder $p \equiv 1 \bmod 4$.
   - Ist $p \equiv 3 \bmod 4$, so ist 2 ein Quadrat oder -2 ein Quadrat in $\mathbb{F}_p$.

6. (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. Zeigen Sie, 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: Benutzen Sie die Vandermondesche Determinante oder betrachten Sie 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) Zerlegen Sie $X^5 + X^4 + 1 \in \mathbb{Z}[X]$ 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) (**SAGE**) Implementieren Sie die explizite Primfaktorzerlegung nach Kronecker aus (b) in SAGE. Nutzen Sie Ihre Methode, um Ihr Ergebnis aus (b) zu überprüfen.