Lösung 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 $\mathbb{F}_p$.

   Lösung: Wir zeigen zuerst, dass $X^4 + 1$ irreduzibel über $\mathbb{Z}$ ist. Wir erkennen, dass wir $X^4 + 1$ aufgefasst als Polynom in $\mathbb{R}[X]$ zerlegen können als

$$X^4 + 1 = (X^2 - \sqrt{2}X + 1)(X^2 + \sqrt{2}X + 1),$$

mit $X^2 - \sqrt{2}X + 1$ und $X^2 + \sqrt{2}X + 1$ irreduzibel (keine weiteren Nullstellen in $\mathbb{R}$). Wir bemerken, dass $\pm\sqrt{2} \notin \mathbb{Q}$.

Angenommen es gäbe eine Zerlegung $X^4 + 1 = p_1 \cdots p_n$ mit p_i irreduzibel und normiert in $\mathbb{Q}[X]$. Nun fassen wir diese Zerlegung über $\mathbb{R}$ auf (da $\mathbb{Q}[X] \subset \mathbb{R}[X]$). Nun müssen die p_i nicht mehr unbedingt irreduzibel sein, aber nach der eindeutigen Primfaktorzerlegung müssen sie aus Produkten von $X^2 - \sqrt{2}X + 1$ und $X^2 + \sqrt{2}X + 1$ bestehen. Dies kann aber nur sein, wenn $i = 1$ ist. Also ist $X^4 + 1$ irreduzibel über $\mathbb{Q}$ und damit auch über $\mathbb{Z}$.

Um zu zeigen, dass $X^4 + 1$ reduzibel über $\mathbb{F}_p$ ist, nehmen wir an, dass $X^4 + 1 = fg$ mit $f, g \in \mathbb{F}_p[X]$. Wir machen den Ansatz $f = X^2 + aX + b$, $g = X^2 + cX + d$ und multiplizieren

$$(X^2 + aX + b)(X^2 + cX + d) = X^4 + (a + c)X^3 + (b + d + ac)X^2 + (ad + bc)X + bd.$$

Wir sehen direkt, dass $c = -a$ und $d = b^{-1}$ und wir vereinfachen zu

$$X^4 + 1 = X^4 + (b + b^{-1} - a^2)X^2 + a(b^{-1} - b)X + 1.$$

Daraus folgt $b + b^{-1} - a^2 = 0$ und $a(b^{-1} - b) = 0$. Wir unterscheiden zwei Fälle:

1. Fall $a = 0$: Dann folgt $b + b^{-1} = 0$ aus der ersten Gleichheit, also $b^2 = -1$.

2. Fall $a \neq 0$: Nun folgt aus der zweiten Gleichheit, dass $b^{-1} - b = 0$, also $b = \pm 1$. Aus der ersten Gleichheit folgt damit $a^2 = \pm 2$.

Nun verwenden wir den Hinweis. Ist $p = 2$ oder $p \equiv 1 \bmod 4$, so ist -1 ein Quadrat in $\mathbb{F}_p$, das heisst es existiert $\tilde{b} \in \mathbb{F}_p$ mit $\tilde{b}^2 = -1$. Dann faktorisiert das Polynom $X^4 + 1$ über $\mathbb{F}_p$ als

$$X^4 + 1 = (X^2 + \tilde{b})(X^2 - \tilde{b}),$$

ist also nicht irreduzibel.

Ist nun $p \equiv 3 \bmod 4$, so ist entweder 2 oder -2 ein Quadrat in $\mathbb{F}_p$, das heisst es existiert $a \in \mathbb{F}_p$ mit $\widetilde{a_\pm}^2 = \pm 2$. Wir sind nun im zweiten Fall und setzen $b = \pm 1$. Angenommen 2 ist ein Quadrat, dann faktorisiert das Polynom $X^4 + 1$ über $\mathbb{F}_p$ als

$$X^4 + 1 = (X^2 + \widetilde{a_+}X + 1)(X^2 - \widetilde{a_+}X + 1),$$

ist also nicht irreduzibel. Angenommen -2 ist ein Quadrat, dann faktorisiert das Polynom $X^4 + 1$ über $\mathbb{F}_p$ als

$$X^4 + 1 = (X^2 + \widetilde{a_-}X - 1)(X^2 - \widetilde{a_-}X - 1),$$

ist also nicht irreduzibel.

Nun ist jede Primzahl p entweder gerade, oder kongruent $1 \bmod 4$ oder kongruent $3 \bmod 4$, das heisst wir haben gezeigt, dass $X^4 + 1$ reduzibel über $\mathbb{F}_p$ ist für alle Primzahlen 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.

Lösung:

(a) Sei P_m der K-Vektorraum aller Polynome $f \in K[X]$ mit $\deg(f) \leqslant m$. Betrachte die K-lineare Abbildung

$$\alpha : \begin{array}{ccc} P_m & \longrightarrow & K^{m+1} \\ f & \longmapsto & (f(a_0), \ldots, f(a_m)) \end{array}.$$

Die Matrix von α bezüglich der Basis $\{1, X, X^2, \ldots, X^m\}$ von P_m und der Standardbasis von K^{m+1} ist

$$A = \begin{pmatrix} 1 & a_0 & \cdots & a_0^m \\ 1 & a_1 & \cdots & a_1^m \\ & & \vdots & \\ 1 & a_m & \cdots & a_m^m \end{pmatrix}.$$

Die Determinante von A ist genau die Vandermondesche Determinante und daher gleich $\prod_{0 \leqslant i < j \leqslant m} (a_j - a_i)$. Hier sind alle Faktoren ungleich Null, da $a_0, \ldots, a_m$ paarweise verschieden sind. Somit ist $\det(A) \neq 0$ und α ein Isomorphismus, das heisst, bijektiv. Für jede Wahl von $b_0, \ldots, b_m \in K$ existiert daher genau ein Polynom $f \in P_m$ mit $f(a_i) = b_i$ für alle $0 \leqslant i \leqslant m$.

Aliter: Für jedes $0 \leqslant i \leqslant m$ betrachte das Polynom

$$f_i(X) := \prod_{\substack{j=0 \\ j \neq i}}^{m} \frac{X - a_j}{a_i - a_j} \in K[X]$$

vom Grad m. Dieses erfüllt $f_i(a_i) = 1$ und $f_i(a_j) = 0$ für $j \neq i$. Für beliebige $b_0, \ldots, b_m \in K$ ist daher

$$f := b_0 f_0 + \cdots b_m f_m \in K[X]$$

ein Polynom vom Grad $\leqslant m$ mit $f(a_i) = b_i$ für alle $0 \leqslant i \leqslant m$.

Falls $g \in K[X]$ ein zweites Polynom vom Grad $\leqslant m$ mit $f(a_i) = b_i$ für alle i ist, hat $f - g$ mindestens die $m+1$ Nullstellen $a_0, \ldots, a_m \in K$. Dies ist wegen $\deg(f - g) \leqslant m$ nur für $f - g = 0$ möglich. Somit ist f eindeutig.

(b) Als normiertes Polynom hat $f(X) := X^5 + X^4 + 1 \in \mathbb{Z}[X]$ eine Primfaktorzerlegung in normierte Polynome. Daher suchen wir nur normierte Teiler von f.

Wir prüfen zuerst nach, ob f einen normierten Teiler $g(X) := X - a$ vom Grad 1 hat, was äquivalent zur Existenz einer Nullstelle $a \in \mathbb{Z}$ von f ist. Für einen solchen Teiler g müsste $a = g(0) \mid f(0) = 1$, also $a = \pm 1$ gelten. Jedoch sind 1 und -1 keine Nullstellen von f. Somit hat f keine Teiler vom Grad 1.

Nun suchen wir normierte Teiler $g(X) := X^2 + aX + b$ vom Grad 2 von f. Wir wählen $a_0 := -1$, $a_1 := 0$ und $a_2 := 1$. Wegen $g(a_i) \mid f(a_i)$ für $i = 0, 1, 2$ muss dann $g(-1) \in \{\pm 1\}$ und $g(1) \in \{\pm 1, \pm 3\}$ und $b = g(0) \in \{\pm 1\}$ gelten. Aus Letzterem und dem Ansatz für g folgt

$$g(-1) + g(1) = 2 + 2b \in \{0, 4\}.$$

Daher bleiben nur die Möglichkeiten

$$(g(-1), g(0), g(1)) = (g(-1), b, g(1)) = (-1, -1, 1), (1, -1, -1), (1, 1, 3).$$

Diese ergeben für g die Kandidaten $X^2 + X - 1$, $X^2 - X - 1$ und $X^2 + X + 1$. Mit Polynomdivision prüft man nach, dass davon nur $X^2 + X + 1$ ein Teiler von f ist und

$$f(X) = (X^2 + X + 1)(X^3 - X + 1)$$

gilt. Da f keine Teiler vom Grad 1 hat, können die in dieser Zerlegung auftretenden Faktoren nicht weiter zerlegt werden. Somit haben wir eine Primfaktorzerlegung von f gefunden.

(c) Eine mögliche Implementierung könnte wie folgt aussehen.

```
def find_factor(f):      #diese Funktion findet einen
   Faktor des Polynoms f
    d = f.degree()
    if d==0 or d==1:
        return f
    R = f.parent()
    S = R.change_ring(QQ)
    X = R.gen()
    m = d//2
    for a in range(m+1):
        if f(a)==0:      #a ist Nullstelle
            return X-a
    div = [divisors(f(a)) +
       list((-1)*vector(divisors(f(a)))) for a in
       range(m+1)]
    counter = [len(div[a])-1 for a in range(m+1)]
    counter_zero = [0 for a in range(m+1)]
    while counter != counter_zero:
        points = [(a,div[a][counter[a]]) for a in
           range(m+1)] #(Punkt,Wert)-Paare
        L = S.lagrange_polynomial(points)
        if L.degree()!=0:
            if f%L==0: #Test ob L ein Teiler ist
                return L
        for a in range(m+1):
            if counter[a]!=0:
                counter[a] = counter[a]-1
                break
            else:
                counter[a]=len(div[a])-1
    return f

def kronecker_factorization(f):
    if f.degree()==1 or f.degree()==0:
        return [f]
    factors = []
    g = find_factor(f)
    if g==f:
        return [f]
    h = f//g
    factors = factors + kronecker_factorization(g) +
       kronecker_factorization(h) #wiederhole den
```

```
        Aufruf fuer g und h
    return factors

R.<x> = PolynomialRing(ZZ)
f = x^5+x^4+1
kronecker_factorization(f)
```