D-MATH Algebra I HS 2022
Prof. Richard Pink

Musterlösung 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 $R = \mathbb{Q}(Y)$.

   Lösung: Es gilt

   $$I(f) \sim \tfrac{1}{6} \cdot I(3X^3 - 18X^2 + 12X - 2) \sim \tfrac{1}{6} \cdot \mathrm{ggT}(3, 18, 12, 2) \sim \tfrac{1}{6},$$
   $$I(g) \sim \tfrac{1}{84} \cdot I(21X^3 - 12X^2 + 14X - 42) \sim \tfrac{1}{84} \cdot \mathrm{ggT}(21, 12, 14, 42) \sim \tfrac{1}{84}$$

   Sodann gilt $(Y^4 - 9) = (Y^2 - 3)(Y^2 + 3)$ und daher

   $$h(X) = (Y^2+3) \cdot \big((Y^2+3)X + (Y^2-3)\big).$$

   Wegen $(Y^2 + 3) - (Y^2 - 3) = 6 \in R^\times$ sind $Y^2 + 3$ und $Y^2 - 3$ teilerfremd, und daraus folgt

   $$I(h) \sim (Y^2+3) \cdot \mathrm{ggT}(Y^2+3, Y^2-3) \sim Y^2 + 3.$$

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 $r \in R \smallsetminus \{0\}$.

   Lösung: Schreibe $f = \sum_{i=0}^{n} \frac{a_i}{b_i} X^n$ für $n \in \mathbb{Z}_{\geqslant 0}$ und Koeffizienten $a_0, \ldots, a_n \in R$ und $b_0, \ldots, b_n \in R \smallsetminus \{0\}$ mit $\mathrm{ggT}(a_i, b_i) \sim 1$. Setze ausserdem $r := \mathrm{kgV}(b_0, \ldots, b_n)$. Wir wollen zeigen, dass rf primitiv ist, woraus dann mit $I(f) \sim \frac{1}{r} I(rf) \sim \frac{1}{r}$ die Aussage folgt.

   Zunächst ist r ein Vielfaches jedes b_i und somit ist $rf \in R[X]$. Da f normiert ist, ist r der führende Koeffizient von rf. Deswegen ist r ein Vielfaches von $I(rf)$. Sei $r = u \prod_{i \in I} p_i^{\mu_i}$ eine Primfaktorzerlegung mit $\mu_i \geqslant 1$ für alle $i \in I$. Da r als kleinstes gemeinsames Vielfaches von $b_0, \ldots, b_n$ definiert ist, existiert für jedes $i \in I$ ein $1 \leqslant j \leqslant n$, sodass $p_j^{\mu_i} | b_j$ ist. Der j-te Koeffizient von rf ist gegeben durch $\frac{a_j r}{b_j}$ und wird nicht von p_j geteilt, da a_j und b_j teilerfremd sind. Somit gibt es keinen Primfaktor, der $I(rf)$ teilt, somit ist rf primitiv.

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

   Lösung:

   - Als lineare Polynome sind X und $X+1 \in \mathbb{F}_2[X]$ irreduzibel.
   - Ein Polynom vom Grad 2 oder 3 über einem Körper K ist genau dann irreduzibel, wenn es keinen Faktor vom Grad 1, also keine Nullstelle in K hat. In unserem Fall sind dies genau die Polynome X^2+X+1 und X^3+X^2+1 und X^3+X+1.
   - Ein Polynom $f \in \mathbb{F}_2[X]$ vom Grad 4 oder 5 ist genau dann irreduzibel, wenn es keinen Faktor vom Grad 1 hat und es nicht Produkt von irreduziblen Polynomen vom Grad 2 oder 3 ist. Deshalb sind genau die Polynome vom Grad 4 und 5 irreduzibel, die keine Nullstellen in $\mathbb{F}_2$ haben und nicht gleich

   $$\begin{aligned} X^4+X^2+1 &= (X^2+X+1)^2, \\ X^5+X+1 &= (X^2+X+1)(X^3+X^2+1), \\ X^5+X^4+1 &= (X^2+X+1)(X^3+X+1) \end{aligned}$$

   sind. Nachrechnen liefert folgende irreduzible Polynome:

   $$\begin{array}{lll} X^4+X^3+X^2+X+1 & X^5+X^4+X^3+X^2+1 & X^5+X^3+1 \\ X^4+X^3+1 & X^5+X^4+X^3+X+1 & X^5+X^2+1 \\ X^4+X+1 & X^5+X^4+X^2+X+1 & \\ & X^5+X^3+X^2+X+1 & \end{array}$$

   Insgesamt gibt es somit 14 irreduzible 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.

   Lösung: Wir betrachten $p := Y^2+Y+f$ als Element von $R[Y]$ für $R := K[X]$. Nimm an, es gebe eine Faktorzerlegung $f = a \cdot b$ mit Nicht-Einheiten $a, b \in R[Y]$. Schreibe

   $$\begin{aligned} a &= \alpha Y^i + \text{ kleinere Terme in } Y, \\ b &= \beta Y^j + \text{ kleinere Terme in } Y \end{aligned}$$

   mit $\alpha, \beta \in R \smallsetminus \{0\}$. Dann gilt $\alpha\beta Y^{i+j} = Y^2$, also $\alpha\beta = 1$ und $i+j = 2$. Somit sind $\alpha, \beta \in R^\times = K[X]^\times = K^\times$. Wegen $a, b \notin R[Y]^\times$ 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 $Y = \delta$ 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.

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

   Lösung: Alle genannten Polynome liegen in $\mathbb{Z}[X]$ und sind primitiv; also sind sie irreduzibel in $\mathbb{Q}[X]$ genau dann, wenn sie irreduzibel in $\mathbb{Z}[X]$ sind.

   (a) Das Polynom $f(X) = X^3 - 3X^2 + 2X - 3$ ist in $\mathbb{Q}[X]$ irreduzibel, da seine Reduktion $X^3 + X^2 + 1$ modulo 2 auch Grad 3 hat und irreduzibel in $\mathbb{F}_2[X]$ ist.

   (b) Das Polynom $g(X) = 7X^3 - X^2 + 4X - 2$ hat die Reduktion $X^3 + 2X^2 + X + 1$ modulo 3. Letztere hat ebenfalls Grad 3 und keine Nullstelle in $\mathbb{F}_3$. Daher ist sie irreduzibel in $\mathbb{F}_3[X]$. Somit ist g in $\mathbb{Q}[X]$ irreduzibel.

   (c) Die Reduktion von $h(X)$ modulo 2 ist X^5 und nützt uns nichts. Die Reduktion modulo 3 hat die Faktorisierung in irreduzible $(X^3+2X+1)(X^2+1)$. Also ist h entweder irreduzibel, oder es ist ein Produkt von irreduziblen Polynomen der Grade 2 und 3. Die Reduktion modulo 5 hat die Faktorisierung in irreduzible $(X^4 + 4X + 4)X$. Also ist der zweite Fall nicht möglich, und h ist irreduzibel. *Aliter:* Die Reduktion von $h(X)$ modulo 7 ist irreduzibel vom selben Grad; also ist h irreduzibel.

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 $\ell, m, n \geqslant 1$.

   Lösung:

   (a) Sei $f(X) := \frac{1}{3}X^3 + \frac{5}{2}X^2 + 3X - 1$. Da 6 eine Einheit in $\mathbb{Q}$ ist, ist

   $$f(X) \;\sim\; 6f(X) \;=\; 2X^3 + 15X^2 + 18X - 6$$

   und es genügt zu zeigen, dass dieses irreduzibel ist. Dieses erfüllt die Voraussetzungen im Eisenstein-Kriterium für das Primelement $3 \in \mathbb{Z}$ und ist folglich irreduzibel in $\mathbb{Z}[X]$. Daher ist es und damit f auch irreduzibel in $\mathbb{Q}[X]$.

   (b) Nach Aufgabe 2 von Serie 13 ist $\mathbb{Z}[i]$ faktoriell und $-1 + 3i = (1 + i)(1 + 2i)$ eine Zerlegung in zueinander nicht assoziierte Primelemente von $\mathbb{Z}[i]$. Daher gilt $(1+i) \mid (-1+3i)$ und $(1+i)^2 \nmid (-1+3i)$. Ausserdem ist $2 = (1+i)(1-i)$ und damit $1 + i$ auch einTeiler von $8i$ und -6. Somit erfüllt das Polynom $X^3 + 8iX^2 - 6X - 1 + 3i$ die Bedingungen des Eisenstein-Kriteriums für das Primelement $p = 1 + i$ in $\mathbb{Z}[i][X]$ und ist daher irreduzibel.

(c) Als Element von $\mathbb{C}[Y,Z][X]$ ist das Polynom $F := X^\ell + Y^m + Z^n$ normiert und daher primitiv, und sein konstanter Koeffizient ist $G := Y^m + Z^n \in \mathbb{C}[Y,Z]$. Wir behaupten, dass G einen irreduziblen Faktor $P \in \mathbb{C}[Y,Z]$ der Multiplizität 1 besitzt. Für diesen erfüllt F das Eisensteinkriterium und ist daher irreduzibel. Um P zu finden, betrachten wir G als Element von $\mathbb{C}[Z][Y]$. Als solches ist es normiert und folglich ein Produkt von normierten irreduziblen Polynomen in $\mathbb{C}[Z][Y]$. Schreibe also $G = \prod_i P_i^{\mu_i}$ mit paarweise verschiedenen normierten irreduziblen Polynomen $P_i \in \mathbb{C}[Z][Y]$ mit $\deg_Y(P_i) \geqslant 1$ und Exponenten $\mu_i \geqslant 1$. Einsetzen von $Z = 1$ liefert dann $Y^m + 1 = \prod_i P_i(Y,1)^{\mu_i}$ mit normierten Polynomen $P_i(Y,1)$ vom Grad $\geqslant 1$ in $\mathbb{C}[Y]$. Aber das Polynom $Y^m + 1$ hat keine mehrfachen Nullstellen in $\mathbb{C}$. Deshalb müssen alle $\mu_i = 1$ sein, und jedes P_i hat die gewünschte Eigenschaft.

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 $\mathbb{Z}$.

Lösung:

(a) Sei P_m der K-Vektorraum alles Polynome $f \in K[X]$ vom Grad $\leqslant m$ und betrachte die K-lineare Abbildung
$$\alpha \colon P_m \longrightarrow K^{m+1}, \quad f \longmapsto (f(a_0), \ldots, f(a_m)).$$

Die Darstellungsmatrix 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. F'ur 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) Siehe van der Waerden, Algebra I, §32.