Musterlösung 5

Euklidische Ringe, Polynomringe, Irreduzibilität in Polynomringe

1. Betrachte den Ring $R := \mathbb{Z}[i] \subset \mathbb{C}$ mit der sogenannten *Normabbildung*

$$N\colon R \to \mathbb{Z}^{\geqslant 0},\; a+bi \mapsto (a+bi)(a-bi) = a^2+b^2.$$

(a) Zeige, dass R ein euklidischer Ring bezüglich N ist.

(b) Bestimme $\mathrm{ggT}(2-i, 2+i)$ und $\mathrm{ggT}(28+10i, 8i-1)$ in R.

(c) Schreibe $-1+3i$ als Produkt von Primelementen aus R.

*(d) Zeige, dass jedes Primelement aus R genau eine Primzahl $p \in \mathbb{Z}$ teilt.

(e) Sei $p \in \mathbb{Z}$ eine Primzahl mit $p \equiv 3 \pmod 4$. Zeige, dass p ein Primelement von R ist.

(f) Zeige, dass $\mathbb{F}_3[X]/(X^2+1)$ ein Körper mit 9 Elementen ist.

Lösung:

(a) Wir überprüfen, dass N eine euklidische Normfunktion ist. Seien dafür $x, y \in R$ mit $y \neq 0$. Es existieren $a, b \in \mathbb{R}$, so dass $\frac{x}{y} = a+bi$ gilt (in der Tat liegen a und b in $\mathbb{Q}$). Wähle $m, n \in \mathbb{Z}$ mit

$$|a-m| \leqslant \frac{1}{2} \quad \text{und} \quad |b-n| \leqslant \frac{1}{2}$$

und setze $q := m+ni$ und $r := x-yq$. Nach Konstruktion haben wir

$$\left|\frac{x}{y} - q\right|^2 = (a-m)^2 + (b-n)^2 \leqslant \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2 < 1.$$

Somit ist $x = yq + r$ mit

$$N(r) = |x-yq|^2 = N(y) \cdot \left|\frac{x}{y} - q\right|^2 < N(y).$$

Also ist N eine euklidische Normfunktion auf R und R ist ein euklidischer Ring.

(b) Anwenden des euklidischen Algorithmus bezüglich der Normfunktion N ergibt

$$2 - i = (2+i)\cdot(1-i) - 1 \quad \text{mit } N(-1) < N(2+i),$$

also $\mathrm{ggT}(2-i, 2+i) = \mathrm{ggT}(2+i, -1) = 1$.

Weiter erhalten wir

$$\begin{aligned} 28 + 10i &= (8i-1)\cdot(1-4i) + (-3-2i) \quad \text{mit } N(-3-2i) < N(8i-1), \\ 8i - 1 &= (-3-2i)\cdot(-1-2i) + 0, \end{aligned}$$

und somit

$$\mathrm{ggT}(28+10i, 8i-1) = \mathrm{ggT}(8i-1, -3-2i) = \mathrm{ggT}(-3-2i, 0) = 3+2i.$$

(c) Die Normfunktion $N : R \to \mathbb{Z}^{\geqslant 0}$, $m + ni \mapsto m^2 + n^2 = |m+ni|^2$ ist multiplikativ, d.h. sie erfüllt

$$\forall \alpha, \beta \in R : N(\alpha\beta) = N(\alpha)N(\beta)$$

Daher erfüllen alle Einheiten $u \in R^\times$ die Bedigung $N(u) = 1$. Umgekehrt sind die Einheiten $1, -1, i, -i$ die einzigen Elemente $u \in R$ mit $N(u) = 1$. Daher haben wir

$$u \in R^\times \iff N(u) = 1 \iff u \in \{\pm 1, \pm i\}.$$

Da $N(-1+3i) = 10$ gilt, kann $-1+3i$ höchstens als Produkt von zwei Elementen $u, v \in R \smallsetminus R^\times$ der Norm 2 und 5 geschrieben werden, die nach der Multiplikativität von N unzerlegbar sein müssen. Eine solche Zerlegung ist beispielsweise durch

$$-1 + 3i = (1+i)(1+2i)$$

gegeben. Der Ring R ist als euklidischer Ring faktoriell. Daher sind unzerlegbare Elemente prim und obige Darstellung ist eine (bis auf Reihenfolge und Einheiten eindeutige) Zerlegung von $-1+3i$ in Primelemente.

(d) Sei $\pi \in R$ prim. Da π keine Einheit ist, gilt $N(\pi) > 1$, also hat $N(\pi)$ eine nicht-triviale Primfaktorzerlegung $N(\pi) = p_1 \cdots p_k$. Wegen $\pi \cdot \overline{\pi} = N(\pi)$ und da π prim ist, teilt π somit mindestens eine der Primzahlen p_i.

Nehmen wir nun an, π teile zwei verschiedene Primzahlen p und q. Da N multiplikativ ist, teilt $N(\pi)$ also $N(p) = p^2$ und $N(q) = q^2$; somit ist aber $N(\pi) = 1$; Widerspruch.

(e) Sei $p \in \mathbb{N}$ eine Primzahl mit $p \equiv 3 \pmod 4$. Da p keine Einheit ist, hat p einen Primteiler $\pi := x + yi \in R$, und da N multiplikativ ist, gilt $N(\pi)|N(p) = p^2$. Da π keine Einheit ist, gilt $N(\pi) \neq 1$. Der Fall $N(\pi) = x^2 + y^2 = p$ ist ebenfalls ausgeschlossen, da Quadratzahlen modulo 4 kongruent zu 0 oder zu 1 sind. Folglich gilt $N(\pi) = p^2 = N(p)$. Schreiben wir $p = \alpha \cdot \pi$ in R, so folgt aus der Multiplikativität von N, dass $N(\alpha) = 1$ gilt, also sind p und π assoziiert, und somit ist p ebenfalls prim in R.

(f) Seien $f, g \in \mathbb{F}_3[X]$ mit $X^2+1 = f\cdot g$. Dann gilt $\deg f + \deg g = 2$, und da X^2+1 in $\mathbb{F}_3$ keine Nullstellen hat, gilt $\deg f, \deg g \neq 1$. Also ist f oder g eine Einheit von $\mathbb{F}_3[X]$. Damit haben wir gezeigt, dass X^2+1 irreduzibel ist. Weil $\mathbb{F}_3[X]$ ein Hauptidealring ist, folgt, dass dass das Ideal $(X^2+1) \subset \mathbb{F}_3[X]$ maximal ist; also ist $\mathbb{F}_3[X]/(X^2+1)$ ein Körper. Die Menge $\{aX+b \mid a, b \in \mathbb{F}_3\} \subset \mathbb{F}_3[X]$ ist ein Repräsentantensystem von $\mathbb{F}_3[X]/(X^2+1)$, also ist $|\mathbb{F}_3[X]/(X^2+1)| = 9$.

Variante: Wegen $\mathbb{F}_3 \cong \mathbb{Z}/3\mathbb{Z}$ gilt

$$\mathbb{F}_3[X]/(X^2+1) \cong \mathbb{Z}[X]/(3, X^2+1) \cong \big(\mathbb{Z}[X]/(X^2+1)\big)/(3) = R/(3).$$

Nach (e) ist $3 \in R$ prim, also ist das Ideal (3) ein vom Nullideal verschiedenes Primideal. Da R ein Hauptidealring ist, ist (3) sogar ein maximales Ideal. Also ist $R/(3)$ ein Körper.

Die Menge $\{a + bi \mid 0 \leqslant a, b \leqslant 2\} \subset R$ ist ein Repräsentantensystem von $R/(3)$, also gilt $|R/(3)| = 9$.

2. Zeige, dass die Anzahl der Divisionen im euklidischen Algorithmus für ganze Zahlen $a_1 > a_2 > 0$ die Grössenordnung $O(\log a_1)$ hat.

(*Hinweis:* Zeige, dass die k-te Zahl a_k der durch den euklidischen Algorithmus produzierte Folge grösser oder gleich der $(m-k)$-ten Fibonacci-Zahl ist, wenn die Folge mit $a_m = 0$ endet.)

Lösung: Let $a_1, \ldots, a_m$ be the numbers obtained by the euclidean algorithm with $a_{m-1} > a_m = 0$. Then for all $1 \leqslant k \leqslant m-2$ we have $a_{k-1} = q_k a_k + a_{k+1}$ with $q_k \geqslant 0$ and $0 \leqslant a_{k+1} < a_k$. So the sequence is strictly decreasing, and so all q_k are positive.

Let $F_0, F_1, \ldots$ be the Fibonacci numbers with $F_0 = 0$ and $F_1 = 1$ and $F_k = F_{k-1} + F_{k-2}$ for all $k \geqslant 2$. We claim that $a_k \geqslant F_{m-k}$ for all $1 \leqslant k \leqslant m$. Indeed, that is already clear for $k = m$ and $k = m-1$. If $2 \leqslant k \leqslant m-1$ and the claim holds for k and $k+1$, we calculate

$$a_{k-1} = q_k a_k + a_{k+1} \geqslant a_k + a_{k+1} \geqslant F_{m-k} + F_{m-k-1} = F_{m-k+1}.$$

Thus the claim follows by downward induction on k. On the other hand it is known that

$$F_k = \frac{\varphi^k - (-\varphi)^{-k}}{\sqrt{5}}$$

with the Golden Ratio ratio $\varphi := \frac{1}{2}\cdot(1+\sqrt{5})$. Here $(-\varphi)^{-k} \to 0$ for $k \to \infty$, and so $\log F_k = k \log\varphi + O(1)$. Therefore

$$\log a_1 \geqslant \log F_{m-1} \geqslant m \log\varphi + O(1)$$

or equivalently

$$m \leqslant \frac{\log a_1}{\log\varphi} + O(1) = O(\log a_1).$$

The number $m-2$ of divisions thus satisfies the same inequality.

3. Bestimme die Einheitengruppe des Rings $(\mathbb{Z}/4\mathbb{Z})[X]$.

   Lösung: We claim that

$$(\mathbb{Z}/4\mathbb{Z})[X]^\times = \big\{1+2f \bigm| f \in \mathbb{Z}/4\mathbb{Z}[X]\big\}.$$

   "$\subset$": Consider the ring homomorphism $\varphi : (\mathbb{Z}/4\mathbb{Z})[X] \to (\mathbb{Z}/2\mathbb{Z})[X]$ attained by reducing coefficients modulo 2. Since $\mathbb{Z}/2\mathbb{Z} = \mathbb{F}_2$ is a field, we already know that $(\mathbb{Z}/2\mathbb{Z})[X]^\times = (\mathbb{Z}/2\mathbb{Z})^\times = \{1\}$. On the other hand, as a ring homomorphism φ maps units to units. Thus for all $g \in (\mathbb{Z}/4\mathbb{Z})[X]^\times$ we have $\varphi(g) = 1$, and so g has the desired form.

   "$\supset$": Let $g := 1+2f$ for some $f \in (\mathbb{Z}/4\mathbb{Z})[X]$. Then we have $g^2 = 1+4f+4f^2 = 1$, so g is a unit in $(\mathbb{Z}/4\mathbb{Z})[X]$.

4. Sei R ein Integritätsbereich. Ein Polynom der Form $f(\underline{X}) = \sum_{\underline{i}}' a_{\underline{i}} \underline{X}^{\underline{i}}$ in $R[\underline{X}] = R[X_1, \ldots, X_n]$, bei der die Summe sich nur über Multiindizes $\underline{i} = (i_1, \ldots, i_n)$ mit $\sum_\nu i_\nu = d$ erstreckt, heisst *homogen vom Grad d*.

   (a) Zeige: Das Produkt zweier homogener Polynome vom Grad d und d' ist homogen vom Grad $d + d'$.

   (b) Zeige: Jeder Teiler eines von Null verschiedenen homogenen Polynoms ist selbst homogen.

   (c) Für welche $a \in \mathbb{R}$ ist das homogene Polynom

$$X^2 + Y^2 + Z^2 + aXY + aXZ + aYZ \in \mathbb{R}[X, Y, Z]$$

   irreduzibel?

   Lösung:

   (a) Let $f(\underline{X}) := \sum_{\underline{i}}' a_{\underline{i}} \underline{X}^{\underline{i}}$ and $g(\underline{X}) := \sum_{\underline{j}}' b_{\underline{j}} \underline{X}^{\underline{j}}$ be homogeneous of degree d and d' respectively. Then

$$f(\underline{X})g(\underline{X}) = \textstyle\sum_{\underline{k}}' (\sum_{\underline{i}+\underline{j}=\underline{k}}' a_{\underline{i}} b_{\underline{j}}) \underline{X}^{\underline{k}}.$$

   For each $\underline{k}$ occuring in the sum, we have $\sum_\nu k_\nu = \sum_\nu i_\nu + \sum_\nu j_\nu = d + d'$. Thus fg is homogeneous of degree $d + d'$.

   (b) Let $f \in R[\underline{X}]$ be a divisor of a non-zero homogeneous polynomial. Then there exists a $g \in R[\underline{X}]$ with fg homogeneous of some degree D. Write f and g as the sum of their homogeneous components:

$$\begin{aligned} f &= \textstyle\sum_{e \geqslant 0}' f_e, \\ g &= \textstyle\sum_{e' \geqslant 0}' g_{e'}, \end{aligned}$$

where f_e and $g_{e'}$ are homogeneous of degrees e and e' repectively. Then

$$fg = \sum\nolimits'_{E\geqslant 0} \sum\nolimits'_{e+e'=E} f_e g_{e'}$$

By (a) each $H_E := \sum'_{e+e'=E} f_e g_{e'}$ is homogeneous of degree E. Since f and g are non-zero, there exist e_1 and e'_1 maximal such that $f_{e_1}, g_{e'_1} \neq 0$. Furthermore, we can find e_0 and e'_0 minimal such that $f_{e_0}, g_{e'_0} \neq 0$. With $E_1 := e_1 + e'_1$ and $E_0 := e_0 + e'_0$ we then have $H_{E_1} = f_{e_1} g_{e'_1}$ and $H_{E_0} = f_{e_0} g_{e'_0}$. Since R and hence $R[\underline{X}]$ is an integral domain, these products are non-zero. Since by assumption $H_E = 0$ for all $E \neq D$, we must have $D = e_1 + e'_1 = e_0 + e'_0$, which is possible if and only if $e_1 = e_0$; so that f is homogeneous of degree e_0.

(c) Wir suchen diejenigen $a \in \mathbb{R}$, für welche das Polynom reduzibel ist. Seien also $f, g \in \mathbb{R}[X, Y, Z]$ nicht-Einheiten mit

$$fg = X^2 + Y^2 + Z^2 + aXY + aXZ + aYZ.$$

Nach (b) sind f und g homogen vom Grad d bzw. d'. Der Grad von $X^2 + Y^2 + Z^2 + aXY + aXZ + aYZ$ ist 2; nach (a) gilt also $d + d' = 2$. Da f und g keine Einheiten sind, gilt zudem $d, d' > 0$, also $d = d' = 1$. Wir machen den Ansatz $f = b_1X + b_2Y + b_3Z$ und $g = c_1X + c_2Y + c_3Z$. Dann ist also

$$\begin{aligned} fg &= b_1c_1X^2 + b_2c_2Y^2 + b_3c_3Z^2 \\ &\quad +(b_1c_2 + b_2c_1)XY + (b_1c_3 + b_3c_1)XZ + (b_2c_3 + b_3c_2)YZ. \end{aligned}$$

Also erhalten wir die Gleichungen

$$(b_1c_2 + b_2c_1) = (b_1c_3 + b_3c_1) = (b_2c_3 + b_3c_2) = a,$$

$$b_1c_1 = b_2c_2 = b_3c_3 = 1.$$

Nach der zweiten Zeile können wir $c_1 = b_1^{-1}$, $c_2 = b_2^{-1}$ und $c_3 = b_3^{-1}$ schreiben. Die erste Zeile wird dann zu

$$b_1b_2^{-1} + b_2b_1^{-1} = b_1b_3^{-1} + b_3b_1^{-1} = b_2b_3^{-1} + b_3b_2^{-1} = a.$$

Aus der Gleichheit $b_1b_2^{-1} + b_2b_1^{-1} = b_1b_3^{-1} + b_3b_1^{-1}$ folgt $b_2 = b_3$ und somit ist

$$a = b_2b_3^{-1} + b_3b_2^{-1} = 2.$$

Das Polynom $X^2 + Y^2 + Z^2 + aXY + aXZ + aYZ$ ist also irreduzibel, falls $a \neq 2$ gilt. Für $a = 2$ hat es die nicht-triviale Faktorzerlegung

$$X^2 + Y^2 + Z^2 + 2XY + 2XZ + 2YZ = (X + Y + Z)^2.$$

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

   Lösung:

   - Klarerweise sind die linearen Polynome $X, X+1 \in \mathbb{F}_2[X]$ irreduzibel.
   - Ein Polynom $f \in \mathbb{F}_2[X]$ mit $\deg(f) \in \{2,3\}$ ist genau dann irreduzibel, wenn es keine Zerlegung $f = g \cdot h$ mit Polynomen $g, h \in \mathbb{F}_2[X]$ mit $\deg(g) = 1$ und $\deg(h) \in \{1,2\}$ gibt. Dies ist genau dann der Fall, wenn f keine Nullstelle in $\mathbb{F}_2[X]$ hat. Somit sind die irreduziblen Polynome vom Grad 2 und 3 in $\mathbb{F}_2[X]$ genau durch $X^2+X+1, X^3+X^2+1, X^3+X+1$ gegeben.
   - Ein Polynom $f \in \mathbb{F}_2[X]$ mit $\deg(f) \in \{4,5\}$ ist genau dann irreduzibel, wenn es keinen Primfaktor 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 in $\mathbb{F}_2[X]$.

6. 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 $a, b \notin R[X]^\times$ 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.

7. 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 (siehe Aufgabe 5).

   (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 Nullstellen 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.