D-MATH Algebra I HS 2022
Prof. Richard Pink

Musterlösung Serie 13

Hauptidealringe, Euklidische Ring, Irreduzible Polynome

1. Die Brüder Dmitrij, Iwan und Alexej Karamasow leben in einem Studentenwohnheim. Dmitrij hat sich angewöhnt alle 5 Tage, Iwan alle 7 Tage, und Alexej alle 11 Tage eine Pizza zu essen. Die erste Pizza des Jahres 2023 essen Dmitrij und Alexej am 3.1. und Iwan am 4.1. An welchem Tag werden sie erstmals alle drei gemeinsam eine Pizza essen?

   Lösung: Sei $x \in \mathbb{Z}^{\geqslant 0}$ die Anzahl Tage, die seit dem 3. Januar vergangen sind, wenn erstmals alle drei gemeinsam eine Pizza essen. Nach Aufgabenstellung ist x die kleinste nicht-negative ganze Zahl, die das folgende Restsystem löst:

$$\begin{aligned} x &\equiv 0 \pmod 5 \\ x &\equiv 0 \pmod{11} \\ x &\equiv 1 \pmod 7 \end{aligned}$$

   Da 5, 7 und 11 paarweise teilerfremd sind, wissen wir nach dem Chinesischen Restsatz, dass dieses System genau eine Lösung x modulo $5 \cdot 7 \cdot 11 = 385$ hat. Nach den ersten beiden Gleichungen ist diese durch 5 und 11 teilbar, also ein Vielfaches von 55. Von den Vielfachen k von 55 mit $0 \leqslant k < 385$ ist 330 auch Lösung der dritten Gleichung. Somit essen erstmals am 330. Tag nach dem 3. Januar, also am 29. November 2023, alle drei zusammen eine Pizza.

2. 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) Zeige, dass jede Primzahl $p \equiv 3 \pmod 4$ 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 $y \neq 0$. Schreibe $\frac{x}{y} = a + bi$ mit $a, b \in \mathbb{Q}$, 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 dann

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

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 (R, N) 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 $\mathrm{ggT}(2 - i, 2 + i) \sim \mathrm{ggT}(2 + i, -1) \sim 1$. Analog rechnen wir

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

daher folgt

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

(c) Die Normfunktion N erfüllt $N(1) = 1$ und ist multiplikativ, d.h., es gilt

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

Für jede Einheit $u \in R^\times$ ist auch $u^{-1} \in R^\times$; daher gilt $N(u) \cdot N(u^{-1}) = N(uu^{-1}) = N(1) = 1$ und somit $N(u) = 1$. Umgekehrt sind die Einheiten $1, -1, i, -i$ die einzigen Elemente $u \in R$ mit $N(u) = 1$. Daher haben wir

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

Wegen $N(-1 + 3i) = 10$ kann $-1 + 3i$ höchstens als Produkt von zwei Elementen $u, v \in R \setminus R^\times$ der Norm 2 und 5 geschrieben werden, die dann nach der Multiplikativität von N unzerlegbar sein müssen. Da die Elemente der Norm 2 genau die Elemente $\pm 1 \pm i$ sind, finden wir durch Probieren z.B. die Zerlegung

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

Der Ring R ist als euklidischer Ring faktoriell. Daher sind unzerlegbare Elemente prim und obige Darstellung ist eine Zerlegung 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. Dann ist 1 eine $\mathbb{Z}$-Linearkombination von p und q und somit auch eine R-Linearkombination. Daher teilt π auch das Element $1 \in R$; Widerspruch.

(e) Betrachte eine Primzahl $p \equiv 3 \pmod 4$. Dann ist $N(p) = p^2 > 1$ und somit $p \notin R^\times \cup \{0\}$. Nehmen wir nun an, dass p kein Primelement von R ist. Da R faktoriell ist, ist p dann zerlegbar, und wegen $N(p) = p^2$ und der Multiplikativität von N muss es eine Zerlegung $p = xy$ mit $N(x) = N(y) = p$ geben. Schreiben wir $x = a + bi$, so folgt also $a^2 + b^2 = p$. Aber jede Quadratzahl in $\mathbb{Z}$ ist kongruent zu 0 oder 1 modulo (4), also kann $a^2 + b^2$ nur kongruent zu 0, 1, oder 2 modulo (4) sein. Wegen $p \equiv 3 \pmod 4$ erhalten wir daher einen Widerspruch, und p ist ein Primelement 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 $|\mathbb{F}_3[X]/(X^2+1)| = 9$.

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

*3. 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 $1 \leqslant k \leqslant m-1$ 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 $\varphi := \frac{1}{2} \cdot (1 + \sqrt{5})$. 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.

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

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

   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

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

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. Choose $g \in R[\underline{X}]$ such that fg is non-zero homogeneous. Then f and g are non-zero. Write

$$f = \sum_{d=d_0}^{d_1} f_d \qquad \text{and} \qquad g = \sum_{e=e_0}^{e_1} g_e$$

with f_d and g_e homogeneous of degree d resp. e and with $f_{d_0}, f_{d_1}, g_{e_0}, g_{e_1} \neq 0$. Then

$$fg \;=\; \sum_{D=d_0+e_0}^{d_1+e_1} \Big(\sum_{d+e=D} f_d g_e \Big).$$

Here the terms for $D = d_0 + e_0$ and $d_1 + e_1$ are $f_{d_0} g_{e_0}$ and $f_{d_1} g_{e_1}$, which are non-zero, because R is integral. As fg is homogeneous, it follows that $d_0 + e_0 = d_1 + e_1$. Therefore f is homogeneous of degree $d_0 = d_1$ and g homogeneous of degree $e_0 = e_1$.

(c) Wir suchen diejenigen $a \in \mathbb{R}$, für welche P_a reduzibel ist. Da P_a homogen vom Grad 2 ist, sind nach (b) alle Teiler homogen vom Grad $\leqslant 2$. Ausserdem ist jedes von Null verschiedene homogene Polynom vom Grad 0 eine Konstante in $K^\times$ und damit eine Einheit. Wir müssen daher nur testen, ob es eine Faktorisierung $P_a = fg$ gibt mit homogenen Faktoren vom Grad 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

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

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

Die zweite Zeile impliziert $c_i = \frac{1}{b_i}$ für alle i. Die erste Zeile wird dann zu

$$\tfrac{b_1}{b_2} + \tfrac{b_2}{b_1} = \tfrac{b_1}{b_3} + \tfrac{b_3}{b_1} = \tfrac{b_2}{b_3} + \tfrac{b_3}{b_2} = a.$$

Die ersten beiden Gleichungen sind äquivalent zu $\{\frac{b_1}{b_2}, \frac{b_2}{b_1}\} = \{\frac{b_1}{b_3}, \frac{b_3}{b_1}\} = \{\frac{b_2}{b_3}, \frac{b_3}{b_2}\}$. Dies ist nur möglich, wenn zwei dieser Mengen auch in der Reihenfolge der genannten Elemente übereinstimmen. Nach einer etwaigen Permutation von $\{1, 2, 3\}$ ist dann zum Beispiel $\frac{b_1}{b_2} = \frac{b_1}{b_3}$ und damit $b_2 = b_3$. Also ist $\{\frac{b_2}{b_3}, \frac{b_3}{b_2}\} = \{1\}$ und damit $b_1 = b_2 = b_3$. und damit $a = 2$. Das Polynom $X^2 + Y^2 + Z^2 + aXY + aXZ + aYZ$ ist also irreduzibel, falls $a \neq 2$ ist. Für $a = 2$ hat es die nicht-triviale Faktorzerlegung

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