Lösung 6

Euklidische Ringe, irreduzible Elemente

1. Sei R der Ring der Eisensteinschen ganzen Zahlen $\mathbb{Z}[\zeta]$ für $\zeta = \frac{-1+i\sqrt{3}}{2}$. Zeigen Sie, dass

   (a) $\mathbb{Z}[\zeta]$ aus allen Elementen der Form $a + b\zeta$ für $a, b \in \mathbb{Z}$ besteht,

   (b) $\mathbb{Z}[\zeta]$ ein euklidischer Ring bezüglich der Normfunktion $N(a + \zeta b) := (a + b\zeta)(a+b\overline{\zeta}) = a^2-ab+b^2$ ist, wobei $\overline{\zeta}$ das komplex konjugierte von ζ bezeichnet.

2. Zeigen Sie, dass es irreduzible Elemente $a, b \in \mathbb{C}[X, Y]$ gibt, so dass $(a) \neq (b)$ und $(a) + (b) \neq \mathbb{C}[X, Y]$.

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

4. (a) (**SAGE**) Programmieren Sie eine Methode mit zwei Parametern p und n, die eine Liste der irreduziblen monischen Polynome vom Grad n in $\mathbb{F}_p[X]$ berechnet, wobei $n \in \mathbb{N}$ und p eine Primzahl ist. Benutzen Sie diese Methode um ihr Ergebnis aus Aufgabe 3 zu überprüfen.

   (b) (**SAGE**) Benutzen Sie Aufgabenteil (a) um eine Methode mit zwei Parametern p und n zu schreiben, die die Anzahl der irreduziblen monischen Polynome vom Grad n in $\mathbb{F}_p[X]$ zurückgibt, wobei $n \in \mathbb{N}$, $n \geqslant 1$ und p eine Primzahl ist. Verwenden Sie diese Methode, um eine Vermutung über die Anzahl der irreduziblen monischen Polynome vom Grad 2 in $\mathbb{F}_p[X]$ in Abhängigkeit von p aufzustellen. Können Sie diese auch beweisen?

5. Sei R der Ring $\mathbb{Z}[\frac{1}{2}, i\sqrt{5}]$. Zeigen Sie, dass

   (a) R aus allen Elementen der Form $a + bi\sqrt{5}$ mit $a, b \in \mathbb{Z}[\frac{1}{2}]$ besteht,

   (b) **Korrektur:** R ein euklidischer Ring bezüglich der Normfunktion

   $$\Phi(a + bi\sqrt{5}) := N(2^n(a + bi\sqrt{5})) = 2^{2n}(a^2 + 5b^2),$$
   $$\text{mit } n \in \mathbb{Z} \text{ minimal, so dass } 2^n a, 2^n b \in \mathbb{Z}$$

   ist.

   Hinweis: Für $z = \frac{g}{f} = a + bi\sqrt{5}$ und $b \in \mathbb{Z} + [-\frac{1}{3}, \frac{1}{3}]$ verwende $q = [a] + [b]i\sqrt{5}$, wobei $[a], [b]$ die nächsten ganzen Zahlen zu a, b bezeichnen. Ansonsten verwende die beste Approximation mit $a, b \in \frac{1}{2}\mathbb{Z}$. Zeichnen Sie eine Skizze.

Lösung:

(a) Es gilt, dass $a + bi\sqrt{5}$ in R liegt für alle $a, b \in \mathbb{Z}[\frac{1}{2}]$, da R ein Ring ist und $\frac{1}{2}$ und $i\sqrt{5}$ enthält.
Andererseits ist $\{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}[\frac{1}{2}]\}$ ein Ring, da 0 in dieser Menge enthalten ist und für $a + bi\sqrt{5}, c + di\sqrt{5}$ aus dieser Menge gilt, dass deren Summe und Produkt wieder in der Menge liegt. Wir rechnen für das Produkt

$$(a + bi\sqrt{5})(c + di\sqrt{5}) = (ac - 5bd) + (ad + bc)i\sqrt{5},$$

mit $ac-5bd$ und $ad+bc$ in $\mathbb{Z}[\frac{1}{2}]$. Da R nach Definition der kleinste Ring ist, der $\frac{1}{2}$ und $i\sqrt{5}$ enthält, gilt auch die andere Inklusion $R \subseteq \{a+bi\sqrt{5} \mid a, b \in \mathbb{Z}[\frac{1}{2}]\}$.

(b) Sei $f \in R \setminus \{0\}$. Aus (a) wissen wir, dass $f = 2^k x + 2^l y i\sqrt{5}$ mit $x, y, k, l \in \mathbb{Z}$, x, y ungerade oder 0. Sind $k, l \geqslant 0$, so ist $f \in \mathbb{Z}[i\sqrt{5}]$ und es gilt $\Phi(f) \leqslant N(f)$.
Wir wollen nun zeigen, dass es $n \in \mathbb{Z}$ gibt mit $\Phi(2^n f) = N(2^n f)$. Dies gilt automatisch, falls $x = y = 0$. Ist $y = 0$ und x ungerade, dann gilt $f = 2^k x$ und $\Phi(2^{-k} f) = \Phi(x) = N(x) = N(2^{-k} f)$, x ungerade und in $\mathbb{Z}$. Ein analoges Argument gilt, falls $x = 0$ und y ungerade. Sind nun beide x, y ungerade, ist es nicht schwer zu überprüfen (indem man alle Fälle von k, l positiv oder negativ durchgeht), dass für $n := -\min\{k, l\}$ gilt, dass $\Phi(2^n f) = N(2^n f)$, da x, y beide ungerade.
Seien nun $f, g \in R \setminus \{0\}$ und wir wollen g mit Rest durch f teilen. Wir nehmen zuerst an, dass $f, g \in \mathbb{Z}[i\sqrt{5}]$ mit $\Phi(f) = N(f)$.
Wir betrachten nun $z := \frac{g}{f} = a + bi\sqrt{5} \in \mathbb{Q}[i\sqrt{5}]$ und folgen dem Hinweis.
Fall 1: $b \in \mathbb{Z} + [-\frac{1}{3}, \frac{1}{3}]$.
Bezeichne mit $[a], [b] \in \mathbb{Z}$ die besten Approximationen von a, b in $\mathbb{Z}$. Definiere $q := [a] + [b]i\sqrt{5} \in \mathbb{Z}[i\sqrt{5}]$ und $r := g - fq$. Wir bemerken, dass $r \in \mathbb{Z}[i\sqrt{5}]$, da $f, g, q \in \mathbb{Z}[i\sqrt{5}]$, und damit gilt $\Phi(r) \leqslant N(r)$. Wir schätzen nun $N(z - q)$ ab, da wir N auf $\mathbb{Q}[i\sqrt{5}]$ fortsetzen können:

$$N(z - q) = (a - [a])^2 + 5(b - [b])^2 \leqslant \frac{1}{4} + 5\frac{1}{9} < 1,$$

da $b \in \mathbb{Z} + [-\frac{1}{3}, \frac{1}{3}]$ und Wahl von $[b]$. Es folgt

$$\Phi(r) \leqslant N(r) = N(g - fq) = N(f)N(z - q) < N(f) = \Phi(f),$$

was zu zeigen war.
Fall 2: $b \notin \mathbb{Z} + [-\frac{1}{3}, \frac{1}{3}]$.
Bezeichne mit $\tilde{a}, \tilde{b} \in \frac{1}{2}\mathbb{Z}$ die besten Approximationen von a, b in $\frac{1}{2}\mathbb{Z}$. Definiere $q := \tilde{a} + \tilde{b}i\sqrt{5} \in \frac{1}{2}\mathbb{Z}[i\sqrt{5}]$ und $r := g - fq$. Wir bemerken, dass $r \in \frac{1}{2}\mathbb{Z}[i\sqrt{5}]$, da $f, g \in \mathbb{Z}[i\sqrt{5}]$ und $q \in \frac{1}{2}\mathbb{Z}[i\sqrt{5}]$. Wir bemerken, dass daraus folgt, dass $\Phi(r) \leqslant 4N(r)$, da $2\tilde{a}$ und $2\tilde{b} \in \mathbb{Z}$, wir also höchstens einmal mit 2 multiplizieren müssen. Nun schätzen wir wieder $N(z - q)$ ab:

$$N(z - q) = (a - \tilde{a})^2 + 5(b - \tilde{b})^2 \leqslant \left(\frac{1}{4}\right)^2 + 5\left(\frac{1}{6}\right)^2 = \frac{1}{16} + 5\frac{1}{36} < \frac{1}{4},$$

nach Wahl von $\tilde{a}$ und $\tilde{b}$ und Benutzung, dass $b \notin \mathbb{Z} + [-\frac{1}{3}, \frac{1}{3}]$. Wir erhalten

$$\Phi(r) \leqslant 4N(r) = 4N(g - fq) = 4N(f)N(z - q) < 4N(f)\frac{1}{4} = N(f) = \Phi(f),$$

was zu zeigen war.

Wir betrachten nun den allgemeinen Fall. Seien nun $g, f \in R$ beliebig, $f \neq 0$. Wir wählen $n \in \mathbb{Z}$ mit $\Phi(f) = \Phi(2^n f) = N(2^n f)$ und setzen $\tilde{f} := 2^n f \in \mathbb{Z}[i\sqrt{5}]$. Wir wählen des weiteren $m \in \mathbb{Z}$ mit $\tilde{g} := 2^m g \in \mathbb{Z}[i\sqrt{5}]$. Wir wenden obige Diskussion auf $\tilde{f}$ und $\tilde{g}$ an und erhalten $\tilde{r}, \tilde{q} \in \mathbb{Z}[\frac{1}{2}, i\sqrt{5}]$ mit $\tilde{g} = \tilde{f}\tilde{q} + \tilde{r}$ und $\Phi(\tilde{r}) < \Phi(\tilde{f})$. Damit ist aber auch

$$g = 2^{-m}\tilde{g} = 2^{-m}(2^n f\tilde{q} + \tilde{r}) = f(2^{n-m}\tilde{q}) + 2^{-m}\tilde{r}.$$

Wir setzen $q := 2^{n-m}\tilde{q}$, $r := 2^{-m}\tilde{r}$, so dass

$$\Phi(r) = \Phi(2^{-m}\tilde{r}) = \Phi(\tilde{r}) < \Phi(\tilde{f}) = \Phi(f),$$

was zu zeigen war.

6. Sei R ein Integritätsbereich. Ein Polynom der Form $f(\underline{X}) = \sum_{\underline{i}} a_{\underline{i}} \underline{X}^{\underline{i}}$ in $R[X_1, \ldots, X_n]$, 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) Zeigen Sie, dass as Produkt zweier homogener Polynome vom Grad d und d' homogen vom Grad $d + d'$ ist.

   (b) Zeigen Sie, dass jeder Teiler eines von Null verschiedenen homogenen Polynoms selbst homogen ist.

   (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) Seien $f(\underline{X}) := \sum_{\underline{i}} a_{\underline{i}} \underline{X}^{\underline{i}}$ and $g(\underline{X}) := \sum_{\underline{j}} b_{\underline{j}} \underline{X}^{\underline{j}}$ homogen vom Grad d bzw. d'. Dann ist

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

Für jedes $\underline{k}$ das in der Summe vorkommt gilt $\sum_\nu k_\nu = \sum_\nu i_\nu + \sum_\nu j_\nu = d + d'$. Daher ist fg homogen vom Grad $d + d'$.

(b) Sei $f \in R[\underline{X}]$ ein Teiler eines von Null verschiedenen homogenen Polynoms. Wähle $g \in R[\underline{X}]$ so dass fg homogen ist und nicht das Nullpolynom. Dann sind f und g beide nicht das Nullpolynom. Wir schreiben f bzw. g als die Summe über ihre homogenen Anteile, d.h.

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

mit f_d und g_e homogen vom Grad d bzw. e und mit $f_{d_0}, f_{d_1}, g_{e_0}, g_{e_1} \neq 0$ und $d_0 \leqslant d_1$ und $e_0 \leqslant e_1$. Um zu zeigen, dass f homogen ist, genügt es zu zeigen, dass $d_0 = d_1$. Wir berechnen

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

Die Terme für $D = d_0 + e_0$ bzw. $D = d_1 + e_1$ sind $f_{d_0} g_{e_0}$ bzw. $f_{d_1} g_{e_1}$, welche nicht die Nullpolynome sind, da R ein Integritätsbereich ist. Da fg homogen ist folgt, dass $d_0 + e_0 = d_1 + e_1$. Deshalb folgt, dass f homogen vom Grad $d_0 = d_1$ und g homogen vom Grad $e_0 = e_1$ sind.

(c) Wir suchen diejenigen $a \in \mathbb{R}$, für welche P_a reduzibel ist. Seien also $f, g \in \mathbb{R}[X, Y, Z]$ nicht-Einheiten mit $fg = P_a$. Nach (b) sind f und g homogen, sagen wir vom Grad d bzw. e. Nach (a) gilt dann $d + e = \deg(P_a) = 2$. Da f und g keine Einheiten sind, gilt zudem $d, e > 0$, also $d = e = 1$. Wir machen den Ansatz $f = b_1 X + b_2 Y + b_3 Z$ und $g = c_1 X + c_2 Y + c_3 Z$. Dann ist also

$$\begin{aligned} fg \;=\; & b_1 c_1 X^2 + b_2 c_2 Y^2 + b_3 c_3 Z^2 \\ & + (b_1 c_2 + b_2 c_1) XY + (b_1 c_3 + b_3 c_1) XZ + (b_2 c_3 + b_3 c_2) YZ. \end{aligned}$$

Also erhalten wir die Gleichungen

$$(b_1 c_2 + b_2 c_1) = (b_1 c_3 + b_3 c_1) = (b_2 c_3 + b_3 c_2) = a,$$

$$b_1 c_1 = b_2 c_2 = b_3 c_3 = 1.$$

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

$$b_1 b_2^{-1} + b_2 b_1^{-1} = b_1 b_3^{-1} + b_3 b_1^{-1} = b_2 b_3^{-1} + b_3 b_2^{-1} = a.$$

Wegen Invarianz unter Skalierung können wir annehmen, dass $b_3 = 1$. Dann erhalten wir

$$b_1 + b_1^{-1} = a = b_2 + b_2^{-1}, \quad b_1 b_2^{-1} + b_2 b_1^{-1} = a.$$

Nun hat $x + x^{-1} = a$ genau eine Lösung, falls $a = \pm 2$ und genau zwei Lösungen r_1 und r_2 mit $|r_1| < 1 < |r_2|$, falls $\frac{a^2}{4} - 1 > 0$. Ist $b_1 = b_2$ so folgt $a = 2$. Ist $a = -2$, so erhalten wir, dass $b_1, b_2 < 0$ aus der ersten Gleichheit, aber dies führt dazu, dass $b_1 b_2^{-1}, b_2 b_1^{-1} > 0$, ein Widerspruch dazu, dass deren Summe gleich $a = -2 < 0$ sein soll. Andernfalls sei $\{b_1, b_2\} = \{r_1, r_2\}$. Dann ist aber auch $b_1 b_2^{-1} \in \{r_1, r_2\}$, was ein Widerspruch ist. Wir schliessen, dass $b_1 = b_2 = b_3$.

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

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