Serie 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.

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.)

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

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?

5. Bestimme alle irreduziblen Polynome vom Grad $\leqslant 5$ 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.

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