Algebra I

Serie 5

Hauptidealringe, Euklidische Ringe, 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 2019 essen Dmitrij und Alexej am 3.1. und Iwan am 4.1. An welchem Tag werden sie erstmals alle drei gemeinsam eine Pizza essen?

2. Im Ring $R := \mathbb{Z}[i\sqrt{5}] \subset \mathbb{C}$ gilt die Gleichheit
$$6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5}).$$
Zeige:
   (a) Die Funktion $N\colon R \to \mathbb{Z}^{\geqslant 0}, z = a + bi\sqrt{5} \mapsto |z|^2 = a^2 + 5b^2$ ist multiplikativ (das heisst, $\forall \alpha, \beta \in R : N(\alpha\beta) = N(\alpha)N(\beta)$).
   (b) $R^\times = \{u \in R \mid N(u) = 1\} = \{\pm 1\}$.
   (c) Die Elemente $2, 3, 1 + i\sqrt{5}, 1 - i\sqrt{5}$ sind unzerlegbar in R.
   (d) Die Elemente $2, 3, 1 + i\sqrt{5}, 1 - i\sqrt{5}$ sind keine Primelemente in R.
   (e) Für das Ideal $I = (2, 1 + i\sqrt{5})$ gilt $I \cdot I = (2)$.
   (f) I ist kein Hauptideal von R.
   (g) I ist ein maximales Ideal von R.
   (h) R ist nicht faktoriell.

3. 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.

*4. 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.)

5. 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?

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.