Universität Konstanz Alexander Taveira Blomenhofer
Fachbereich Mathematik und Statistik Markus Schweighofer
Sommersemester 2019

Übungsblatt 7 zur Zahlentheorie

Aufgabe 1. Sei R ein kommutativer Ring mit $0 \neq 1$ und M ein R-Modul. Zeige, dass die Zuordnungen

$$f \mapsto \begin{pmatrix} R[X] \times M \to M \\ \quad (p, x) \mapsto p(f)(x) \end{pmatrix}$$

$$\begin{pmatrix} M \to M \\ x \mapsto X \cdot x \end{pmatrix} \leftarrow\!\shortmid \ \cdot$$

eine Bijektion vermittelt zwischen $\operatorname{End}(M)$ und der Menge aller Fortsetzungen der Skalarmultiplikation des R-Moduls M, die M zu einem $R[X]$-Modul machen.

Aufgabe 2. Seien R ein kommutativer Ring, M ein endlich erzeugter R-Modul und $f, g \in \operatorname{End}(M)$ mit $fg = gf$ und $\operatorname{im} f \subseteq \operatorname{im} g$. Zeige, dass es ein $n \in \mathbb{N}$ und ein $h \in \operatorname{End}(M)$ gibt mit

$$f^n = hg.$$

Folgere daraus noch einmal die Aussage aus Aufgabe 3 auf Blatt 5.

Hinweis. Falls $0 \neq 1$ in R, dann mache M zum $R[X]$-Modul vermöge $Xx := g(x)$ für $x \in M$.

Aufgabe 3. Sei $p \in \mathbb{P}$ mit $p \equiv_{(4)} 1$. Betrachte den quadratischen Zahlring $\mathscr{O}_{-1} = \mathbb{Z}[\mathring{\imath}]$ der Gaußschen Zahlen und den Körper $\mathbb{F}_p = \mathbb{Z}/(p)$ mit p Elementen. Zeige:

(a) Für $m := \frac{p-1}{4} \in \mathbb{N}$ ist jedes Element von $\{x^4 \mid x \in \mathbb{F}_p^\times\}$ eine Nullstelle des Polynoms $X^m - 1 \in \mathbb{F}_p[X]$.

(b) Es gibt $x \in \mathbb{F}_p^\times \setminus \{\pm 1\}$ mit $x^4 = 1$.

(c) Das Polynom $X^4 - 1$ zerfällt in $\mathbb{F}_p[X]$ in Linearfaktoren.

(d) Das Polynom $X^4 - 1$ zerfällt in $\mathscr{O}_{-1}[X]$ in Linearfaktoren.

(e) p ist nicht prim in $\mathscr{O}_{-1}$.

(f) p ist in $\mathscr{O}_{-1}$ reduzibel.

(g) Es gibt $a, b \in \mathbb{Z}$ mit $p = a^2 + b^2$.

Hinweis: Wäre p prim in $\mathscr{O}_{-1}$, so zeige man, dass man eine kanonische Körpereinbettung $\mathbb{F}_p \hookrightarrow \mathscr{O}_{-1}/(p)$ hätte. Benutze, dass $\mathscr{O}_{-1}$ faktoriell ist. Benutze die komplexe Konjugation.

Abgabe bis Mittwoch, den 5. Juni 2019, um 11:44 Uhr in die Zettelkästen neben F411.