TECHNISCHE UNIVERSITÄT GRAZ
INSTITUT FÜR ANALYSIS UND ZAHLENTHEORIE
Marc Technau

Sommersemester 2023
Graz, den 15.06.2023

14. Übung zur Einführung in die Algebra

14.1. *(Nicht-prime irreduzible Elemente)*
Betrachten Sie den Ring $R := \mathbb{Z}[i\sqrt{5}] = \{a + i\sqrt{5}b \in \mathbb{C} : a, b \in \mathbb{Z}\}$. (Die Ringaxiome nachzurechnen ist hier nicht gefordert.) Zeigen Sie dann, dass es sich bei

$$2 \cdot 3 = (1 + i\sqrt{5}) \cdot (1 - i\sqrt{5}),$$

um zwei Zerlegungen von $6 \in R$ in Produkte irreduzibler Elemente handelt, aber die darin vorkommenden Elemente keine Primelemente in R sind.
(Hinweis: betrachten Sie die Funktion $N : R \to \mathbb{Z}$ aus Aufgabe 12.3; wegen $N(xy) = N(x)N(y)$ für alle $x, y \in R$ lässt sich damit Teilbarkeit in R auf Teilbarkeit in $\mathbb{Z}$ zurückführen.)

14.2. *(Ein Körper mit genau 4 Elementen)* (4 Punkte)
Es sei $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ und $f = X^2 + X + 1_{\mathbb{F}_2} \in \mathbb{F}_2[X]$. Ferner sei $K = \mathbb{F}_2[X]/\langle f \rangle$.

(a) Zeigen Sie, dass f irreduzibel ist und folgern Sie, dass K ein Körper ist.

(b) Bestimmen Sie alle Elemente von K und stellen Sie die zugehörigen Additions- und Multiplikationstafeln auf (vgl. Tutoriumsblatt 1).

(c) Ist $K^\times$ zyklisch? Falls ja, bestimmen Sie *alle* Erzeuger von $K^\times$.

14.3. *(Satz über rationale Nullstellen)* (4 Punkte)

(a) Es sei $f = c_n X^n + \ldots + c_1 X + c_0 X^0 \in \mathbb{Z}[X]$ ein Polynom vom Grad $n \geq 1$ mit rationaler Nullstelle $\frac{a}{q} \in \mathbb{Q}$, a und q teilerfremd. Zeigen Sie $a \mid c_0$ und $q \mid c_n$.

(b) Benutzen Sie Teil (a), um einzusehen, dass $\sqrt{2}$ (eine Nullstelle von $X^2 - 2$) nicht rational ist.

(c) Bestimmen Sie alle Nullstellen in $\mathbb{Q}$ des Polynoms $3X^4 - 5X^3 + X^2 - 5X - 2$.

14.4. *(Ein irreduzibles Polynom über $\mathbb{F}_p$)*
Für eine Primzahl p sei $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Zeigen Sie, dass das Polynom $f = X^p - X - 1 \in \mathbb{F}_p[X]$ irreduzibel ist.
(Hinweis: zeigen Sie, dass f invariant unter Einsetzen von $X + 1$ für X ist. Betrachten Sie anschließend die hieraus hervorgehende Operation von $(\mathbb{F}_p, +) \cong (C_p, \oplus)$ auf der Menge der Primteiler von f.)

Geben Sie Ihre Lösung bitte am 22.06.2023 vor der Vorlesung ab.
https://www.math.tugraz.at/~mtechnau/teaching/2023-s-einf-algebra.html