Technische Universität Graz
Institut für Analysis und Zahlentheorie
Marc Technau & Christian Elsholtz

Sommersemester 2021
Graz, den 04.06.2021

11. Übung zur Einführung in die Algebra

11.1. *(Längen von Zerlegungen in irreduzible Elemente)*
Es sei R ein Integritätsbereich und $R[X]$ der Polynomring über R in einer Variablen. $R[X^2, X^3]$ bezeichne den kleinsten Teilring von $R[X]$, der R, X^2 und X^3 enthält. Zeigen Sie:

(a) $R[X^2, X^3] = \left\{ \sum_n a_n X^n : a_n \in R, \text{fast alle gleich } 0_R,\ a_1 = 0_R \right\}$.

(b) Die Elemente X^2 und X^3 sind beide irreduzibel in $R[X^2, X^3]$.

(c) $R[X^2, X^3]$ ist nicht faktoriell.

11.2. *(Ein Körper mit genau 9 Elementen)* (4 Punkte)
Es sei $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$ und $f = X^2 + 1 \in \mathbb{F}_3[X]$. Ferner sei $K = \mathbb{F}_3[X]/\langle f \rangle$.

(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 $K^\times$.

11.3. *(Satz über rationale Nullstellen)*

(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) Bestimmen Sie alle Nullstellen in $\mathbb{Q}$ des Polynoms $2X^4 - X^3 - 4X^2 - X - 6$.

11.4. *(Die ganzen Gaußsche Zahlen, II)* (4 Punkte)
Betrachten Sie den Ring $\mathbb{Z}[\mathrm{i}]$ der ganzen Gaußschen Zahlen aus Aufgabe 9.3. Ferner sei $p \in \mathbb{N}$ eine Primzahl. Zeigen Sie:

(a) Für jedes Primelement π von $\mathbb{Z}[\mathrm{i}]$ ist $N(\pi)$ entweder eine Primzahl in $\mathbb{N}$ oder das Quadrat einer solchen. (Hinweis: $N(\pi) = \pi\overline{\pi}$.)

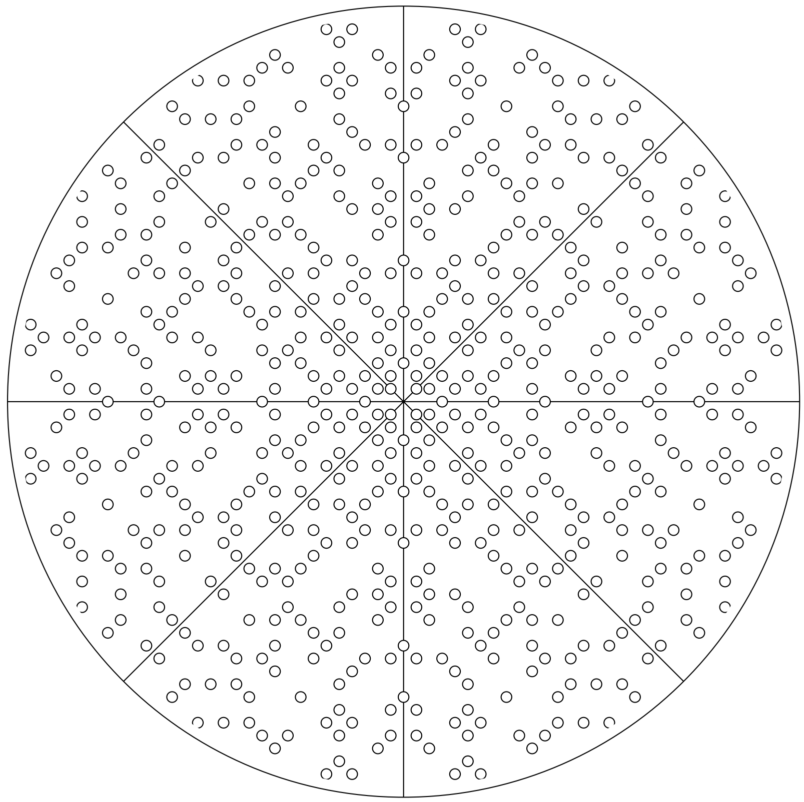
(b) (1) Ist p Summe zweier Quadrate, d.h. $p = a^2 + b^2$ mit $a, b \in \mathbb{Z}$, so ist $p = (a + \mathrm{i}b)(a - \mathrm{i}b)$ eine Zerlegung von p in Primelemente von $\mathbb{Z}[\mathrm{i}]$ und $a + \mathrm{i}b$ ist dann und nur dann assoziiert zu $a - \mathrm{i}b$, wenn $|a| = |b| = 1$ ist.

(2) Ist p nicht Summe zweier Quadrate, so ist p ein Primelement von $\mathbb{Z}[\mathrm{i}]$.

Geben Sie Ihre Lösung bitte digital bis zum 11.06.2021, 10:00 Uhr, im zugehörigen TeachCenter-Kurs ab. Dort und auf der Vorlesungswebseite finden Sie auch weitere Informationen.
`https://tc.tugraz.at/main/course/view.php?id=352`
`https://www.math.tugraz.at/~mtechnau/teaching/2021-s-einf-algebra.html`

(c) Ist $p \equiv 3 \bmod 4$, so ist p ein Primelement von $\mathbb{Z}[\mathrm{i}]$. (Hinweis: $a^2 + b^2 \equiv \boxed{?} \bmod 4$.)

(d) Bestimmen Sie alle Primelemente $a + \mathrm{i}b$ von $\mathbb{Z}[\mathrm{i}]$ mit $a, b \in \mathbb{Z}$ und $0 \leq a, b \leq 6$ und zeichnen Sie diese in der Gaußschen Zahlenebene.



(Hinweis: in dem obigen Bild ist (bei geeigneter Vergrößerung) die Lösung zu Teil (d) zu finden. Benutzen Sie dies aber allenfalls zur Selbstkontrolle Ihres Ergebnises und nicht zur Lösungsfindung.)