UNIVERSITÄT PADERBORN
INSTITUT FÜR MATHEMATIK
Marc Technau
Nicolas Potthast

Wintersemester 2024/25
Paderborn, den 17.01.2025

13. Übung zur Algebra 1

13.1. *(Erweiterter Euklidischer Algorithmus)* (4 Punkte)

(a) (Aufwärmübung:) Benutzen Sie das in den Vorlesungsnotizen in § 8.1.2 beschriebene Verfahren, um aus dem nachstehenden Divisionsschema Zahlen $x, y \in \mathbb{Z}$ mit $24x + 7y = 1$ zu gewinnen:

$$\begin{cases} 24 = 3 \cdot 7 + 3, \\ 7 = 2 \cdot 3 + 1, \\ 3 = 3 \cdot 1 + 0. \end{cases}$$

(b) Wir schreiben $\mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$ und $\overline{a} = a + 5\mathbb{Z}$. Finden Sie Polynome $f, g \in \mathbb{F}_5[X]$ mit

$$(X^5 + X^2 + \overline{2}X - \overline{1})f + (X^2 + \overline{1})g = \overline{1}.$$

(Ihr Rechenweg ist mit anzugeben und sollte sich an § 8.1.2 orientieren.)

(c) Es sei $\mathfrak{a} = \langle X^5 + X^2 + \overline{2}X - \overline{1} \rangle$. Folgern Sie aus (b), dass $(X^2 + \overline{1}) + \mathfrak{a} \in \mathbb{F}_5[X]/\mathfrak{a}$ invertierbar ist und geben Sie das zugehörige multiplikativ inverse Element an.

13.2. *(Irreduzibilität von Polynomen mit kleinem Grad)* (4 Punkte)
Sei R ein Integritätsbereich. Ein Element $p \in R \setminus (R^\times \cup \{0_R\})$ heißt ***irreduzibel***, falls jede Zerlegung $p = ab$ mit $a, b \in R$ automatisch $a \in R^\times$ oder $b \in R^\times$ erfüllt. K sei ein beliebiger Körper und $f \in K[X]$ ein Polynom mit Grad n.

(a) Ist $n = 1$, so ist f irreduzibel. (Hinweis: Gradformel, Proposition 7.2.)

(b) Ist $n \in \{2, 3\}$, so ist f genau dann irreduzibel, wenn f keine Nullstelle in K besitzt. (Hinweis: Wenn $f = ab$ mit Polynomen a, b gilt, welche Grade kommen dann für a und b in Frage?)

(c) Gilt $1_K + 1_K \neq 0_K$, so ist das quadratische Polynom $aX^2 + bX + c \in K[X]$ ($a, b, c \in K$, $a \neq 0_K$) genau dann irreduzibel, wenn seine ***Diskriminante*** $b^2 - 4ac$ kein Quadrat in K ist (d.h. wenn es kein $x \in K$ mit $x^2 = b^2 - 4ac$ gibt).

(d) $3X^2 + 4X + 3$ ist irreduzibel als Polynom über $\mathbb{Z}[i\sqrt{5}]$, aber reduzibel als Polynom über $\mathbb{Q}[i\sqrt{5}]$. (Hinweis: Bei $\mathbb{Q}[i\sqrt{5}]$ handelt es sich sogar um einen Körper, wie man analog zu Aufgabe 9.1 sieht. Das dürfen Sie ohne Beweis benutzen.)

13.3. *(Längen von Zerlegungen in irreduzible Elemente)* (4 Punkte)
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:

Geben Sie Ihre Lösung bitte bis zum 24.01.2025, 13:00 Uhr, auf PANDA ab.

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

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

13.4. *(Die ganzen Gaußschen Zahlen, II)* (4 Punkte)
Betrachten Sie den Ring $\mathbb{Z}[\mathrm{i}]$ der ganzen Gaußschen Zahlen aus Aufgabe T9.2. Ferner sei $p \in \mathbb{N}$ eine Primzahl. Zeigen Sie:

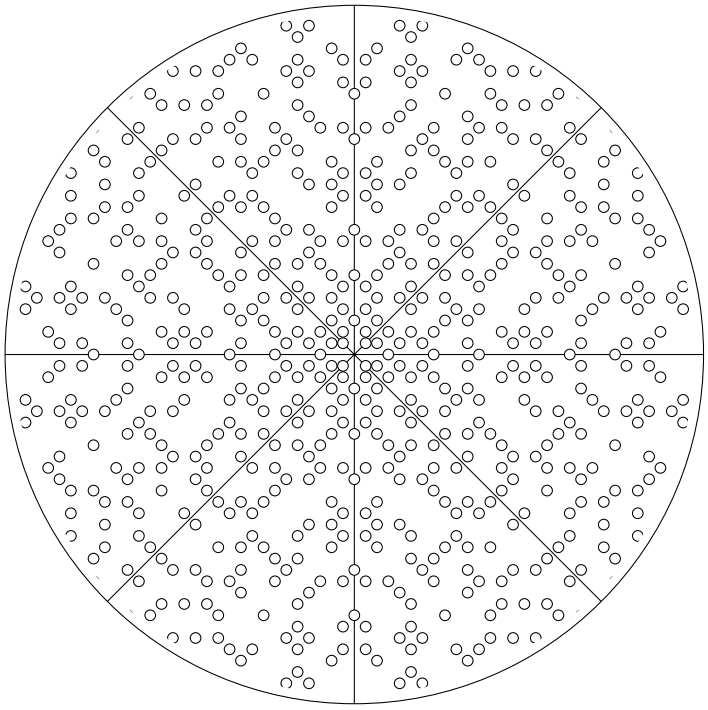
(a) Für jedes Primelement π von $\mathbb{Z}[\mathrm{i}]$ ist $N(\pi)$ entweder eine Primzahl in $\mathbb{N}$ oder das Quadrat einer solchen. (Hinweis: $N(\pi) = \pi\overline{\pi}$.)

(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 $\mathbb{Z}[\mathrm{i}]$.

(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.)