TECHNISCHE UNIVERSITÄT GRAZ
INSTITUT FÜR ANALYSIS UND ZAHLENTHEORIE
Marc Technau

Sommersemester 2023
Graz, den 22.06.2023

15. Übung zur Einführung in die Algebra

15.1. *(Faktorisieren von Polynomen)*
Zerlegen Sie die folgenden Polynome über $\mathbb{Z}[X]$ in Primfaktoren:

(a) $2X^2 + 4X + 2$,

(b) $6X^2 + 12$.

15.2. *(Irreduzibilität)*
Untersuchen Sie die folgenden Polynome auf Irreduzibilität:

(a) $X^4 + 4X^3 + 6X^2 + 4X + 10 \in \mathbb{Q}[X]$.

(b) $X^4 + 9 \in \mathbb{Q}[X]$.

(c) $X^2 + Y^2 - 1 \in \mathbb{Q}[X, Y]$. (Hinweis: $\mathbb{Q}[X, Y] \cong (\mathbb{Q}[X])[Y]$ und Eisenstein.)

(d) $X^2 + Y^2 \in \mathbb{R}[X, Y]$. (Hinweis: man faktorisiere zunächst in $\mathbb{C}[X, Y]$.)

(e) $X^4 + 4Y^4 \in \mathbb{R}[X, Y]$. (Hinweis: $X^2 + Y^2 - aXY$.)

Zeigen Sie ferner:

(f) Es gibt unendlich viele irreduzible Polynome $f \in \mathbb{Q}[X]$ mit $\deg f = 12$.

15.3. *(Faktorisierungsmethode von Kronecker)*
Es sei R ein Integritätsbereich mit unendlich vielen Elementen und $K = \operatorname{Quot}(R)$ sein Quotientenkörper. Für jedes $a \in R$ sei $T(a) = \{\, b \in R : b \mid a \,\}$ die Menge seiner Teiler und diese sei für alle $a \neq 0_R$ endlich.

(a) Es sei $f \in R[X]$ ein Polynom vom Grad $n > 1$ und m sei $\max\{\, r \in \mathbb{N} : 2r \leq n \,\}$. Zeigen Sie:

(1) Es gibt paarweise verschiedene $a_0, \dots, a_m \in R$ derart, dass die Mengen $T_i := T(f(a_i))$ für $i = 0, \dots, m$ endlich sind.

(2) Zu jedem $\boldsymbol{b} = (b_0, \dots, b_m) \in T_0 \times \cdots \times T_m =: T$ gibt es genau ein $g_{\boldsymbol{b}} \in K[X]$ mit Grad $\leq m$ und $g_{\boldsymbol{b}}(a_i) = b_i$ für $i = 0, \dots, m$.

(3) f ist genau dann reduzibel in $R[X]$, wenn es ein $\boldsymbol{b} \in T$ gibt derart, dass $g_{\boldsymbol{b}}$ in $R[X] \setminus R^\times \subseteq K[X]$ liegt und ein Teiler von f ist.

(b) Nun sei zusätzlich angenommen, dass für jedes $r \in R \setminus \{0_R\}$ die Menge $T(r)$ in endlich vielen „Rechenschritten“ bestimmbar ist und auch Addition und Multiplikation von Elementen in R in endlich vielen Rechenschritten durchführbar sind.

Dieses Blatt wird nicht mehr korrigiert und auch nicht besprochen.

Beschreiben Sie dann ein Verfahren, welches jedes Polynom aus $R[X]$ in endlich vielen Schritten in über R irreduzible Polynome zerlegt.

(c) Zerlegen Sie das folgende Polynom unter Anwendung der durch Teil (a) nahegelegten Methode in irreduzible Faktoren über $\mathbb{Z}$:

$$3X^5 + 2X^4 - 24X^3 - 26X^2 + 11X - 1.$$

(Achtung: dies ist ggf. aufwändig. Bloßes Hinschreiben einer geeigneten Faktorisierung und Prüfen, dass diese passt, ist nicht erlaubt. Der Rechenweg sollte — jedenfalls grob — ersichtlich sein.)

15.4. *(Die ganzen Gaußschen Zahlen, II)*
Betrachten Sie den Ring $\mathbb{Z}[\mathrm{i}]$ der ganzen Gaußschen Zahlen aus Aufgabe 12.2. Ferner sei $p \in \mathbb{N}$ eine Primzahl. Zeigen Sie:

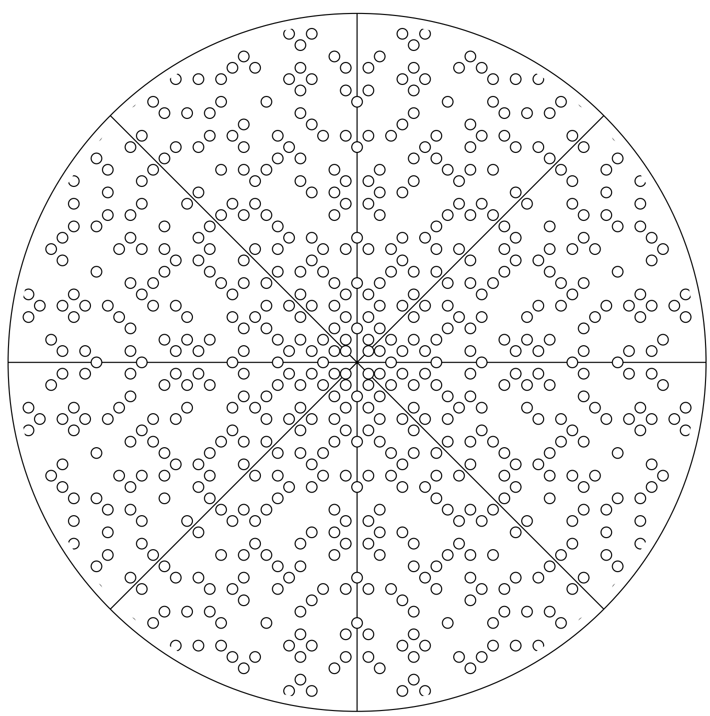
(a) Für jedes Primelement π von $\mathbb{Z}[\mathrm{i}]$ ist $N(\pi)$ entweder eine Primzahl in $\mathbb{N}$ oder das Quadrat einer solchen. (Hinweis: $N(\pi) = \pi\overline{\pi}$.)

(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 $0 \le a, b \le 6$ 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.)