Übungen zur Algebra I

Wintersemester 2020/21

Universität Heidelberg
Mathematisches Institut
Prof. Dr. A. Schmidt
Dr. M. Leonhardt

Blatt 03
Abgabetermin: Freitag, 27.11.2020, 9:15 Uhr

Aufgabe 1. *(Polynomring)* (6 Punkte) Es sei K ein Körper.

(a) (1 Punkt) Bestimmen Sie den ggT von $f = X^3 - 3$ und $g = X^2 - 4$ in $\mathbb{Q}[X]$.

(b) (1 Punkt) Bestimmen Sie den ggT von $f = X^3 - 3$ und $g = X^2 - 4$ in $\mathbb{F}_5[X]$.

(c) (2 Punkte) Zeigen Sie, dass $K[X]$ unendlich viele irreduzible, normierte Polynome enthält. *(Hinweis: Imitieren Sie den Beweis für die Unendlichkeit der Primzahlen in $\mathbb{Z}$.)*

(d) (2 Punkte) Es sei $f \in K[X]\backslash\{0\}$ und $L := K[X]/(f)$. Zeigen Sie, dass jede Restklasse $\overline{g} \in L$ einen eindeutigen Repräsentanten $g \in K[X]$ mit $\deg(g) < \deg(f)$ besitzt und folgern Sie $\dim_K L = \deg(f)$. Falls $\deg(f) \geq 1$, zeigen Sie weiter, dass $\overline{X} \in L$ eine Nullstelle von $f \in K[X] \subset L[X]$ ist.

Aufgabe 2. *(Irreduzible Polynome)* (6 Punkte; je 2 Punkte) Zeigen Sie, dass die folgenden Polynome irreduzibel sind:

(a) $X^3 + 2X^2 - 20 \in \mathbb{Q}[X]$,

(b) $X^6 + X^3 + 1 \in \mathbb{Q}[X]$,

(c) $X^7 + 2X^5Y + 3XY^3 + 4Y^3 + 5XY + 6X \in \mathbb{C}[X, Y]$.

Aufgabe 3. *(Nullstellen normierter Polynome über faktoriellen Ringen)* (6 Punkte) Es sei R ein faktorieller Ring mit Quotientenkörper $K := Q(R)$. Zeigen Sie:

(a) (1 Punkt) Sind $a, b, c \in R$ und gilt $a|bc$ sowie $\mathrm{ggT}(a, b) = 1$, so folgt $a|c$.

(b) (3 Punkte) Ist $f = X^n + a_{n-1}X^{n-1} + \ldots + a_0$ ein normiertes Polynom in $R[X]$ und $\alpha \in K$ eine Nullstelle von f, so liegt α bereits in R und ist dort ein Teiler von a_0.

(c) (2 Punkte) Das Polynom $X^3 + aX^2 + bX + 1 \in \mathbb{Z}[X]$ ist genau dann irreduzibel in $\mathbb{Z}[X]$ (oder $\mathbb{Q}[X]$), wenn $a \neq b$ und $a + b \neq -2$.

Aufgabe 4. *(Inhalt)* (6 Punkte; je 2 Punkte) Es sei R ein faktorieller Ring und $K := Q(R)$ sein Quotientenkörper. Für $f \in R[X]$ definieren wir den Inhalt $I(f) \in R$ als den ggT aller Koeffizienten von f (eindeutig bis auf Assoziiertheit). Für $f \in K[X]$ wählen wir ein $a \in R$ mit $af \in R[X]$ und definieren $I(f) := a^{-1}I(af) \in K$. Zeigen Sie:

(a) Für jedes $f \in K[X]$ existiert solch ein $a \in R$ und die Definition von $I(f)$ ist unabhängig von der Wahl von a. Bestimmen Sie $I(f)$ für $R = \mathbb{Z}$ und $f = \frac{3}{7}X^3 + X - 5 \in \mathbb{Q}[X]$.

(b) Für $f, g \in K[X]$ gilt $I(fg) = I(f)I(g)$.

(c) Sei $r \in R$, $f \in R[X]$ und $h(X) := f(X + r) \in R[X]$. Dann gilt $I(h) = I(f)$.

Bonusaufgabe 5. *(Zwei-Quadrate-Satz)* (6 Bonuspunkte) Wir wollen die schwierigere Implikation des folgenden Satzes zeigen: *Eine ungerade Primzahl p lässt sich genau dann als Summe zweier Quadratzahlen schreiben, wenn $p \equiv 1 \bmod 4$.*
Zuerst untersuchen wir den euklidischen Ring $\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}\}$ (vgl. Blatt 02, Aufgabe 1 und 5; siehe auch LA2, SS2020, Blatt 3, Aufgabe 13; verfügbar auf Mampf) zusammen mit der multiplikativen Normfunktion (= Betragsquadrat in $\mathbb{C}$)

$$N \colon \mathbb{Z}[i] \longrightarrow \mathbb{Z}, \quad N(a + bi) := a^2 + b^2.$$

(a) (1 Punkt) Zeigen Sie $\mathbb{Z}[i]^\times = \{\pm 1, \pm i\}$.

(b) (3 Punkte) Es sei $p \in \mathbb{Z}$ eine Primzahl der Form $p = 4n + 1$ mit $n \in \mathbb{N}$. Zeigen Sie: p teilt das Produkt $((2n)! + i)((2n)! - i) = (2n)!^2 + 1$, aber keinen der Faktoren, ist also kein Primelement in $\mathbb{Z}[i]$. *(Hinweis: Satz von Wilson, Blatt 01, Aufgabe 2)*

(c) (2 Punkte) Sei $\pi \in \mathbb{Z}[i]$ ein Primelement mit $\pi | p$ in $\mathbb{Z}[i]$. Benutzen Sie (a), um $N(\pi) = p$ zu zeigen. Folgern Sie, dass p Summe zweier Quadratzahlen ist.

Bemerkung: Die andere Richtung des Zwei-Quadrate-Satzes geht so: Da Quadratzahlen immer kongruent zu 0 oder 1 modulo 4 sind (wieso?), kann keine Primzahl $p \equiv 3 \bmod 4$ Summe zweier Quadratzahlen sein.