9. Übung zur Algebra

Prof. M. Geck, SoSe 2023

Aufgabe 1. Ist ein Polynom in $\mathbb{Z}[X]$ gegeben, so kann man oft das Reduktions-Kriterium (siehe Lemma 13.3) verwenden, um zu zeigen, dass dieses Polynom irreduzibel ist. Wir werden in dieser Aufgabe sehen, dass das Reduktions-Kriterium nicht für das Polynom $X^4 + 1$ funktioniert.

(a) Finden Sie Formeln für die 4 Nullstellen von $X^4 + 1 \in \mathbb{C}[X]$ in $\mathbb{C}$.

(b) Zeigen Sie: $X^4 + 1 \in \mathbb{Q}[X]$ ist irreduzibel.

(c) Sei p eine Primzahl und $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ Körper mit p Elementen. Sei $G := \{x^2 \mid x \in \mathbb{F}_p^\times\}$. Zeigen Sie, dass G eine Untergruppe von $\mathbb{F}_p^\times$ ist mit $[\mathbb{F}_p^\times : G] \leq 2$. Schließen Sie daraus: Sind $y_1, y_2 \in \mathbb{F}_p^\times$ gegeben mit $y_1 y_2 \notin G$, so folgt $y_1 \in G$ oder $y_2 \in G$.

(d) Schließen Sie mit Hilfe von (c), dass $X^4 + \bar{1} \in \mathbb{F}_p[X]$ für jede Primzahl p reduzibel ist.

[*Hinweis zu (a):* Es gilt zunächst $f = (X^2+i)(X^2-i)$; Sie müssen also noch $z \in \mathbb{C}$ finden mit $z^2 = \pm i$; machen Sie einen Satz $z = a+bi$ mit $a, b \in \mathbb{R}$. *Hinweis zu (b):* Sie können zum Beispiel die Formeln in (a) verwenden. *Hinweis zu (c):* $\mathbb{F}_p^\times$ ist zyklisch; siehe Beispiel 12.9 der Vorlesung. Wenn $[\mathbb{F}_p^\times : G] \leq 2$ gezeigt ist, so gilt außerdem: Ist $y \in \mathbb{F}_p^\times \setminus G$, so gilt $\mathbb{F}_p^\times = G \cup yG$ (disjunkte Vereinigung). *Hinweis zu (d):* Behandeln Sie $p = 2$ separat. Sei nun $p \geq 3$. Gibt es ein $a \in \mathbb{Z}$ mit $\bar{a}^2 = y_1 := \bar{2}$, so gilt $X^4+\bar{1} = (X^2+\bar{1})^2-\bar{2}X^2 = (X^2+1+\bar{a}X)(X^2+1-\bar{a}X)$. Verfahren Sie ähnlich für den Fall, dass es ein $b \in \mathbb{Z}$ gibt mit $\bar{b}^2 = y_2 := -\bar{1}$, oder ein $c \in \mathbb{Z}$ mit $\bar{c}^2 = -\bar{2}$. Benutzen Sie dann die Aussage in (c). Für weitere Hinweise und alternative Beweismöglichkeiten siehe auch `https://math.stackexchange.com/questions/427439/`]

Aufgabe 2. Für $n \geq 1$ sei $\Phi_n \in \mathbb{Z}[X]$ das n-te Kreisteilungspolynom mit $\mathrm{Grad}(\Phi_n) = \phi(n)$, wie in Satz 12.12 der Vorlesung.

(a) Zeigen Sie: Ist $n > 1$ ungerade, so gilt $\Phi_{2n} = \Phi_n(-X)$.
Zum Beispiel: $\Phi_3 = X^2 + X + 1$ und $\Phi_6 = X^2 - X + 1 = \Phi_3(-X)$.

(b) Finden Sie eine explizite Formel für Φ_n für den Fall, dass n eine Potenz von 2 ist.

Aufgabe 3. Sei $0 \neq f = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$. Zeigen Sie: Ist $\alpha = \frac{a}{b} \in \mathbb{Q}$ mit $a, b \in \mathbb{Z}$, $b \neq 0$ (gekürzter Bruch) eine Nullstelle von f, so gilt $a \mid a_0$ und $b \mid a_n$.

Aufgabe 4. Für jedes der folgenden Polynome bestimmen Sie eine Zerlegung als Produkt von irreduziblen Polynomen.

(i) $X^4 + 1$ in $\mathbb{R}[X]$; **(ii)** $X^7 + 11X^3 - 33X + 22$ in $\mathbb{Q}[X]$;
(iii) $X^3 + X^2 + X + 1$ in $\mathbb{Z}[X]$; **(iv)** $X^3 - 7X^2 + 3X + 3$ in $\mathbb{Q}[X]$;
(v) $X^3 + X + 763$ in $\mathbb{Z}[X]$: **(vi)** $X^4 + 4X^2 + 3$ in $\mathbb{Z}[X]$;
(vii) $X^5 + X^2 + X + 2$ in $\mathbb{Q}[X]$; **(viii)** $X^5 - X - 1$ in $\mathbb{Q}[X]$;
(ix) $2X^5 + 15X^4 + 9X^3 + 3$ in $\mathbb{Z}[X]$; **(x)** $X^4 + 15X^3 + 7$ in $\mathbb{Q}[X]$;
(xi) $X^4 + X^3 + X^2 + X + 1$ in $\mathbb{Z}[X]$; **(xii)** $X^4 + X^3 + X^2 + X + 1$ in $\mathbb{R}[X]$;
(xiii) $X^5 + X^4 + X^3 + X^2 + X + 1$ in $\mathbb{Z}[X]$; **(xiv)** $X^5 + 5X^4 + 10X^3 + 10X^2 + 25X + 26$ in $\mathbb{Z}[X]$.

[*Hinweis:* In einigen Fällen hilft es, anstelle des gegebenen Polynoms f das Polynom $f(X \pm 1)$ zu betrachten.]