UNIVERSITÄT PADERBORN
INSTITUT FÜR MATHEMATIK
Marc Technau
Nicolas Potthast

Wintersemester 2024/25
Paderborn, den 24.01.2025

14. Übung zur Algebra 1

14.1. *(Ein irreduzibles Polynom über $\mathbb{F}_p$)*
Für eine Primzahl p sei $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Zeigen Sie, dass das Polynom $f = X^p - X - 1 \in \mathbb{F}_p[X]$ irreduzibel ist.
(Hinweis: zeigen Sie, dass f invariant unter Einsetzen von $X+1$ für X ist. Betrachten Sie anschließend die hieraus hervorgehende Operation von $(\mathbb{F}_p, +) \cong (C_p, \oplus)$ auf der Menge der Primteiler von f.)

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

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

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

14.3. *(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 $\deg f = 12$.

14.4. *(Faktorisierungsmethode von Kronecker)*
Es sei R ein Integritätsbereich mit unendlich vielen Elementen und $K = \operatorname{Quot}(R)$ sein Quotientenkörper. (Sie dürfen auch gerne $R = \mathbb{Z}$ und $K = \mathbb{Q}$ annehmen, falls Ihnen das hilft.) 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 $a_0, \ldots, a_m \in R$ derart, dass die Mengen $T_i := T(f(a_i))$ für $i = 0, \ldots, m$ endlich sind.

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

Geben Sie Ihre Lösung bitte bis zum 31.01.2025, 13:00 Uhr, auf PANDA ab.

(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. 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.)