12. Übung zur Algebra

Prof. M. Geck, Dr. L. Iancu, WiSe 2023/2024

Aufgabe 1. (V) Bestimmen Sie Zerfällungskörper $L \supseteq \mathbb{Q}$ (jeweils als Teilkörper von $\mathbb{C}$) der folgenden Polynome $f \in \mathbb{Q}[X]$, sowie die Körpergrade $[L : \mathbb{Q}]$:

$$X^3 - 1, \qquad X^3 - 3, \qquad X^6 - 8, \qquad X^4 + 5X^2 + 6, \qquad X^5 - 1.$$

Hinweis : Für das letzte Polynom, bestimmen Sie zuerst $\cos(2\pi/5)$ und $\sin(2\pi/5)$.

Aufgabe 2. (Schriftlich, 8=2+2+2+2 Punkte) Sei $\alpha = 2\cos(2\pi/9) \in \mathbb{R}$.

(a) Zeigen Sie, dass α algebraisch über $\mathbb{Q}$ ist. Schreiben Sie dazu $\alpha = \zeta_9 + \zeta_9^{-1}$, wobei $\zeta_9 = e^{2\pi i/9} \in \mathbb{C}$ eine primitive neunte Einheitswurzel ist.

(b) Bestimmen Sie das Minimalpolynom $f = \mu_\alpha \in \mathbb{Q}[X]$ von α über $\mathbb{Q}$. Schreiben Sie dazu $\alpha = \zeta_9 + \zeta_9^{-1}$ wie in (a), berechnen Sie damit $\alpha^2, \alpha^3, \ldots$, und versuchen Sie, eine Linearkombination zwischen diesen Potenzen zu finden.

(c) Zeigen Sie (z.B. mit einer Kurvendiskussion), dass f drei verschiedene reelle Nullstellen hat. Zeigen Sie, dass $\beta = 2\cos(4\pi/9)$ und $\gamma = 2\cos(8\pi/9)$ die beiden weiteren Nullstellen sind.

(d) Nach **(c)** ist $L = \mathbb{Q}(\alpha, \beta, \gamma) \subseteq \mathbb{R}$ ein Zerfällungskörper von f. Bestimmen Sie $[L : \mathbb{Q}]$.

Aufgabe 3. (V) Sei $p = 3$ und $f := X^2 + \bar{1} \in \mathbb{F}_3[X]$. Dann ist f irreduzibel (keine Nullstelle in $\mathbb{F}_3$). Nach Vorlesung ist $K := \mathbb{F}_3[X]/(f)$ ein endlicher Körper mit $|K| = 3^2 = 9$. Sei $\alpha = \bar{X} \in K$; dann lässt sich jedes Element $x \in K$ eindeutig schreiben als $x = a_0 + a_1\alpha$ mit $a_0, a_1 \in \mathbb{F}_3$.

(a) Bestimmen Sie die Multiplikationstabelle für K, d.h., für $x = a_0 + a_1\alpha \in K$ und $y = b_0 + b_1\alpha \in K$ (mit $a_i, b_j \in \mathbb{F}_3$), bestimmen Sie $c_0, c_1 \in \mathbb{F}_3$ mit $x \cdot y = c_0 + c_1\alpha$.

(b) Bestimmen Sie ein Element $\gamma = c_0 + c_1\alpha \in K$ mit $K^\times = \langle\gamma\rangle$.

Aufgabe 4. (Schriftlich, 11=2+3+3+3 Punkte)
(a) Sei $p = 2$, $n = 3$ und $f := X^3 + X + \bar{1} \in \mathbb{F}_2[X]$. Zeigen Sie, dass f irreduzibel ist.
Nach Vorlesung ist $K = \mathbb{F}_2[X]/(f)$ ein Körper mit $|K| = 2^3 = 8$.

(b) Zeigen Sie, dass $K^\times = \langle\alpha\rangle$ gilt, wobei $\alpha = \bar{X} \in K$.

(c) Nach **(b)** gilt $K = \{0\} \cup \{\alpha^i \mid i = 0, 1, \ldots, 7\}$. Bestimmen Sie die Additionstabelle von K. D.h., für $x = \alpha^i \in K$ und $y = \alpha^j \in K$, finden Sie heraus, ob $x + y = 0$ gilt; wenn nicht, so finden Sie $l \in \{0, 1, \ldots, 7\}$ mit $x + y = \alpha^l$.

(d) Finden Sie $i \in \{0, 1, 2, \ldots, 7\}$ mit $(\alpha + \bar{1})^{-1} = \alpha^i$.

Aufgabe 5. (V) Sei $f := X^3 + \bar{3}X + \bar{4} \in \mathbb{F}_5[X]$.
(a) Wir betrachten den Faktorring $K = \mathbb{F}_5[X]/(f)$. Wieviele Elemente hat K ? Ist K ein Körper ? Sei $\alpha := \bar{X} \in K$; dann lässt sich jedes Element $x \in K$ eindeutig schreiben als $x = a_0 + a_1\alpha + a_2\alpha^2$ mit $a_0, a_1, a_2 \in \mathbb{F}_5$.

(b) Schreiben Sie in dieser Form folgende Elemente :
$\alpha^4, \quad \alpha^5, \quad (\bar{2}\alpha + \bar{3})(\bar{3}\alpha^2 + \alpha + \bar{4}), \quad (\bar{4}\alpha^2 + \bar{3})^2.$

(c) Bestimmen Sie $a_0, a_1, a_2 \in \mathbb{F}_5$ mit $(\bar{3} + \bar{4}\alpha^2)^{-1} = a_0 + a_1\alpha + a_2\alpha^2$.

Aufgabe 6. (Z) Sei p eine Primzahl und K ein endlicher Körper mit $|K| = p^n$, wobei $n \geq 1$. Ziel dieser Aufgabe ist es, einen Überblick über alle Teilkörper von K zu erhalten.

(a) Sei $K' \subseteq K$ ein Teilkörper. Dann haben wir Körpererweiterungen $\mathbb{F}_p \subseteq K' \subseteq K$. Schließen Sie daraus, dass $|K'| = p^d$ mit $d \in \mathbb{N}$ und $d \mid n$ gilt. Zeigen Sie dann $K' = \{x \in K \mid x^{p^d} = x\}$.

(b) Umgekehrt: Sei $d \in \mathbb{N}$ mit $d \mid n$. Zeigen Sie, dass dann $p^d - 1 \mid p^n - 1$ gilt. Schließen Sie daraus, dass $K' = \{x \in K \mid x^{p^d} = x\}$ ein Teilkörper von K mit $|K'| = p^d$ ist.

Damit ist also gezeigt: Ist $d \mid n$, so gibt es genau einen Teilkörper $K' \subseteq K$ mit $|K'| = p^d$ (nämlich $K' = \{x \in L \mid x^{p^d} = x\}$). Sonst gibt es keine weiteren Teilkörper von K.

Abgabe der schriftlichen Aufgaben: Am 22./23. Januar, vor den Übungsgruppen.