

12. Übung zur Algebra

Dr. L. Iancu, WiSe 2020/21

Aufgabe 1. Sei $f = X^3 + X + 1 \in \mathbb{Q}[X]$.

(a) Zeigen Sie, dass f irreduzibel ist.

(b) Zeigen Sie (z.B. mit einer Kurvendiskussion), dass f eine reelle und zwei konjugiert-komplexe Nullstellen besitzt. Seien dies $\alpha_1, \alpha_2, \alpha_3$, wobei $\alpha_1 \in \mathbb{R}$ und $\alpha_3 = \bar{\alpha}_2 \in \mathbb{C} \setminus \mathbb{R}$.

(c) Sei $L := \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) \subseteq \mathbb{C}$ Zerfällungskörper von f . Bestimmen Sie $[L : \mathbb{Q}]$. (Nach Satz 17.4 der Vorlesung wissen wir bereits, dass $[L : \mathbb{Q}] \leq 3! = 6$ gilt.)

Aufgabe 2. (Schriftlich, 8 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 $\alpha^2, \alpha^3, \dots$, 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. (Schriftlich, 7 Punkte) Nach Beispiel 17.8 der Vorlesung gibt es drei normierte irreduzible Polynome in $\mathbb{F}_3[X]$ vom Grad 2, nämlich $f_1 = X^2 + \bar{1}$, $f_2 = X^2 + X + \bar{2}$, $f_3 = X^2 + \bar{2}X + \bar{2}$. Entsprechend erhalten wir drei Körper $K_i = \mathbb{F}_3[X]/(f_i)$ ($i = 1, 2, 3$) mit 9 Elementen, die aber nach Satz 17.7 zueinander isomorph sind.

(a) Für $i = 1, 2, 3$ sei $\alpha_i := X + (f_i) \in K_i$. Zeigen Sie für $i = 2, 3$, dass $K_i^\times = \langle \alpha_i \rangle$ gilt, und damit $K_i = \{0\} \cup \{1, \alpha_i, \alpha_i^2, \alpha_i^3, \alpha_i^4, \alpha_i^5, \alpha_i^6, \alpha_i^7\}$. Für $i = 1$ ist dagegen $\langle \alpha \rangle \subsetneq K_1^\times$, also wird K_1 am besten als $K_1 = \{a + b\alpha_1 \mid a, b \in \mathbb{F}_3\}$ beschrieben.

(b) Geben Sie konkret einen Isomorphismus $\varphi: K_2 \rightarrow K_1$ an. Wegen $K_2^\times = \langle \alpha_2 \rangle$ ist φ eindeutig festgelegt durch $\varphi(\alpha_2) \in K_1$; es sind also $a, b \in \mathbb{F}_3$ anzugeben mit $\varphi(\alpha_2) = a + b\alpha_1$. Geben Sie analog einen Isomorphismus $\varphi: K_3 \rightarrow K_1$ an.

Aufgabe 4. Sei $f = X^4 + X^3 + X^2 + X + 1 \in \mathbb{F}_2[X]$; nach Ü8A3, ist dieses Polynom irreduzibel in $\mathbb{F}_2[X]$ und damit $K = \mathbb{F}_2[X]/(f)$ ein Körper mit 16 Elementen. Sei nun $\alpha := X + (f) \in K$.

(a) Bestimmen Sie die Ordnung von α in $K^\times$.

(b) Finden Sie einen Erzeuger γ der zyklischen Gruppe $K^\times$.

(c) Bestimmen Sie Ausdrücke in der Form $\sum_{i=0}^3 c_i \alpha^i$ mit $c_i \in \mathbb{F}_2$ für die folgenden Elemente :

$$\alpha^4, \alpha^6, \alpha^{-1}, (\alpha^3 + 1)^2, (\alpha^2 + \alpha + 1)^{-1}.$$

(d) Bestimmen Sie Ausdrücke in der Form γ^i für die folgenden Elemente :

$$\alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^{-1}, (\alpha^3 + 1)^2.$$

Aufgabe 5. Für jede der folgenden Zahlen n entscheiden Sie ob ein Körper K mit $|K| = n$ existiert oder nicht. Wenn ja, geben Sie eine konkrete Konstruktionsmethode an :

$$n = 8, 25, 27, 32, 37, 81, 121, 144, 343, 625, 1000.$$

Aufgabe 6. (Zum Selbststudium) 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 $K' = \{x \in K \mid x^{p^d} = x\}$). Sonst gibt es keine weiteren Teilkörper von K .

Abgabe der schriftlichen Aufgaben: Bis Mittwoch, den 3.02., vor den Übungsgruppen.