

Aufgabe	A3	A4	A5	Σ
Punkte				

Aufgabe 3. (a) Beh.: Mit $\mathbb{F}_9 = \mathbb{F}_3/(X^2 + 1)$ ist $\mathbb{F}_9 = \mathbb{F}_3(\overline{X})$ und $\text{Gal}(\mathbb{F}_9/\mathbb{F}_3) = \langle \sigma \rangle$ wobei $\sigma: \mathbb{F}_9 \rightarrow \mathbb{F}_9$ den Frobenius-Automorphismus bezeichne

Beweis. Sei $f := X^2 + 1 \in \mathbb{F}_3[X]$. Betrachte zunächst $K := \mathbb{F}_3/(f)$. Es ist f irreduzibel, da $\deg(f) = 2$, also falls f reduzibel, zerfiele f in Linearfaktoren über $\mathbb{F}_3$. Jedoch hat f keine Nullstellen in $\mathbb{F}_3$, denn $f(0) = 1$, $f(1) = 2$ und $f(2) = 2$. Also ist K Körper, da $\mathbb{F}_3[X]$ euklidisch und damit HIR.

Nach einem der ersten Zettel gilt $\dim_{\mathbb{F}_3} K = \deg(f) = 2$. Da $\#\mathbb{F}_3 = 3$ folgt $\#K = 3^2 = 9$. Also folgt $K \cong \mathbb{F}_9$. Weiter gilt mit dieser Konstruktion von $\mathbb{F}_9$: $\mathbb{F}_9 = \mathbb{F}_3(\overline{X})$, denn für $g \in \mathbb{F}_9$ ist

$$g = aX + b + (X^2 + 1) = a\overline{X} + b$$

für $a, b \in \mathbb{F}_3$.

Jede algebraische Erweiterung eines endlichen Körpers ist separabel und normal, also $\mathbb{F}_9/\mathbb{F}_3$ galoissch und nach VL gilt $\text{Gal}(\mathbb{F}_9/\mathbb{F}_3) = \langle \sigma^r \rangle$ wobei σ^r der relative Frobenius-Automorphismus mit $r = 1$, da $3 = 3^1$. Damit folgt die Behauptung. $\square$

(b) Beh.: $\mathbb{Q}(\sqrt{3}, \sqrt{5}) = \mathbb{Q}(\sqrt{3} + \sqrt{5})$ und $\text{Gal}(\mathbb{Q}(\sqrt{3}, \sqrt{5})/\mathbb{Q}) = \langle \sigma, \tau \rangle$ mit (angegeben mit den Werten auf den Erzeugern $\sqrt{3}$ und $\sqrt{5}$):

$$\begin{aligned} \sigma(\sqrt{3}) &= -\sqrt{3} & \sigma(\sqrt{5}) &= \sqrt{5} \\ \tau(\sqrt{3}) &= \sqrt{3} & \tau(\sqrt{5}) &= -\sqrt{5}. \end{aligned}$$

Beweis. Sei $L := \mathbb{Q}(\sqrt{3} + \sqrt{5})$. Zunächst ist $L \ni (\sqrt{3} + \sqrt{5})^2 = 3 + 2\sqrt{3}\sqrt{5} + 5$, also $\sqrt{3}\sqrt{5} \in L$. Damit ist $L \ni (\sqrt{3} + \sqrt{5})\sqrt{3}\sqrt{5} - 3(\sqrt{3} + \sqrt{5}) = 3\sqrt{5} + 5\sqrt{3} - 3\sqrt{3} - 3\sqrt{5} = 2\sqrt{3}$. Also $\sqrt{3} \in L$ und damit auch $\sqrt{5} \in L$. Da trivialerweise $\sqrt{3} + \sqrt{5} \in \mathbb{Q}(\sqrt{3}, \sqrt{5})$ folgt $L = \mathbb{Q}(\sqrt{3}, \sqrt{5})$.

Weiter ist $\text{char } \mathbb{Q} = 0$ also L separabel und $f = (X^2 - 3)(X^2 - 5)$ hat in L genau die vier Nullstellen $N = \{\pm\sqrt{3}, \pm\sqrt{5}\}$. L ist also Zerfällungskörper von f über K , insbesondere normal. Außerdem ist $[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt{3})] = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \cdot 2 = 4$. Also $\#\text{Gal}(L/\mathbb{Q}) = 4$.

$L/\mathbb{Q}$ hat die Zwischenkörper $\mathbb{Q}(\sqrt{3})$ und $\mathbb{Q}(\sqrt{5})$. Diese sind Zerfällungskörper der nach Eisenstein über $\mathbb{Q}$ irreduziblen Polynome $X^2 - 3$ und $X^2 - 5$. Ihre Galoisgruppen operieren also transitiv auf den entsprechenden Nullstellen. Diese werden erzeugt von den entsprechenden Einschränkungen von σ bzw. τ . Damit ergibt sich die Galoisgruppe von L als $\langle \sigma, \tau \rangle$. $\square$

Aufgabe 4. Sei L/K endliche Erweiterung.

Lemma 4.1. Für $\alpha \in L$ und zwei Zwischenkörper M, M' von $K(\alpha)/K$ gilt

$$M \subseteq M' \iff f_M \in M'[X]$$

wobei f_M das Minimalpolynom von α über M bezeichne.

Beweis. „ $\implies$ “ ist trivial. Seien nun M, M' Zwischenkörper von L/K mit $f_M \in M'[X]$. Dann seien $a_0, \dots, a_n \in M \cap M'$ die Koeffizienten von f_M . Dann setze $M'' := K(a_0, \dots, a_n)$. Dann folgt $M'' \subseteq M$ und $M'' \subseteq M'$. Da f_M irreduzibel über M , insbesondere irreduzibel über M'' , also $f_M = f_{M''}$ und damit

$$\deg(f_M) = [K(\alpha) : M''] = \underbrace{[K(\alpha) : M]}_{=\deg(f_M)} [M : M''],$$

also $M = M''$ und damit $M \subseteq M'$. $\square$

Beh.: Siehe Aufgabe.

Beweis. Falls K endlich, ist K vollkommen, also jede algebraische Erweiterung separabel und damit nach dem Satz vom primitiven Element einfach. Außerdem ist dann auch L endlich, also hat L nur endlich viele Teilmengen, insbesondere existieren nur endlich viele Zwischenkörper von L/K .

Sei also K unendlich.

- „(i) $\implies$ (ii)“: Sei $L = K(\alpha)$ und zu jedem Zwischenkörper M von L/K sei $f_M \in M[X]$ das Minimalpolynom von α über M . Seien nun M, M' zwei Zwischenkörper von L/K mit $f_M = f_{M'}$. Damit ist $f_M \in M'[X]$ und $f_{M'} \in M[X]$ also $M \subseteq M'$ und $M' \subseteq M$ nach Lemma 4.1, insgesamt $M = M'$. Also bestimmt jedes f_M den Körper M eindeutig.

Weiter ist $f_K(\alpha) = 0$ und $f_M(\alpha) = 0$. Außerdem ist $f_K \in M[X]$ und f_M Minimalpolynom von α über M , also $f_K \in (f_M)$. Damit ex. ein $g \in M[X]$, s.d. $f_K = gf_M$. Da $M \subseteq L$ folgt $g \in L[X]$. Also $f_M \mid f_K$ in $L[X]$.

Da $L[X]$ faktoriell, besitzt f_K eine eindeutige (endliche) Primfaktorzerlegung in $L[X]$. Insbesondere hat f_K in $L[X]$ nur endlich viele Teiler. Also existieren mit den Vorüberlegungen nur endlich viele Zwischenkörper von L/K .

- „(ii) $\implies$ (i)“: L/K habe nur endlich viele Zwischenkörper.

Sei zunächst $L = K(\alpha, \beta)$. Dann existieren $c, c' \in K$ mit $c \neq c'$ und $K(\alpha + c\beta) = K(\alpha + c'\beta)$ (Da $\#K = \infty$, gäbe es sonst unendlich Zwischenkörper von L/K der Form $K(\alpha + c\beta)$ mit $c \in K$).

Z.z.: $\alpha, \beta \in K(\alpha + c\beta)$. Es ist $\alpha + c'\beta \in K(\alpha + c\beta)$. Also

$$K(\alpha + c\beta) \ni \alpha + c\beta - (\alpha + c'\beta) = \beta(c - c').$$

Da $c \neq c'$ folgt $c - c' \in K^\times$ und damit $\beta \in K(\alpha + c\beta)$. Also auch $\alpha \in K(\alpha + c\beta)$. Da trivialerweise $\alpha + c\beta \in K(\alpha, \beta)$ folgt $L = K(\alpha + c\beta)$, also L einfach.

Sei nun $L = K(\alpha_1, \dots, \alpha_n)$. Induktion über n : Für $n = 1$ ist L trivialerweise einfach. Sei nun $n \in \mathbb{N}$ und $L = K(\alpha_1, \dots, \alpha_{n+1})$. Nach IV existiert ein $\alpha \in L$ mit $K(\alpha_1, \dots, \alpha_n) = K(\alpha)$. Also folgt $L = K(\alpha, \alpha_{n+1})$. Damit ist L einfach mit der Vorüberlegung. □

Aufgabe 5. Sei L/K endlich, galoissch und abelsch. Sei weiter $f \in K[X]$ irreduzibel mit $\alpha \in L$ und $f(\alpha) = 0$.

Beh.: $M := K(\alpha)$ ist Zerfällungskörper von f über K und ein endlicher, normaler Zwischenkörper von L/K .

Beweis. Es ist M/K endlich, denn $[M : K] = \deg(f) < \infty$. Es ist $K \subseteq M \subseteq L$ d.h. nach dem Hauptsatz der Galoisstheorie ex. eine Untergruppe $H \subseteq \text{Gal}(L/K)$ mit $L^H = M$. Es ist $\text{Gal}(L/K)$ abelsch, also H Normalteiler in $\text{Gal}(L/K)$. Insbesondere ist L^H/K normal also M/K normal. Außerdem ist $\alpha \in M$ und M normal also zerfällt f über M in Linearfaktoren. Wegen $M = K(\alpha)$ wird M von den Nullstellen von f erzeugt, also ist M Zerfällungskörper von f über K . □