

Aufgabe	A1	A2	A3	A4	Σ
Punkte					

Aufgabe 1. (a) Es ist L Zerfällungskörper von f über K , also L/K normal. Außerdem ist f irreduzibel und $f' = nx^{n-1}$ und $\text{char } K \nmid n$ also $f' \neq 0$. Also f separabel. Also sind die Nullstellen von f separabel und da L von den Nullstellen von f über K erzeugt, folgt L/K separabel, insgesamt also galoissch.

Sei nun $b \in L$ eine Nullstelle von f und $\mu_n = \{\zeta_1, \dots, \zeta_n\}$. Diese sind paarw. verschieden. Setze nun $\alpha_k := \zeta_k b$. Dann ist für $k \in \{1, \dots, n\}$:

$$f(\alpha_k) = (\zeta_k b)^n - a = \zeta_k^n b^n - a = b^n - a = 0.$$

Das heißt α_k sind Nullstellen von f und paarweise verschieden (Ang. es gäbe $i \neq j$ mit $\alpha_i = \alpha_j \implies \zeta_i = \zeta_j \not\Rightarrow$), also sind die n Nullstellen von f genau die $(\alpha_k)_{k=1}^n$. Da $\mu_n \subseteq K$ folgt $\alpha_k \in K(b) \forall k \in \{1, \dots, n\}$, also $L = K(b)$.

(b) Sei $\beta \in L$ eine Nullstelle von f . Dann sind analog zu (a) $\alpha_k = \zeta_k \beta$ die Nullstellen von f .

- Z.z.: ψ wohldefiniert. Seien b, b' Nullstellen von f . Dann ex. $i, j \in \{1, \dots, n\}$, s.d. $b = \zeta_i \beta$ und $b' = \zeta_j \beta$. Dann folgt

$$\frac{\sigma(b)}{b} = \frac{\sigma(\zeta_i \beta)}{\zeta_i \beta} = \frac{\zeta_i \sigma(\beta)}{\zeta_i \beta} = \frac{\sigma(\beta)}{\beta} = \frac{\zeta_j \sigma(\beta)}{\zeta_j \beta} = \frac{\sigma(\zeta_j \beta)}{\zeta_j \beta} = \frac{\sigma(b')}{b'}.$$

- Z.z.: ψ Gruppenhomomorphismus Seien $\sigma, \tau \in \text{Gal}(L/K)$. Dann ex. ein $i \in \{1, \dots, n\}$, s.d. $\tau(\beta) = \alpha_i$. Dann gilt

$$\psi(\sigma \circ \tau) = \frac{\sigma \circ \tau(\beta)}{\beta} = \frac{\sigma(\zeta_i \beta)}{\beta} = \frac{\beta \zeta_i \sigma(\beta)}{\beta^2} = \frac{\tau(\beta)}{\beta} \frac{\sigma(\beta)}{\beta}.$$

- Z.z.: ψ injektiv. Sei $\sigma \in \text{Gal}(L/K)$ mit $\psi(\sigma) = 1$. Dann ex. ein $i \in \{1, \dots, n\}$, s.d. $\sigma(\beta) = \alpha_i$. Damit folgt

$$1 = \psi(\sigma) = \frac{\sigma(\beta)}{\beta} = \frac{\zeta_i \beta}{\beta} = \zeta_i.$$

Also $\sigma(\beta) = \beta$. Da L/K von β erzeugt wird, legt $\sigma(\beta)$ σ eindeutig fest, d.h. $\sigma = \text{id}$.

- Z.z.: $\text{Bild}(\psi) = \mu_n$. Sei $\sigma \in \text{Gal}(L/K)$. Dann ex. ein $i \in \{1, \dots, n\}$, s.d. $\sigma(\beta) = \zeta_i \beta$. Also

$$\psi(\sigma) = \frac{\sigma(\beta)}{\beta} = \frac{\zeta_i \beta}{\beta} = \zeta_i \in \mu_n.$$

Also folgt $\text{Bild}(\psi) \subseteq \mu_n$. Da $L = K(\beta)$ und f Mipo von β , folgt $[L : K] = n$, also $\#\text{Gal}(L/K) = n$. Da ψ injektiv, ist also $\#\text{Bild}(\psi) = n$ und da $\#\mu_n = n$ folgt $\text{Bild}(\psi) = \mu_n$.

Damit ist also $\text{Gal}(L/K) \cong \mu_n$. Da μ_n zyklisch, folgt $\text{Gal}(L/K)$ zyklisch.

(c) Betrachte $K = \mathbb{Q}$, $f = X^4 - 2$. Dann ist f irred. nach Eisenstein und nach Blatt 5 ist $L = \mathbb{Q}(\sqrt[4]{2}, i)$ und $\text{Gal}(L/\mathbb{Q}) \cong D_4$, aber D_4 ist nicht abelsch, insbesondere nicht zyklisch.

Aufgabe 2. Zunächst beachte:

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \text{GL}_2(\mathbb{F}_p) \iff \begin{vmatrix} a & b \\ 0 & d \end{vmatrix} = ad \neq 0 \stackrel{\mathbb{F}_p \text{ nullt.frei.}}{\iff} a \neq 0 \wedge d \neq 0.$$

Damit ist

$$G = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in M_{2,2}(\mathbb{F}_p) \mid a, b, d \in \mathbb{F}_p, a \neq 0 \neq d \right\}.$$

Damit folgen

$$\begin{aligned}
 G \begin{pmatrix} 0 \\ 0 \end{pmatrix} &= \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} 0 \\ 0 \end{pmatrix} \mid a, b, d \in \mathbb{F}_p, a \neq 0 \neq d \right\} \\
 &= \left\{ \begin{pmatrix} 0 \\ 0 \end{pmatrix} \right\} \\
 G \begin{pmatrix} 1 \\ 0 \end{pmatrix} &= \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} \mid a, b, d \in \mathbb{F}_p, a \neq 0 \neq d \right\} \\
 &= \left\{ \begin{pmatrix} a \\ 0 \end{pmatrix} \mid a \in \mathbb{F}_p^\times \right\} \\
 G \begin{pmatrix} 0 \\ 1 \end{pmatrix} &= \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} \mid a, b, d \in \mathbb{F}_p, a \neq 0 \neq d \right\} \\
 &= \left\{ \begin{pmatrix} b \\ d \end{pmatrix} \mid b, d \in \mathbb{F}_p, d \neq 0 \right\}.
 \end{aligned}$$

- (a) Es ist $\begin{pmatrix} 0 \\ 0 \end{pmatrix} \notin G \begin{pmatrix} 1 \\ 0 \end{pmatrix} \cup G \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ und $\begin{pmatrix} 1 \\ 0 \end{pmatrix} \notin G \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Da V in die disjunkte Vereinigung der Bahnen zerfällt, sind also $G \begin{pmatrix} 0 \\ 0 \end{pmatrix}, G \begin{pmatrix} 1 \\ 0 \end{pmatrix}, G \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ paarw. verschieden.

Sei nun $x \in V$ beliebig. Dann ex. $a, b \in \mathbb{F}_p$ mit $x = \begin{pmatrix} a \\ b \end{pmatrix}$. Falls $a = b = 0$, dann folgt $x \in G \begin{pmatrix} 0 \\ 0 \end{pmatrix}$.

Falls $b \neq 0$. Dann ist

$$\underbrace{\begin{pmatrix} 1 & a \\ 0 & b \end{pmatrix}}_{\in G} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} a \\ b \end{pmatrix} = x \implies x \in G \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

Falls $b = 0$, dann ist $a \neq 0$ und es gilt

$$\underbrace{\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix}}_{\in G} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} a \\ 0 \end{pmatrix} = x \implies x \in G \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Das zeigt die Behauptung.

- (b) Seien nun $x_1 := \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, $x_2 := \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ und $x_3 := \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. Es ist offensichtlich $G_{x_1} = G$.

Es gilt

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \iff \begin{pmatrix} a \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \iff a = 1.$$

Also folgt

$$G_{x_2} = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in M_{2,2}(\mathbb{F}_p) \mid a, b, d \in \mathbb{F}_p, d \neq 0, a = 1 \right\}.$$

Weiter gilt

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \iff \begin{pmatrix} b \\ d \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \iff b = 0 \wedge d = 1.$$

Also folgt

$$G_{x_3} = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in M_{2,2}(\mathbb{F}_p) \mid a, b, d \in \mathbb{F}_p, a \neq 0, b = 0, d = 1 \right\}.$$

- (c) Für die Bahnen siehe Vorbemerkung. Es ist ebenfalls nach Vorbemerkung $\#G = (p-1)^2 p$. Mit (b) folgt nun:

- $\#(Gx_1) = 1$ und $\#G_{x_1} = \#G$, also $\#G_{x_1} \#(Gx_1) = \#G$.
- $\#(Gx_2) = p-1$ und $\#G_{x_2} = p(p-1)$, also $\#G_{x_2} \#(Gx_2) = (p-1)^2 p = \#G$.
- $\#(Gx_3) = p(p-1)$ und $\#G_{x_3} = p-1$, also $\#G_{x_3} \#(Gx_3) = (p-1)^2 p = \#G$.

(d) Es ist nach Lagrange

$$(G : G_x) = \frac{\#G}{\#G_x} = \frac{(p-1)^2 p}{\#G_x}.$$

Also folgt durch Einsetzen der Ergebnisse aus (c): $(G : G_{x_1}) = 1$, $(G : G_{x_2}) = p - 1$ und $(G : G_{x_3}) = (p - 1)p$. Damit folgt

$$1 + (p - 1)p + p - 1 = 1 + p^2 - p + p - 1 = p^2 = \#V.$$

Aufgabe 3. (a) Sei G endlich mit $\#G = 2020$. Dann ist $2020 = 2^2 \cdot 5 \cdot 101$. Da $101 \mid \#G$, ex. ein $a \in G$ mit $\text{ord}(a) = 101$, also $H := \langle a \rangle$ ist 101-Gruppe und $101 \nmid 2^2 \cdot 5 = (G : H)$, also H 101-Sylowgruppe. Sei s die Anzahl der 101-Sylowgruppen. Nach Sylowsätzen gilt nun $s \mid \#G$ und $s \equiv 1 \pmod{101}$. Da aber $2^2 \cdot 5 < 101$ sind alle Teiler $t \neq 1$ von 2020 mit $101 \nmid t$, bereits $t \not\equiv 1 \pmod{101}$. Also folgt $s = 1$.

Da alle 101-Sylowgruppen zueinander konjugiert sind, gilt für $g \in G$: $gHg^{-1} = H$. Also ist H Normalteiler in G . Außerdem ist $\#H = 101$, also $H \cong \mathbb{Z}/101\mathbb{Z}$, insbesondere abelsch.

(b) Sei G endlich mit $\#G = 2021$. Es ist $2021 = 43 \cdot 47$. Da $43 < 47$ und $43 \nmid 46 = 47 - 1$ folgt nach VL, dass G zyklisch ist und damit $G \cong \mathbb{Z}/2021\mathbb{Z}$.

(c) Sei G endlich mit $\#G = 36 = 2^2 \cdot 3^2$. Sei s die Anzahl der 3-Sylowgruppen. Es ist $s \mid \#G$ und $s \equiv 1 \pmod{3}$, also folgt $s \in \{1, 4\}$, da $2 \equiv 2 \pmod{3}$. Falls $s = 1$: Wende Argument aus (a) an.

Falls $s = 4$: Dann sei X die Menge der 3-Sylowgruppen auf denen G mittels Konjugation wirkt. Es ist dann $\#X = 4$ und $\forall H \in X$ ist $\#H = 9$, also $\{1\} \neq H \neq G$. Sei $\varphi: G \rightarrow \mathfrak{S}(X) \cong \mathfrak{S}_4$, der zur Konjugationswirkung assoziierte Gruppenhomomorphismus. Da

$$\#\mathfrak{S}_4 = 4! = 24 < 36 = \#G$$

folgt $\ker \varphi \neq \{1\}$. Falls $\varphi(G) = \{\text{id}\}$: Dann ist für $H \in X$ und $g \in G$:

$$gHg^{-1} = H^g = \varphi(g)H = H.$$

Also H nicht-trivialer Normalteiler in G . Sei nun $\#\varphi(G) > 1$: Da $G/\ker \varphi \cong \varphi(G)$, folgt $\#\varphi(G)\#\ker \varphi = \#G$. Da $\#\varphi(G) > 1$, folgt also $\#\ker \varphi < 36$, also insgesamt $G \neq \ker \varphi \neq \{1\}$. Damit ist $\ker \varphi$ nicht-trivialer Normalteiler in G .

Aufgabe 4. (a) Sei $(x_1 \dots x_r)$ ein r -Zykel in $\mathfrak{S}_n$ und $\sigma \in \mathfrak{S}_n$ beliebig. Sei $x \in \{1, \dots, n\}$.

Falls es ex. ein $i \in \{1, \dots, r\}$ mit $\sigma^{-1}(x) = x_i$, dann ist $\sigma(x_i) = x$ und $(x_1 \dots x_r)x_i = x_{i+1}$ mit $x_{r+1} := x_1$. Dann gilt

$$\sigma(x_1 \dots x_r)\sigma^{-1}(x) = \sigma(x_1 \dots x_r)x_i = \sigma(x_{i+1}) = (\sigma(x_1) \dots \sigma(x_r))\sigma(x_i) = (\sigma(x_1) \dots \sigma(x_r))x.$$

Falls $\sigma^{-1}(x) \notin \{x_1, \dots, x_r\}$, dann ist $x \notin \{\sigma(x_1), \dots, \sigma(x_r)\}$ und

$$\sigma(x_1 \dots x_r)\sigma^{-1}(x) = \sigma\sigma^{-1}(x) = x = (\sigma(x_1) \dots \sigma(x_r))x.$$

(b) Für ein Produkt aus zwei 2-er Zykeln gilt für $\sigma \in \mathfrak{S}_n$:

$$\sigma(x_1 x_2)(x_3 x_4)\sigma^{-1} = \sigma(x_1 x_2)\sigma^{-1}\sigma(x_3 x_4)\sigma^{-1} \stackrel{(a)}{=} (\sigma(x_1)\sigma(x_2))(\sigma(x_3)\sigma(x_4)).$$

Also ist ein Produkt aus zwei 2-er Zykeln nach Konjugation wieder ein Produkt aus zwei 2-er Zykeln. Außerdem ist, falls $x_1, \dots, x_4$ paarweise verschieden, auch $\sigma(x_1), \dots, \sigma(x_4)$ paarweise verschieden, da σ injektiv. Außerdem gilt $\sigma \text{id} \sigma^{-1} = \text{id}$.

Da $\mathfrak{V}_4$ gerade aus id und allen Produkten aus zwei 2-er Zykeln mit paarweise verschiedenen Einträgen besteht, folgt $\sigma\mathfrak{V}_4\sigma^{-1} = \mathfrak{V}_4$, also $\mathfrak{V}_4$ Normalteiler in $\mathfrak{S}_4$.

(c) Es ist $1 \triangleleft \mathfrak{V}_4$ trivial und $\#\mathfrak{V}_4/1 = \#\mathfrak{V}_4 = 4 = 2^2$, also $\mathfrak{V}_4/1$ abelsch.

Da $\mathfrak{V}_4 \triangleleft \mathfrak{S}_4$ und $\text{sgn}(\sigma) = 1 \forall \sigma \in \mathfrak{V}_4$ folgt $\mathfrak{V}_4 \triangleleft \mathfrak{A}_4$. Da $\#\mathfrak{A}_4 = \frac{4!}{2} = 12$ folgt $\#\mathfrak{A}_4/\mathfrak{V}_4 = 3$, also $\mathfrak{A}_4/\mathfrak{V}_4$ abelsch.

Da $\mathfrak{A}_4 = \ker \text{sgn}$ ist $\mathfrak{A}_4 \triangleleft \mathfrak{S}_4$ und $\#\mathfrak{S}_4/\mathfrak{A}_4 = 2$, also $\mathfrak{S}_4/\mathfrak{A}_4$ abelsch.