Klausur Algebra

Prof. Dr. C. Löh/F. Hofmann 9. Februar 2026

Matrikelnummer: | | | | | | | |

- Diese Klausur besteht aus 7 Seiten. Bitte überprüfen Sie, ob Sie alle Seiten erhalten haben.
- Bitte versehen Sie *alle* Seiten mit Ihrer Matrikelnummer.
- Bitte schreiben Sie Lösungen zu verschiedenen Aufgaben auf verschiedene Blätter. Sie können Ihre Lösungen direkt in die Klausur schreiben.
- Beginn: 9:00. Sie haben 120 Minuten Zeit, um die Klausur zu bearbeiten; bitte legen Sie Ihren Studierendenausweis oder Lichtbildausweis zu Beginn der Klausur vor sich auf den Tisch. Um Unruhe in den letzten Minuten zu vermeiden, geben Sie bitte entweder um 11:00 Uhr oder vor 10:40 Uhr ab.
- Die Klausur besteht aus 6 Aufgaben. Es können im Total 60 Punkte erreicht werden. Zum Bestehen genügen voraussichtlich 50% der Punkte.
- Es sind keinerlei Hilfsmittel wie Taschenrechner, Computer, Bücher, Vorlesungsmitschriften, Mobiltelephone etc. gestattet; Papier wird zur Verfügung gestellt. *Alle* Täuschungsversuche führen zum Ausschluss von der Klausur; die Klausur wird dann als nicht bestanden gewertet!
- Fragen zur Klausur können nur schriftlich (unter Angabe von Matrikelnummer und Aufgabennummer) gestellt werden. Es werden nur Fragen beantwortet, die auf missverständlich oder inkorrekt gestellten Aufgaben beruhen. Inhaltliche Fragen werden nicht beantwortet. Antworten werden schriftlich gegeben.

Viel Erfolg!

Aufgabe	1	2	3	4	5	6	Summe
Punkte maximal	10	10	10	10	12	8	60
erreichte Punkte							

Note: Unterschrift:

Aufgabe 1 $(1 + 3 + 3 + 3 = 10$ Punkte**).**

1. Geben Sie die Definition für den Begriff des *Index* einer Untergruppe.
2. Zeigen Sie, dass S_5 eine Untergruppe vom Index 24 enthält.
3. Gibt es einen surjektiven Gruppenhomomorphismus $A_5 \longrightarrow \mathbb{Z}/3$?
   Begründen Sie Ihre Antwort.
4. Ist für jede auflösbare Gruppe G auch $G \times G$ auflösbar?
   Begründen Sie Ihre Antwort.

Lösung:

1. Sei G eine Gruppe und sei $H \subset G$ eine Untergruppe. Die Anzahl (bzw. Kardinalität)
$$[G : H] := \#\{g \cdot H \mid g \in G\}$$
der Linksnebenklassen von H in G bezeichnet man als *Index von H in G*.

2. Sei H die von $\sigma := (1\ 2\ 3\ 4\ 5)$ erzeugte Untergruppe von S_5. Wegen $\operatorname{ord}\sigma = 5$ ist $\#H = \#(\mathbb{Z}/5) = 5$.
   Mit dem Satz von Lagrange (angewendet auf die Kette $\{e\} \subset H \subset G$) folgt
$$[G : H] = \frac{\#G}{\#H} = \frac{\#S_5}{5} = \frac{5!}{5} = 4! = 24.$$

3. *Behauptung.* Nein, es gibt keinen Gruppenhomomorphismus $A_5 \longrightarrow \mathbb{Z}/3$, der surjektiv ist.

   Beweis. Angenommen, es gäbe einen Gruppenhomomorphismus $\varphi\colon A_5 \longrightarrow \mathbb{Z}/3$, der surjektiv ist. Mit dem Homomorphiesatz folgt
$$A_5/\ker\varphi \cong_{\mathsf{Group}} \mathbb{Z}/3.$$
   Insbesondere wäre dann $\ker\varphi$ ein Normalteiler von A_5 mit $\ker\varphi \neq \{e\}$ und $\ker\varphi \neq A_5$. Dies widerspricht der Tatsache, dass die Gruppe A_5 einfach ist.
   Also gibt es keinen solchen Gruppenhomomorphismus. □

4. *Behauptung.* Ja, ist G eine auflösbare Gruppe, so ist auch $G \times G$ auflösbar.

Beweis. Sei $\pi\colon G \times G \longrightarrow G$ die Projektion auf die zweite Komponente und $N := \ker \pi$. Dann ist N ein Normalteiler von $G \times G$ mit $N = G \times \{e\} \cong_{\mathsf{Group}} G$ und der Homomorphiesatz liefert

$$(G \times G)/N \cong_{\mathsf{Group}} \operatorname{im} \pi = G.$$

Mit den Vererbungseigenschaften auflösbarer Gruppen folgt somit aus der Auflösbarkeit von G (die die Auflösbarkeit von N und $(G \times G)/N$ nach sich zieht) auch die Auflösbarkeit von $G \times G$.

[Alternativ kann man auch induktiv die abgeleiteten Gruppen von $G \times G$ berechnen.] □

Aufgabe 2 ($1 + 3 + 3 + 3 = 10$ Punkte).

1. Geben Sie die Definition dafür, dass ein Ideal eines Ringes *prim* ist.
2. Zeigen Sie: Ist R ein Ring und $p \subset R$ ein Primideal, so ist der Ring R/p *nicht* isomorph zum Ring $\mathbb{Q} \times \mathbb{Q}$.
3. Ist das Ideal $(2 \cdot X + 2)$ in $\mathbb{Q}[X]$ prim?

   Begründen Sie Ihre Antwort.
4. Ist das Polynom $T^3 + T + 1 \in \mathbb{Q}[T]$ in $\mathbb{Q}[T]$ irreduzibel?

   Begründen Sie Ihre Antwort.

Lösung:

1. Sei R ein Ring. Ein Ideal $p \subset R$ in R ist *prim*, wenn $p \neq R$ ist und

$$\forall_{x,y \in R} \quad x \cdot y \in p \Longrightarrow (x \in p \vee y \in p).$$

2. Sei R ein Ring und sei $p \subset R$ ein Primideal. Dann ist R/p ein Integritätsring.

   Der Ring $\mathbb{Q} \times \mathbb{Q}$ ist jedoch *kein* Integritätsring, da etwa $(1, 0)$ ein nicht-trivialer Nullteiler ist: Es gilt $(1, 0) \neq (0, 0)$ und $(0, 1) \neq (0, 0)$, aber

$$(1, 0) \cdot (0, 1) = (1 \cdot 0, 0 \cdot 1) = (0, 0).$$

3. *Behauptung.* Ja, das Ideal $(2 \cdot X + 2)$ in $\mathbb{Q}[X]$ ist prim.

   Beweis. Da 2 eine Einheit in $\mathbb{Q}[X]$ ist, folgt $(2 \cdot X + 2) = (X + 1)$.

   Das Polynom $X + 1$ in $\mathbb{Q}[X]$ ist (aus Gradgründen) irreduzibel.

   Da $\mathbb{Q}[X]$ als Polynomring über einem Körper ein faktorieller Ring (sogar ein Hauptidealring) ist, ist somit das Ideal $(X + 1)$ ein Primideal in $\mathbb{Q}[X]$.

   [Alternativ kann man zeigen, dass der Restklassenring $\mathbb{Q}[X]/(2 \cdot X + 2) \cong_{\mathsf{Ring}} \mathbb{Q}$ ein Integritätsring ist, und daraus schließen, dass das Ideal prim ist.] □

4. *Behauptung.* Ja, das Polynom $T^3 + T + 1$ in $\mathbb{Q}[T]$ ist irreduzibel.

Beweis. Es ist $\mathbb{Q} = Q(\mathbb{Z})$ und das gegebene Polynom $f := T^3 + T + 1$ liegt in $\mathbb{Z}[T]$ und erfüllt $\deg f > 0$.

Wir verwenden das Reduktionskriterium bezüglich der Primzahl $2 \in \mathbb{Z}$: Die Primzahl 2 teilt den höchsten Koeffizienten von f nicht und Reduktion modulo 2 liefert das Polynom

$$\overline{f} := T^3 + T + [1] \in \mathbb{F}_2[T].$$

Das Polynom $\overline{f}$ ist in $\mathbb{F}_2[T]$ nach dem Nullstellenkriterium irreduzibel, denn $\deg \overline{f} = 3$ und $\overline{f}$ besitzt wegen

$$\overline{f}([0]) = [1] \neq [0] \quad \text{und} \quad \overline{f}([1]) = [1] + [1] + [1] = [1] \neq [0]$$

keine Nullstellen in $\mathbb{F}_2$.

Nach dem Reduktionskriterium ist somit f in $\mathbb{Q}[T]$ irreduzibel. □

Aufgabe 3 $(1 + 3 + 3 + 3 = 10$ Punkte**).**

1. Geben Sie die Definition dafür, dass eine algebraische Körpererweiterung *normal* ist.
2. Zeigen Sie, dass die Körpererweiterung $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \mid \mathbb{Q}$ algebraisch und normal ist.
3. Ist jede endliche Körpererweiterung von $\mathbb{Q}$ normal?

   Begründen Sie Ihre Antwort.
4. Gibt es einen Körper K mit $K^\times \cong_{\mathsf{Group}} \mathbb{Z}/17$?

   Begründen Sie Ihre Antwort.

Lösung:

1. Eine algebraische Körpererweiterung $L \mid K$ ist *normal*, wenn für jedes $\alpha \in L$ das Minimalpolynom von α über K bereits in $L[T]$ in Linearfaktoren zerfällt.
2. Die Elemente $\sqrt{2}$ und $\sqrt{3}$ sind algebraisch über $\mathbb{Q}$ (als Nullstellen von $T^2 - 2$ bzw. $T^2 - 3 \in \mathbb{Q}[T]$).

   Also ist die von $\sqrt{2}$ und $\sqrt{3}$ erzeugte Körpererweiterung $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \mid \mathbb{Q}$ algebraisch.

   Da $T^2 - 2$ und $T^2 - 3$ in $\mathbb{Q}[T]$ normiert und irreduzibel sind (z.B. nach dem Eisensteinschen Irreduzibilitätskriterium), handelt es sich dabei bereits um die Minimalpolynome von $\sqrt{2}$ bzw. $\sqrt{3}$ über $\mathbb{Q}$. Diese zerfallen über $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ in Linearfaktoren, denn

   $$T^2 - 2 = (T - \sqrt{2}) \cdot (T + \sqrt{2}) \quad \text{und} \quad T^2 - 3 = (T - \sqrt{3}) \cdot (T + \sqrt{3}).$$

   Somit ist die von $\sqrt{2}$ und $\sqrt{3}$ erzeugte Körpererweiterung $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \mid \mathbb{Q}$ normal.
3. *Behauptung.* Nein, nicht jede endliche Körpererweiterung von $\mathbb{Q}$ ist normal.

   Beweis. Die Körpererweiterung $\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q}$ ist endlich, da sie von dem über $\mathbb{Q}$ algebraischen Element $\sqrt[3]{2}$ erzeugt wird.

   Diese Körpererweiterung ist jedoch *nicht* normal, denn: Es ist $\mu := T^3 - 2 \in \mathbb{Q}[T]$ das Minimalpolynom von $\sqrt[3]{2}$ über $\mathbb{Q}$ (z.B. nach dem Eisensteinschen Irreduzibilitätskriterium).

Es ist $\zeta_3 \cdot \sqrt[3]{2} \in \mathbb{C}$ eine nicht-reelle Nullstelle von μ. Wegen $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ liegt diese Nullstelle *nicht* in $\mathbb{Q}(\sqrt[3]{2})$. Somit zerfällt μ über $\mathbb{Q}(\sqrt[3]{2})$ *nicht* in Linearfaktoren. Daher ist $\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q}$ *nicht* normal. □

4. *Behauptung.* Nein, es gibt *keinen* Körper K mit $K^\times \cong_{\mathsf{Group}} \mathbb{Z}/17$.

   Beweis. Angenommen, es gäbe einen solchen Körper K. Wegen $K^\times = K \setminus \{0\}$ wäre dann

   $$\#K = 1 + \#K^\times = 1 + \#(\mathbb{Z}/17) = 1 + 17 = 18.$$

   Insbesondere wäre K ein endlicher Körper.

   Nach der Klassifikation der endlichen Körper müsste somit $\#K = 18$ eine Primpotenz sein. Wegen der Primfaktorzerlegung $18 = 2 \cdot 3^2$ ist dies jedoch nicht der Fall.

   Dieser Widerspruch zeigt, dass es keinen solchen Körper K gibt. □

Aufgabe 4 $(3 + 3 + 4 = 10$ Punkte**).**

1. Formulieren Sie den *kleinen Satz von Fermat*.
2. Beweisen Sie den kleinen Satz von Fermat.
3. Bestimmen Sie die letzte Ziffer der Dezimaldarstellung von 7^{33}.

Lösung:

1. Sei $p \in \mathbb{N}$ prim. Dann gilt
$$x^{p-1} \equiv 1 \mod p$$
für alle $x \in \mathbb{Z}$ mit $p \nmid x$.
[Alternativ könnte man auch die verallgemeinerte Version formulieren:
Sei $m \in \mathbb{N}_{>0}$. Dann gilt
$$x^{\varphi(m)} \equiv 1 \mod m$$
für alle $x \in \mathbb{Z}$ mit $\mathrm{ggT}(x, m) = 1$.]

2. *Beweis.* Wir beweisen dies, indem wir die dazu äquivalente Behauptung
$$\forall_{z \in (\mathbb{Z}/(p)) \setminus \{0\}} \quad z^{p-1} = [1]$$
in $\mathbb{Z}/(p)$ beweisen.
Wir wissen, dass $\mathbb{Z}/(p)$ ein Körper ist; insbesondere ist $(\mathbb{Z}/(p)) \setminus \{0\}$ eine Gruppe bezüglich Multiplikation mit genau $p - 1$ Elementen.
Mit dem Satz von Lagrange folgt, dass $z^{p-1} = [1]$ für alle $z \in \mathbb{Z}/(p) \setminus \{0\}$ gilt. □
[Wird im ersten Teil die verallgemeinerte Version formuliert, so ist auch die verallgemeinerte Version zu beweisen:

Beweis. Wir beweisen die zur Behauptung äquivalente Aussage
$$\forall_{x \in \mathbb{Z}} \quad \mathrm{ggT}(x, m) = 1 \Longrightarrow [x]^{\varphi(m)} = [1]$$
in $\mathbb{Z}/(m)$.
Sei $x \in \mathbb{Z}$ mit $\mathrm{ggT}(x, m) = 1$. Nach den Eigenschaften der eulerschen φ-Funktion ist $[x]$ dann eine Einheit in $\mathbb{Z}/(m)$.
Außerdem enthält die Einheitengruppe $\mathbb{Z}/(m)^\times$ von $\mathbb{Z}/(m)$ genau $\varphi(m)$ Elemente. Mit dem Satz von Lagrange erhalten wir daher in $\mathbb{Z}/(m)$:
$$[x]^{\varphi(m)} = [1]$$ □
]

3. Wir verwenden die verallgemeinerte Version des kleinen Satzes von Fermat: Es gilt

$$\varphi(10) = \#\{1,3,7,9\} = 4.$$

Wegen $\mathrm{ggT}(7,10) = 1$ gilt in $\mathbb{Z}/(10)$:

$$[7^{33}] = [7]^{33} = [7]^{4\cdot 8+1} = ([7]^4)^8 \cdot [7]^1 = [1]^8 \cdot [7] = [7]$$

Also ist 7 die letzte Ziffer von 7^{33} im Dezimalsystem.

[Alternativ kann man mit der nicht-verallgemeinerten Version und dem chinesischen Restsatz argumentieren:

- In $\mathbb{Z}/(2)$ gilt (da 7 ungerade ist)

$$[7^{33}] = [7]^{33} = [1]^{33} = [1].$$

- In $\mathbb{Z}/(5)$ gilt nach dem kleinen Fermat (da 5 prim und $\mathrm{ggT}(7,5) = 1$ ist):

$$[7^{33}] = [7]^{33} = [7]^{4\cdot 8+1} = ([7]^4)^8 \cdot [7]^1 = [1]^8 \cdot [7] = [7] = [2].$$

- Wegen $\mathrm{ggT}(2,5) = 1$ liefert der chinesische Restsatz, dass die kanonischen Projektionen einen Ringisomorphismus $\mathbb{Z}/(10) \cong_{\mathsf{Ring}} \mathbb{Z}/(2) \times \mathbb{Z}/(5)$ definieren. Das Urbild von $([1],[2])$ unter diesem Isomorphismus ist $[7]$.

Also ist $[7^{33}] = [7]$ in $\mathbb{Z}/(10)$, und damit ist 7 die letzte Ziffer von 7^{33} im Dezimalsystem.]

[Alternativ kann man auch $33 = 2^5 + 1$ nutzen und $[7^{33}] \in \mathbb{Z}/(10)$ durch iteriertes Quadrieren bestimmen.]

[Alternativ kann man auch mit viel Geduld ausrechnen, dass

$$7^{33} = 773099371970744452413709 4407$$

ist (keine gute Idee!) und davon die letzte Ziffer als 7 ablesen.]

Aufgabe 5 ($3+3+3+3=12$ Punkte). Sei $\alpha \in \mathbb{C}$ mit

$$(\alpha - 1)^4 = 3$$

1. Zeigen Sie, dass $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ ist.
2. Zeigen Sie, dass $[\mathbb{Q}(\sqrt[5]{3}, \alpha) : \mathbb{Q}(\alpha)] = 5$ ist.
3. Zeigen Sie, dass $\#\operatorname{Gal}(\mathbb{Q}(\alpha), \mathbb{Q}) = 2$ ist.
4. Ist $\mathbb{Q}(\alpha)$ ein Zerfällungskörper von $(T-1)^4 - 3$ über $\mathbb{Q}$?
   Begründen Sie Ihre Antwort.

Lösung:

1. Es bietet sich an, die folgende Vorüberlegung zu machen: Sei $\beta := \alpha - 1$. Dann gilt $\mathbb{Q}(\beta) = \mathbb{Q}(\alpha)$ (da $-1 \in \mathbb{Q}$) und $\beta^4 = 3$.

   Sei $\mu \in \mathbb{Q}[T]$ das Minimalpolynom von β über $\mathbb{Q}$. Dann gilt $\mu = T^4 - 3$, denn dieses Polynom ist normiert, liegt in $\mathbb{Q}[T]$, hat β als Nullstelle und ist über $\mathbb{Q} = Q(\mathbb{Z})$ irreduzibel (nach dem Eisensteinschen Irreduzibilitätskriterium bezüglich der Primzahl 3 in $\mathbb{Z}$).

   Also ist $[\mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\beta) : \mathbb{Q}] = \deg \mu = 4$.

   [Ohne die Vorüberlegung kann man alternativ auch feststellen, dass das Polynom $(T-1)^4 - 3 = T^4 - 4 \cdot T^3 + 6 \cdot T^2 - 4 \cdot T - 2$ das Minimalpolynom von α über $\mathbb{Q}$ ist (nach Eisenstein bezüglich der Primzahl 2 in $\mathbb{Z}$).]

2. Es gilt $[\mathbb{Q}(\sqrt[5]{3}) : \mathbb{Q}] = 5$ (das Minimalpolynom von $\sqrt[5]{3}$ über $\mathbb{Q}$ ist nach Eisenstein $T^5 - 3$).

   Also ist $\operatorname{ggT}([\mathbb{Q}(\sqrt[5]{3}) : \mathbb{Q}], [\mathbb{Q}(\alpha) : \mathbb{Q}]) = \operatorname{ggT}(5, 4) = 1$. Mit der Gradformel für Komposita ergibt sich somit

   $$[\mathbb{Q}(\sqrt[5]{3}, \alpha) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[5]{3}) \cdot \mathbb{Q}(\alpha) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[5]{3}) : \mathbb{Q}] \cdot [\mathbb{Q}(\alpha) : \mathbb{Q}] = 5 \cdot 4.$$

   Mit der Multiplikativität des Grades erhalten wir daraus

   $$[\mathbb{Q}(\sqrt[5]{3}, \alpha) : \mathbb{Q}(\alpha)] = \frac{[\mathbb{Q}(\sqrt[4]{3}, \alpha) : \mathbb{Q}]}{[\mathbb{Q}(\alpha) : \mathbb{Q}]} = \frac{5 \cdot 4}{4} = 5.$$

3. Sei $X := \{x \in \mathbb{Q}(\beta) \mid \mu(x) = 0\}$ Nach dem Konjugationsprinzip ist

$$\#\operatorname{Gal}(\mathbb{Q}(\alpha), \mathbb{Q}) = \#\operatorname{Gal}(\mathbb{Q}(\beta), \mathbb{Q}) = \#X.$$

Es gilt

$$X = \{x \in \mathbb{Q}(\beta) \mid x^4 = 3\} = \{\sqrt[4]{3}, -\sqrt[4]{3}, i \cdot \sqrt[4]{3}, -i \cdot \sqrt[4]{3}\} \cap \mathbb{Q}(\beta).$$

Wegen $\beta \in X$ können wir die folgenden Fälle unterscheiden:

① Sei $\beta = \sqrt[4]{3}$ (analog: $\beta = -\sqrt[4]{3}$). Dann ist $-\beta \in X$ und $\mathbb{Q}(\beta) \subset \mathbb{R}$.
Insbesondere liegen $\pm i \cdot \sqrt[4]{3}$ nicht in $\mathbb{Q}(\beta)$.
Also ist $\#X = \#\{\sqrt[4]{3}, -\sqrt[4]{3}\} = 2$.

② Sei $\beta = i \cdot \sqrt[4]{3}$ (analog: $\beta = -\sqrt[4]{3}$). Dann ist $-\beta \in X$.
Nach dem ersten Fall ist $\pm\sqrt[4]{3}$ nicht in $\mathbb{Q}(\beta)$.
Also ist $\#X = \#\{i \cdot \sqrt[4]{3}, -i \cdot \sqrt[4]{3}\} = 2$.

In beiden Fällen ergibt sich also $\#\operatorname{Gal}(\mathbb{Q}(\alpha), \mathbb{Q}) = 2$.

[Da $\mathbb{Q}(\alpha) \mid \mathbb{Q}$ keine Galoiserweiterung ist, kann man nicht den Hauptsatz der Galoistheorie direkt auf die Körpererweiterung $\mathbb{Q}(\alpha) \mid \mathbb{Q}$ anwenden.]

4. *Behauptung.* Nein, $\mathbb{Q}(\alpha)$ ist *kein* Zerfällungskörper von $(T-1)^4 - 3$ über $\mathbb{Q}$.

Beweis. Angenommen, $\mathbb{Q}(\alpha)$ wäre ein Zerfällungskörper von $(T-1)^4 - 3$ über $\mathbb{Q}$. Dann wäre $\mathbb{Q}(\alpha) \mid \mathbb{Q}$ eine endliche Galoiserweiterung (endlich nach dem ersten Teil, normal nach der Annahme, separabel aufgrund von Charakteristik 0).

Dann wäre (nach den Berechnungen im ersten bzw. dritten Teil)

$$4 = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \#\operatorname{Gal}(\mathbb{Q}(\alpha), \mathbb{Q}) = 2,$$

was nicht sein kann. □

Aufgabe 6 (2 + 3 + 3 = 8 Punkte)**.** Sei $L \mid K$ eine endliche Galoiserweiterung, sei $G := \mathrm{Gal}(L, K)$ und es gelte $\#G = 75$.

1. Bestimmen Sie die Anzahl der 5-Sylowgruppen von G.

   Begründen Sie Ihre Antwort.

2. Zeigen Sie, dass es genau einen Zwischenkörper M von $L \mid K$ gibt, der $[M : K] = 3$ erfüllt.

3. Zeigen Sie, dass es ein Element in L gibt, dessen Minimalpolynom über K den Grad 15 besitzt.

Lösung:

1. Sei s_5 die Anzahl der 5-Sylowgruppen von G. Nach den Sylowsätzen gilt

   $$s_5 \equiv 1 \mod 5 \quad \text{und} \quad s_5 \mid 75,$$

   und damit $s_5 \in \{1, 6, 11, 16, \dots\} \cap \{1, 3, 5, 15, 25, 75\} = \{1\}$. Also ist $s_5 = 1$.

   [Behauptungen wie „Es gibt eine 5-Sylowgruppe in G.“ o.ä. geben den Sachverhalt nicht vollständig wieder. Korrekt wäre in diesem Fall „Es gibt genau eine 5-Sylowgruppe in G.“ Dies ist ein fundamentaler Unterschied.]

2. Ist M ein Zwischenkörper von $L \mid K$, so gilt (da $L \mid K$ und $L \mid M$ endliche Galoiserweiterungen sind)

   $$[M : K] = \frac{[L : K]}{[L : M]} = \frac{\#\,\mathrm{Gal}(L, K)}{\#\,\mathrm{Gal}(L, M)} = \big[G : \mathrm{Gal}(L, M)\big].$$

   Nach dem Hauptsatz der Galoistheorie ist die Anzahl der Zwischenkörper M von $L \mid K$ mit $[M : K] = 3$ also genau die Anzahl der Untergruppen H von G mit $[G : H] = 3$.

   Nach dem Satz von Lagrange stimmt letztere Anzahl mit der Anzahl der Untergruppen H von G mit $\#H = 75/3 = 25$ überein.

   Wegen $75 = 3 \cdot 5^2$ ist diese Anzahl also die Anzahl aller 5-Sylowgruppen von G.

   Nach dem ersten Teil ist diese Anzahl 1.

   [Oft wurde nur die Existenz gezeigt oder eine Mischversion, bei der nicht klar war, ob Existenz oder Eindeutigkeit gezeigt wird (da nicht deutlich gesagt wurde, was vorausgesetzt wird und was konstruiert wird).]

3. Wegen $\#G = 75 = 3 \cdot 5^2$ enthält G nach dem Satz von Cauchy ein Element g der Ordnung 5. Sei $H := \langle g \rangle_G$. Dann ist $H \cong_{\mathsf{Group}} \mathbb{Z}/5$, und damit $\#H = 5$.

   Nach dem Hauptsatz der Galoistheorie gibt es einen Zwischenkörper M von $L \mid K$ mit (nämlich $M = L^H$)

   $$[M : K] = [G : H] = \frac{\#G}{\#H} = \frac{75}{5} = 15.$$

   Da $M \mid K$ eine endliche separable Körpererweiterung ist, gibt es nach dem Satz vom primitiven Element ein $\alpha \in M$ mit $M = K(\alpha)$.

   Sei $\mu \in K[T]$ das Minimalpolynom von α über K. Dann ist

   $$\deg \mu = [K(\alpha) : K] = [M : K] = 15.$$

P.S.:

- Die Zahlen 15, 25, 24, 1, 34 sind in $\mathbb{Z}$ *nicht* prim.
- Die Zahl 2 ist in $\mathbb{Q}$ *nicht* prim.