Wiederholungsklausur zur Algebra

Prof. Dr. C. Löh/D. Fauser/J. Witzig 4. April 2018

Name: Vorname:

Matrikelnummer: ☐☐☐☐☐☐☐ Übungsleiter:

- Diese Klausur besteht aus 8 Seiten. Bitte überprüfen Sie, ob Sie alle Seiten erhalten haben.
- Bitte versehen Sie *alle* Seiten mit Ihrem Namen und Ihrer Matrikelnummer.
- Bitte schreiben Sie nicht Lösungen zu verschiedenen Aufgaben auf dasselbe Blatt.
- Sie haben zwei Stunden (= 120 Minuten) Zeit, um die Klausur zu bearbeiten; bitte legen Sie Ihren Studentenausweis und einen Lichtbildausweis zu Beginn der Klausur vor sich auf den Tisch und halten Sie die Ausweise bei der Abgabe bereit. 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 7 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!

Viel Erfolg!

Aufgabe	1	2	3	4	5	6	7	Summe
Punkte maximal	9	9	9	9	9	9	6	60
erreichte Punkte								

Note: Unterschrift:

Aufgabe 1 (3 + 3 + 3 = 9 Punkte)**.** Welche der folgenden Aussagen sind wahr? Begründen Sie jeweils kurz Ihre Antwort.

1. Für jede Gruppe G gilt

$$\forall_{g \in G} \quad \exists_{h \in G} \quad h \cdot g \cdot h^{-1} = g^{-1}.$$

2. Für jeden Gruppenhomomorphismus $f\colon G \longrightarrow H$ ist $\operatorname{im} f \cong \ker f$.

3. Die Gruppe $S_3 \times S_3$ ist auflösbar.

Lösung:

1. Diese Aussage ist falsch, denn: Sei etwa $G := \mathbb{Z}$ und $g := 1 \in \mathbb{Z}$. Da G abelsch ist, gilt für jedes $h \in \mathbb{Z}$ (wobei wir die Verknüpfung additiv statt multiplikativ schreiben)
$$h + g + (-h) = g = 1 \neq -1 = -g.$$

2. Diese Aussage ist falsch, denn: Zum Beispiel erhalten wir für den Gruppenhomomorphismus $f := \operatorname{id}_{\mathbb{Z}}\colon \mathbb{Z} \longrightarrow \mathbb{Z}$, dass

$$\operatorname{im} f = \mathbb{Z} \not\cong \{0\} = \ker f.$$

3. Diese Aussage ist wahr, denn: Wir betrachten $H := S_3 \times \{e\} \subset S_3 \times S_3 =: G$. Dann ist H ein Normalteiler in G und $G/H \cong S_3$. Da S_3 bekanntlich auflösbar ist, sind also H und G/H auflösbar. Nach den Vererbungseigenschaften auflösbarer Gruppen ist somit auch G auflösbar.

   [Die Tatsache, dass jede Gruppe mit weniger als 60 Elementen auflösbar ist, zu verwenden, ist etwas unsportlich, und sollte eigentlich nur dann verwendet werden, wenn man sie auch selbst beweisen kann.]

Aufgabe 2 (3 + 3 + 3 = 9 Punkte)**.** Welche der folgenden Aussagen sind wahr? Begründen Sie jeweils kurz Ihre Antwort.

1. Das Polynom $T^{2018} - 4 \cdot T^{1009} + 4 \in \mathbb{Z}[T]$ ist irreduzibel in $\mathbb{Z}[T]$.
2. Ist R ein Hauptidealring, so ist auch $R[T]$ ein Hauptidealring.
3. Es gibt ein irreduzibles Polynom $f \in \mathbb{Q}[X,Y]$ mit $\mathbb{Q}[X,Y]/(f) \cong \mathbb{Q} \times \mathbb{Q}$.

Lösung:

1. Diese Aussage ist falsch, denn: Es gilt
$$T^{2018} - 4 \cdot T^{1009} + 4 = (T^{1009} - 2)^2$$
und $T^{1009} - 2 \neq 0$ ist *keine* Einheit in $\mathbb{Z}[T]$.
2. Diese Aussage ist falsch, denn: Der Ring $\mathbb{Z}$ ist ein Hauptidealring, aber $\mathbb{Z}[T]$ ist *kein* Hauptidealring (zum Beispiel ist $(2,T)$ *kein* Hauptideal in $\mathbb{Z}[T]$).
3. Diese Aussage ist falsch, denn: *Angenommen*, es gäbe ein irreduzibles Polynom $f \in \mathbb{Q}[X,Y]$ mit $\mathbb{Q}[X,Y]/(f) \cong \mathbb{Q} \times \mathbb{Q}$. Da $\mathbb{Q} \times \mathbb{Q}$ kein Integritätsring ist, ist das Ideal (f) *nicht* prim in $\mathbb{Q}[X,Y]$. Also ist f *nicht* irreduzibel (der Ring $\mathbb{Q}[X,Y]$ ist faktoriell).

Aufgabe 3 (3 + 3 + 3 = 9 Punkte)**.** Welche der folgenden Aussagen sind wahr? Begründen Sie jeweils kurz Ihre Antwort.

1. Es gibt eine transzendente Körpererweiterung über $\mathbb{F}_{17}$.
2. Ist K ein endlicher Körper, so ist die additive Gruppe $(K, +)$ zyklisch.
3. Jede separable Körpererweiterung ist eine Galoiserweiterung.

Lösung:

1. Diese Aussage ist wahr, denn: Die Körpererweiterung $\mathbb{F}_{17}(T) \mid \mathbb{F}_{17}$ des rationalen Funktionenkörpers über $\mathbb{F}_{17}$ ist eine transzendente Körpererweiterung.
2. Diese Aussage ist falsch, denn: *Angenommen,* $(\mathbb{F}_4, +)$ wäre zyklisch. Wegen $|\mathbb{F}_4| = 4$ enthielte $\mathbb{F}_4$ insbesondere ein Element der additiven Ordnung 4. Da $\mathbb{F}_4$ jedoch die Struktur eine $\mathbb{F}_2$-Vektorraums besitzt, hat jedes nicht-triviale Elemente in $\mathbb{F}_4$ additive Ordnung 2. Also ist $(\mathbb{F}_4, +)$ *nicht* zyklisch.

   [Alternativ kann man auch eine explizite Konstruktion von $\mathbb{F}_4$ (oder ähnlichen Körpern) verwenden oder mithilfe der Distributivität von Addition/Multiplikation aus der Annahme $(\mathbb{F}_4, +) \cong \mathbb{Z}/4$ ableiten, dass $\mathbb{F}_4$ Nullteiler enthalten müsste.]
3. Diese Aussage ist falsch, denn: Die Körpererweiterung $\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q}$ ist separabel (wegen Charakteristik 0). Aber diese Erweiterung ist *nicht* normal (und damit auch keine Galoiserweiterung), denn: Das Minimalpolynom von $\sqrt[3]{2}$ über $\mathbb{Q}$ ist $T^3 - 2$ (Eisenstein); dieses Polynom besitzt nicht nur reelle Nullstellen, aber $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$.

Aufgabe 4 (2 + 3 + 3 + 1 = 9 Punkte).

1. Wie lautet die Definition des Zentrums einer Gruppe? Wie lautet die Definition des Zentralisators eines Gruppenelements?
2. Formulieren Sie die Klassengleichung.
3. Wie beweist man die Klassengleichung?
4. Nennen Sie eine Anwendung der Klassengleichung.

Lösung:

1. *Definition.* Sei G eine Gruppe. Das *Zentrum von G* ist
$$Z(G) := \bigl\{g \in G \bigm| \forall_{h \in G} \quad g \cdot h = h \cdot g\bigr\} \subset G.$$
Ist $h \in G$, so ist der *Zentralisator von h in G* definiert als
$$Z_G(h) := \{g \in G \mid g \cdot h = h \cdot g\} \subset G.$$

2. *Klassengleichung.* Sei G eine endliche Gruppe und sei $(g_i)_{i \in I}$ ein Repräsentantensystem für die nicht-trivialen Konjugationsklassen in G (d.h. für die Bahnen der Konjugationsoperation von G auf G, die nicht von Elementen aus dem Zentrum stammen). Dann ist
$$|G| = |Z(G)| + \sum_{i \in I} \bigl[G : Z_G(g_i)\bigr].$$

3. *Beweis der Klassengleichung.* Die Konjugationsoperation von G auf sich selbst ist durch die Abbildung
$$\begin{aligned} G &\longrightarrow \operatorname{Aut}(G) \\ g &\longmapsto (h \mapsto g \cdot h \cdot g^{-1}) \end{aligned}$$
gegeben. Ist $g \in G$, so ist der Stabilisator von g unter der Konjugationsoperation der Zentralisator $Z_G(g)$ von g in G; ist $g \in Z(G)$, so ist der Stabilisator von g ganz G. Mit der Bahnengleichung folgt somit
$$|G| = \sum_{G \cdot x \in G \backslash G} [G : G_x] = |Z(G)| + \sum_{i \in I} \bigl[G : Z_G(g_i)\bigr].$$

4. Mithilfe der Klassengleichung kann man zeigen, dass jede nicht-triviale endliche p-Gruppe ein nicht-triviales Zentrum besitzt (induktiv folgt daraus die Auflösbarkeit von endlichen p-Gruppen).

Aufgabe 5 (3 + 3 + 3 = 9 Punkte). Sei $\alpha \in \mathbb{C}$ mit

$$(\alpha^5 + 3 \cdot \alpha^4 - 99 \cdot \alpha - 33)^2 = 0.$$

1. Zeigen Sie, dass $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 5$.
2. Zeigen Sie: Es gibt *keinen* Körperhomomorphismus $\mathbb{Q}(\alpha) \longrightarrow \mathbb{Q}(\zeta_{10})$.
3. Zeigen Sie: Es gibt einen Zwischenkörper M von $\mathbb{C} \mid \mathbb{Q}(\alpha)$, so dass die Erweiterung $M \mid \mathbb{Q}$ normal ist und $[M : \mathbb{Q}] \leq 120$ gilt.

Lösung:

1. Sei $f := T^5 + 3 \cdot T^4 - 99 \cdot T - 33 \in \mathbb{Q}[T]$. Dann ist $f(\alpha) = 0$ und f ist normiert und irreduzibel in $\mathbb{Z}[T]$ bzw. $\mathbb{Q}[T]$ (Eisenstein für die Primzahl $3 \in \mathbb{Z}$). Also ist f das Minimalpolynom von α über $\mathbb{Q}$ und es folgt

$$\big[\mathbb{Q}(\alpha) : \mathbb{Q}\big] = \deg f = 5.$$

2. *Angenommen,* es gäbe eine Körperhomomorphismus $\sigma \colon \mathbb{Q}(\alpha) \longrightarrow \mathbb{Q}(\zeta_{10})$. Dann ist σ eine $\mathbb{Q}$-lineare Abbildung (da $\mathbb{Q}$ der Primkörper der beiden Körper ist) und als Körperhomomorphismus injektiv. Mit der Dimensionsoformel folgt daher (mit dem ersten Teil)

$$5 = \big[\mathbb{Q}(\alpha) : \mathbb{Q}\big] = \dim_{\mathbb{Q}} \mathbb{Q}(\alpha) \leq \dim_{\mathbb{Q}} \mathbb{Q}(\zeta_{10}) = \big[\mathbb{Q}(\zeta_{10}) : \mathbb{Q}\big] = \varphi(10) = 4,$$

was nicht sein kann. Also gibt es *keinen* Körperhomomorphismus $\mathbb{Q}(\alpha) \longrightarrow \mathbb{Q}(\zeta_{10})$.

3. Seien $\alpha_2, \dots, \alpha_5 \in \mathbb{C}$ die anderen Nullstellen von f in $\mathbb{C}$. Dann ist $M := \mathbb{Q}(\alpha, \alpha_2, \dots, \alpha_5) \subset \mathbb{C}$ ein Zerfällungskörper von f über $\mathbb{Q}$ und $\mathbb{Q}(\alpha) \subset M$; insbesondere ist die Erweiterung $M \mid \mathbb{Q}$ normal.

   Dabei gilt $[M : \mathbb{Q}] \leq 120$, denn: Es gilt (wie man zum Beispiel anhand von Minimalpolynomen ablesen kann)

$$\big[\mathbb{Q}(\alpha) : \mathbb{Q}\big] = 5, \big[\mathbb{Q}(\alpha, \alpha_2) : \mathbb{Q}(\alpha)\big] \leq 4, \dots,$$

   und damit (Multiplikativität des Grades)

$$[M : \mathbb{Q}] \leq 5! = 120.$$

   [Alternativ kann man in diesem Schritt auch mit dem Konjugationsprinzip und $|S_5| = 120$ argumentieren.]

Aufgabe 6 ($3 + 3 + 3 = 9$ **Punkte).** Sei $L \mid K$ eine endliche Galoiserweiterung, sei $G := \mathrm{Gal}(L, K)$ und es gelte $|G| = 99$.

1. Bestimmen Sie die Anzahl der 3-Sylowgruppen von G.
2. Zeigen Sie, dass G auflösbar ist.
3. Zeigen Sie: Es gibt mindestens elf verschiedene Elemente in L, deren Minimalpolynome über K den Grad 11 besitzen.

Lösung:

1. Sei s_3 die Anzahl der 3-Sylowgruppen von G. Nach den Sylowsätzen gilt dann
$$s_3 \mid 99 \quad \text{und} \quad s_3 \equiv 1 \mod 3.$$
Die einzigen Teiler von 99 sind $1, 3, 9, 11, 33, 99$. Aus den obigen Bedingungen folgt daher $s_3 = 1$. Also besitzt G genau eine 3-Sylowgruppe.

2. Sei $S \subset G$ die 3-Sylowgruppe von G. Da S die einzige 3-Sylowgruppe von G ist, ist S ein Normalteiler von G. Also ist
$$|G/S| = \frac{|G|}{|S|} = \frac{99}{9} = 11.$$
Da 11 prim ist, ist G/S auflösbar; als 3-Gruppe ist auch S auflösbar. Nach den Vererbungseigenschaften auflösbarer Gruppen ist somit auch G auflösbar.

3. Sei $M := L^S$. Nach dem Hauptsatz der Galoistheorie ist dann $M \mid K$ eine Galoiserweiterung und
$$[M : K] = \frac{[L : K]}{[L : M]} = \frac{|\,\mathrm{Gal}(L, K)|}{|\,\mathrm{Gal}(L, M)|} = \frac{|G|}{|S|} = \frac{99}{9} = 11.$$
Nach dem Satz vom primitiven Element gibt es ein $\alpha \in M$ mit $K(\alpha) = M$. Sei $\mu_\alpha \in K[T]$ das Minimalpolynom von α über K; insbesondere ist dann
$$\deg \mu_\alpha = [M : K] = 11.$$
Da $M \mid K$ normal und separabel ist, zerfällt μ_α in $M[T]$ in elf verschiedene Linearfaktoren. Die zugehörigen elf Nullstellen haben daher die gewünschte Eigenschaft.

Aufgabe 7 (6 Punkte)**.** Zeigen Sie, dass es eine Galoiserweiterung $L \mid \mathbb{Q}$ mit $\mathrm{Gal}(L, \mathbb{Q}) \cong \mathbb{Z}/5$ gibt.
Hinweis. ζ_{11}

Lösung: Sei $M := \mathbb{Q}(\zeta_{11}) \subset \mathbb{C}$. Dann ist

$$G := \mathrm{Gal}\big(\mathbb{Q}(\zeta_{11}), \mathbb{Q}\big) \cong \big(\mathbb{Z}/(11)\big)^{\times} \cong \mathbb{Z}/10$$

(da $\mathbb{Z}/(11)$ ein endlicher Körper ist und also eine zyklische Einheitengruppe besitzt).

Insbesondere enthält die Gruppe G einen Normalteiler N mit

$$G/N \cong \mathbb{Z}/5$$

(nämlich die der von $[5]$ erzeugten Untergruppe $\{[0], [5]\}$ von $\mathbb{Z}/10$ entsprechenden Untergruppe von G).

[Man kann an dieser Stelle auch mit $|G| = 10$ und der Klassifikation endlicher abelscher Gruppen argumentieren.]

Nach dem Hauptsatz der Galoistheorie ist die Erweiterung $L \mid \mathbb{Q}$ zu $L := M^N$ eine Galoiserweiterung mit

$$\mathrm{Gal}(L, \mathbb{Q}) \cong G/N \cong \mathbb{Z}/5.$$