Klausur zur Algebra

Prof. Dr. C. Löh/D. Fauser/J. Witzig — 16. Februar 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
$$\forall_{g\in G} \quad \exists_{h\in G} \quad g \cdot h^2 = g^{-1}.$$
2. Für jeden Gruppenhomomorphismus $f\colon G \longrightarrow H$ ist $\{g \in G \mid f(g)^2 = e\}$ ein Normalteiler in G.
3. Ist G eine Gruppe, so gibt es eine freie Gruppenoperation von G auf der Menge G.

Lösung:

1. Diese Aussage ist wahr, denn: Ist G eine Gruppe und $g \in G$, so erfüllt $h := g^{-1} \in G$ die Gleichung
$$g \cdot h^2 = g \cdot (g^{-1})^2 = g^{-1}.$$
2. Diese Aussage ist falsch, denn: Für den Homomorphismus $f := \mathrm{id}_{S_3}\colon S_3 \longrightarrow S_3$ ist
$$\{g \in S_3 \mid f(g)^2 = e\} = \{g \in S_3 \mid g^2 = e\} = \{\mathrm{id}_{\{1,2,3\}}, (1\ 2), (1\ 3), (2\ 3)\}$$
noch nicht einmal eine Untergruppe von S_3.
[Manche haben nur überprüft, dass
$$\forall_{g\in G} \quad \forall_{h\in G} \quad f(g)^2 = e \Longrightarrow f(h \cdot g \cdot h^{-1})^2 = e$$
gilt. Dies war ein unbeabsichtigter Stolperstein.]
3. Diese Aussage ist wahr, denn: Ist G eine Gruppe, so ist die Linkstranslationsoperation von G auf G, gegeben durch
$$\begin{aligned} G &\longrightarrow S_G \\ g &\longmapsto (x \mapsto g \cdot x) \end{aligned}$$
bzw.
$$\begin{aligned} G \times G &\longrightarrow G \\ (g, x) &\longmapsto g \cdot x, \end{aligned}$$
eine freie Gruppenoperation von G auf G.

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

1. Das Polynom $T^{2018} - 18 \cdot T^3 + 21 \in \mathbb{Z}[T]$ ist irreduzibel in $\mathbb{Z}[T]$.
2. Sind $a, b \subset \mathbb{Z}$ Ideale, so gilt $\mathbb{Z}/a \cong \mathbb{Z}/b$.
3. Jeder Restklassenring von $\mathbb{Q}[X, Y]$ ist ein Integritätsring.

Lösung:

1. Diese Aussage ist wahr, denn: Das gegebene Polynom ist primitiv und wegen
$$3 \nmid 1, \quad 3 \mid -18, \quad 3 \mid 21, \quad 3^2 \nmid 21$$
ist das Eisensteinsche Irreduzibilitätskriterium für das Primelement $3 \in \mathbb{Z}$ darauf anwendbar.
2. Diese Aussage ist falsch, denn: Für die Ideale $a := \mathbb{Z} \subset \mathbb{Z}$ und $b := \{0\} \subset \mathbb{Z}$ in $\mathbb{Z}$ gilt
$$\mathbb{Z}/a \cong \{0\} \ncong \mathbb{Z} \cong \mathbb{Z}/b.$$
[Allgemeiner gilt, dass $\mathbb{Z}/a$ genau dann zu $\mathbb{Z}/b$ isomorph ist, wenn $a = b$ ist.]
3. Diese Aussage ist falsch, denn: Wir betrachten das Ideal $a := (X^2, Y) \subset \mathbb{Q}[X, Y]$. Dann ist
$$\mathbb{Q}[X, Y]/a \cong \mathbb{Q}[X]/(X^2).$$
In $\mathbb{Q}[X]/(X^2)$ ist aber die Restklasse von X ein nicht-trivialer Nullteiler.
[Es gibt viele weitere Beispiele solcher Ideale; ein etwas pathologischer Fall ist das Ideal $\mathbb{Q}[X, Y]$ in $\mathbb{Q}[X, Y]$: Der zugehörige Restklassenring ist der Nullring (und dieser ist nach unserer Konvention *kein* Integritätsring).]

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

1. Sind K und L endliche Körper mit $|K| = |L|$, so folgt $K \cong L$.
2. Es gibt einen Körper K, so dass die Einheitengruppe $K^\times$ eine Untergruppe enthält, die isomorph zu $\mathbb{Z}/3 \times \mathbb{Z}/9$ ist.
3. Jede endliche Körpererweiterung ist eine Galoiserweiterung.

Lösung:

1. Diese Aussage ist wahr, denn: Dies folgt aus dem Klassifikationssatz für endliche Körper.

   Genauer: Seien K und L endliche Körper mit $|K| = |L|$. Sei $p := \operatorname{char} K$ und $q := \operatorname{char} L$. Dann existieren $k, m \in \mathbb{N}$ mit

   $$|K| = p^k \quad \text{und} \quad |L| = q^m.$$

   Die eindeutige Primfaktorzerlegung in $\mathbb{Z}$ liefert also $p = q$ und $k = m$. Nach dem Klassifikationssatz für endliche Körper sind dann K und L isomorph.

2. Diese Aussage ist falsch, denn: Die Gruppe $\mathbb{Z}/3 \times \mathbb{Z}/9$ ist eine endliche Gruppe. Aber die Gruppe $\mathbb{Z}/3 \times \mathbb{Z}/9$ ist *nicht* zyklisch (sie enthält genau 27 Elemente, aber jedes Element von $\mathbb{Z}/3 \times \mathbb{Z}/9$ hat höchstens Ordnung 9).

   Da endliche Untergruppen von Einheitengruppen von Körpern zyklisch sind, kann $\mathbb{Z}/3 \times \mathbb{Z}/9$ *nicht* als Isomorphietyp einer Untergruppe der Einheitengruppe eines Körpers auftreten.

3. Diese Aussage ist falsch, denn: Die Körpererweiterung $\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q}$ ist endlich (sie hat bekanntlich Grad 3), aber *nicht* normal (da $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$, aber das Minimalpolynom $T^3 - 2$ von $\sqrt[3]{2}$ über $\mathbb{Q}$ auch nicht-reelle Nullstellen in $\mathbb{C}$ besitzt). Insbesondere ist diese Körpererweiterung somit *keine* Galoiserweiterung.

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

1. Formulieren Sie den kleinen Satz von Fermat.
2. Beweisen Sie den kleinen Satz von Fermat.
3. Nennen Sie eine Anwendung des kleinen Satzes von Fermat.
4. Wie ist der Frobeniusendomorphismus definiert? Nennen Sie außerdem einen Zusammenhang mit dem kleinen Satz von Fermat!

Lösung:

1. *Der kleine Satz von Fermat.* Sei $p \in \mathbb{N}$ prim. Dann gilt
$$x^{p-1} \equiv 1 \mod p$$
für alle $x \in \mathbb{Z}$ mit $p \nmid x$.
[Es ist natürlich auch möglich, die allgemeinere Formulierung (mit der eulerschen φ-Funktion) zu nennen.]
2. 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 bereits, 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.
[Es gibt viele alternative Beweise des kleinen Satzes von Fermat (z.B. per Induktion) und jeder korrekte Beweis gibt natürlich volle Punktzahl.]
3. Zum Beispiel das RSA-Verschlüsselungsverfahren.
[Oder probablistische Primzahltests, . . .]
4. *Definition des Frobeniusendomorphismus.* Sei $p \in \mathbb{N}$ prim und sei K ein Körper mit $\operatorname{char} K = p$. Der *Frobeniusendomorphismus von* K ist definiert als
$$\begin{aligned} F_K \colon K &\longrightarrow K \\ x &\longmapsto x^p. \end{aligned}$$
Ist P der Primkörper von K (und damit isomorph zu $\mathbb{F}_p$), so ist die Einschränkung $F_K|_P$ nach dem kleinen Satz von Fermat die Identität auf P.
[Dieser Sachverhalt kann auf verschiedene Weisen formuliert werden, z.B. auch: Im Fall $K = \mathbb{F}_p$ ist F_K nach dem kleinen Satz von Fermat die Identität.]

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

$$(\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1) \cdot (\alpha^2 + 2) = 0.$$

1. Zeigen Sie, dass $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\sqrt[5]{2}) = \mathbb{Q}$ ist.
2. Zeigen Sie, dass die Körpererweiterung $\mathbb{Q}(\alpha) \mid \mathbb{Q}$ normal ist.
3. Zeigen Sie, dass $\mathrm{Gal}(\mathbb{Q}(\alpha), \mathbb{Q})$ auflösbar ist.

Lösung: Um die Darstellung zu vereinfachen, machen wir die folgende Vorüberlegung: Wegen der gegebenen Gleichung für α folgt

$$\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1 = 0 \qquad \text{oder} \qquad \alpha^2 + 2 = 0.$$

Ist $\mu_\alpha \in \mathbb{Q}[T]$ das Minimalpolynom von α, so ist also μ_α ein Teiler von $\Phi_5 = T^4 + T^3 + T^2 + T + 1$ oder von $T^2 + 2$. Die letzteren beiden Polynome sind irreduzibel in $\mathbb{Q}[T]$ (denn Φ_5 ist das fünfte Kreisteilungspolynom; auf $T^2 + 2$ ist das Eisensteinsche Irreduzibilitätskriterium für die Primzahl $2 \in \mathbb{Z}$ anwendbar). Also ist

$$\mu_\alpha = \Phi_5 \qquad \text{oder} \qquad \mu_\alpha = T^2 + 2.$$

[Punkte für diese Beobachtungen wurden in der Teilaufgabe vergeben, in der sie gemacht wurden. Man beachte, dass $\mathbb{Q}(\alpha) \neq \mathbb{Q}(i \cdot \sqrt{2}, \zeta_5)$ ist, da α ja nur eine der Nullstellen von $\Phi_5 \cdot (T^2 + 2)$ ist.]

1. Sei $K := \mathbb{Q}(\alpha) \cap \mathbb{Q}(\sqrt[5]{2})$. Dann ist K ein Zwischenkörper von $\mathbb{Q}(\alpha) \mid \mathbb{Q}$ und von $\mathbb{Q}(\sqrt[5]{2}) \mid \mathbb{Q}$. Nach der Vorüberlegung ist

   $$\big[\mathbb{Q}(\alpha) : \mathbb{Q}\big] = \deg \mu_\alpha \in \{4, 2\};$$

   andererseits ist (Eisenstein ...)

   $$\big[\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}\big] = 5.$$

   Mit der Multiplikativität des Grades erhalten wir also, dass $[K : \mathbb{Q}]$ ein Teiler von 4 (bzw. 2) und 5 ist. Also ist $[K : \mathbb{Q}] = 1$, und damit $\mathbb{Q}(\alpha) \cap \mathbb{Q}(\sqrt[5]{3}) = K = \mathbb{Q}$.

   [So ganz ohne Erweiterungsgrade ist das nur schwer zu beweisen und erfordert sehr große Sorgfalt.]

2. Wir unterscheiden die folgenden Fälle:

– Ist $\mu_\alpha = \Phi_5$, so ist $\mathbb{Q}(\alpha) = \mathbb{Q}(\zeta_5)$ und somit ist $\mathbb{Q}(\alpha)$ (als Zerfällungskörper von $T^5 - 1$) normal über $\mathbb{Q}$.

– Ist $\mu_\alpha = T^2 + 2$, so zerfällt μ_α in $\mathbb{Q}(\alpha)$ in Linearfaktoren (Mitternachtsformel ...), und daher ist $\mathbb{Q}(\alpha) \mid \mathbb{Q}$ normal.

[Alternativ kann man auch die Tatsache verwenden, dass alle Körpererweiterungen vom Grad 2 normal sind.]

3. Wir unterscheiden die folgenden Fälle:

– Ist $\mu_\alpha = \Phi_5$, so ist $\mathbb{Q}(\alpha) = \mathbb{Q}(\zeta_5)$, und damit

$$\mathrm{Gal}\big(\mathbb{Q}(\alpha), \mathbb{Q}\big) = \mathrm{Gal}\big(\mathbb{Q}(\zeta_5), \mathbb{Q}\big) \cong \big(\mathbb{Z}/(5)\big)^\times.$$

Als abelsche (sogar zyklische) Gruppe ist $(\mathbb{Z}/(5))^\times$ auflösbar.

– Ist $\mu_\alpha = T^2 + 2$, so ist

$$\mathrm{Gal}\big(\mathbb{Q}(\alpha), \mathbb{Q}\big) \cong \mathbb{Z}/2;$$

dies folgt aus dem Konjugationsprinzip oder wegen $|\mathrm{Gal}(\mathbb{Q}(\alpha), \mathbb{Q})| = [\mathbb{Q}(\alpha) : \mathbb{Q}] = 2$ aus der Klassifikation der zwei-elemetigen Gruppen (dabei verwenden wir, dass die Erweiterung normal ist!). Also ist auch in diesem Fall die Galoisgruppe abelsch, und damit auflösbar.

[Alternativ genügt es sich auch zu überlegen, dass $\mathrm{Gal}(\mathbb{Q}(\alpha), \mathbb{Q})$ eine 2-Gruppe ist.

Besonders elegant ist der folgende Lösungsweg: Wegen $\deg \mu_\alpha \leq 4$ ist die Gruppe $\mathrm{Gal}(\mathbb{Q}(\alpha), \mathbb{Q})$ nach dem Konjugationsprinzip zu einer Untergruppe von S_4 isomorph. Da S_4 auflösbar ist, ist auch jede Untergruppe von S_4 auflösbar. Insbesondere ist dann auch $\mathrm{Gal}(\mathbb{Q}(\alpha), \mathbb{Q})$ auflösbar.

Eine weitere Variante ist, über Wurzelerweiterungen zu argumentieren.]

Aufgabe 6 (3 + 3 + 3 = 9 Punkte)**.** Sei $L \mid K$ eine endliche Galoiserweiterung, sei $G := \mathrm{Gal}(L, K)$ und es gelte $|G| = 63$.

1. Zeigen Sie, dass es ein Element in L gibt, dessen Minimalpolynom (über K) den Grad 63 besitzt.

2. Seien M und M' Zwischenkörper von $L \mid K$ mit $[M : K] = 7 = [M' : K]$. Zeigen Sie: Dann gilt $\mathrm{Gal}(L, M) \cong \mathrm{Gal}(L, M')$.

3. Bestimmen Sie die Anzahl der 7-Sylowgruppen von G.

Lösung:

1. Als Galoiserweiterung ist $L \mid K$ insbesondere separabel. Nach dem Satz vom primitiven Element besitzt die endliche separable Körpererweiterung $L \mid K$ also ein primitives Element $\alpha \in L$, d.h. es gilt $L = K(\alpha)$. Sei $\mu_\alpha \in K[T]$ das Minimalpolynom von α über K. Dann ist

$$\deg \mu_\alpha = \big[K(\alpha) : K\big] = [L : K] = 63.$$

2. Da mit $L \mid K$ auch $L \mid M$ und $L \mid M'$ endliche Galoiserweiterungen sind, folgt (zusammen mit der Multiplikativität des Grades)

$$\big|\mathrm{Gal}(L, M)\big| = [L : M] = \frac{[L : K]}{[M : K]} = \frac{\big|\mathrm{Gal}(L, K)\big|}{7} = \frac{63}{7} = 9 = 3^2$$

und analog auch

$$\big|\mathrm{Gal}(L, M')\big| = 3^2.$$

Wegen $63 = 3^2 \cdot 7$ handelt es sich also bei $\mathrm{Gal}(L, M)$ und $\mathrm{Gal}(L, M')$ um 3-Sylowgruppen von $\mathrm{Gal}(L, K)$. Nach den Sylowsätzen sind alle 3-Sylowgruppen der Gruppe $\mathrm{Gal}(L, K)$ konjugiert zueinander, und damit insbesondere isomorph.

3. Sei s_7 die Anzahl der 7-Sylowgruppen von G. Nach den Sylowsätzen gilt dann

$$s_7 \mid 63 \quad \text{und} \quad s_7 \equiv 1 \mod 7.$$

Die einzigen Teiler von 63 sind $1, 3, 7, 9, 21, 63$. Aus den obigen Bedingungen folgt daher $s_7 = 1$. Also besitzt G genau eine 7-Sylowgruppe.

Aufgabe 7 (6 Punkte). Sei $L \mid \mathbb{Q}$ eine endliche Körpererweiterung. Zeigen Sie, dass $L \mid \mathbb{Q}$ nur endlich viele Zwischenkörper besitzt.

Lösung: Als endliche Körpererweiterung ist $L \mid \mathbb{Q}$ algebraisch. Wegen $\operatorname{char} \mathbb{Q} = 0$ ist die Körpererweiterung $L \mid \mathbb{Q}$ separabel. Nach dem Satz vom primitiven Element gibt es also ein $\alpha \in L$ mit

$$L = \mathbb{Q}(\alpha).$$

Sei M ein Zerfällungskörper des Minimalpolynoms von α über $\mathbb{Q}$ mit $L \subset M$ (ein solcher kann zum Beispiel mit der Standardkonstruktion von Zerfällungskörpern gewonnen werden). Dann ist die Körpererweiterung $M \mid \mathbb{Q}$ eine endliche Galoiserweiterung.

Nach dem Hauptsatz der Galoistheorie stimmt die Anzahl der Zwischenkörper von $M \mid \mathbb{Q}$ mit der Anzahl der Untergruppen der Gruppe $\operatorname{Gal}(M, \mathbb{Q})$ überein. Da $M \mid \mathbb{Q}$ eine endliche Galoiserweiterung ist, ist wegen

$$\left|\operatorname{Gal}(M, \mathbb{Q})\right| = [M : \mathbb{Q}]$$

auch die Gruppe $\operatorname{Gal}(M, \mathbb{Q})$ endlich und besitzt somit nur endlich viele Untergruppen. Also besitzt $M \mid \mathbb{Q}$ nur endlich viele Zwischenkörper.

Da L nach Konstruktion ein Zwischenkörper von $M \mid \mathbb{Q}$ ist, ist jeder Zwischenkörper von $L \mid \mathbb{Q}$ auch einer von $M \mid \mathbb{Q}$. Insbesondere besitzt auch die Körpererweiterung $L \mid \mathbb{Q}$ nur endlich viele Zwischenkörper.

[Man kann auch ohne den Satz vom primitiven Element argumentieren, aber dann ist die Konstruktion einer Galoiserweiterung, die $L \mid \mathbb{Q}$ umfasst, ein bisschen aufwendiger.]