Probeklausur zur Algebra

Prof. Dr. C. Löh/D. Fauser/J. Witzig 9. 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
$$\forall_{g,h\in G} \quad g \cdot h \cdot g^{-1} = h.$$

2. Für jeden Gruppenhomomorphismus $f\colon G \longrightarrow H$ gibt es einen Normalteiler $N \subset G$ mit
$$\forall_{g,h\in G} \quad g \cdot N = h \cdot N \iff f(g) = f(h).$$

3. Die Gruppe $S_6 \times \mathbb{Z}/6$ ist auflösbar.

Lösung:

1. Diese Aussage ist falsch, denn: Für $g := (1\ 2), h := (1\ 2\ 3) \in S_3$ gilt
$$g \cdot h \cdot g^{-1} = (3\ 2\ 1) \neq (1\ 2\ 3) = h.$$

2. Diese Aussage ist wahr, denn: Ist $f\colon G \longrightarrow H$ ein Gruppenhomomorphismus, so ist $N := \ker f \subset G$ ein Normalteiler in G. Ist $\overline{f}\colon G/N \longrightarrow H$ der von f induzierte Gruppenhomomorphismus, so gilt (da $\overline{f}$ injektiv ist)
$$\forall_{g,h\in G} \quad g \cdot N = h \cdot N \iff f(g) = \overline{f}(g \cdot N) = \overline{f}(h \cdot N) = f(h).$$

3. Diese Aussage ist falsch, denn: Die Gruppe $S_6 \times \mathbb{Z}/6$ enthält eine zu S_5 isomorphe Untergruppe. Da S_5 *nicht* auflösbar ist und Auflösbarkeit auf Untergruppen vererbt wird, folgt, dass auch $S_6 \times \mathbb{Z}/6$ *nicht* auflösbar ist.

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

1. Das Polynom $T^3 + 2017 \cdot T^2 + 2018 \cdot T + 2019 \in \mathbb{Z}[T]$ ist irreduzibel in $\mathbb{Z}[T]$.
2. Jedes Ideal $a \subset \mathbb{Z}$ mit $5 \in a$ und $a \neq \mathbb{Z}$ ist maximal.
3. Es gibt ein Ideal $a \subset \mathbb{Q}[T]$ mit $\mathbb{Q}[T]/a \cong \mathbb{F}_5$.

Lösung:

1. Diese Aussage ist wahr, denn: Wir betrachten das Reduktionskriterium für die Primzahl $2 \in \mathbb{Z}$. Reduktion modulo 2 liefert das Polynom

$$\mathbb{F}_2[T] \ni T^3 + [2017] \cdot T^2 + [2018] \cdot T + [2019] = T^3 + T^2 + 1.$$

   Einsetzen der beiden Werte in $\mathbb{F}_2$ zeigt, dass dieses Polynom keine Nullstelle in $\mathbb{F}_2$ besitzt. Da das Polynom Grad 3 hat, folgt mit dem Nullstellenkriterium, dass es in $\mathbb{F}_2[T]$ irreduzibel ist. Also liefert das Reduktionskriterium, dass auch das ursprüngliche Polynom in $\mathbb{Z}[T]$ irreduzibel ist.

2. Diese Aussage ist wahr, denn: Sei $a \subset \mathbb{Z}$ ein Ideal mit $5 \in a$ und $a \neq \mathbb{Z}$. Da $\mathbb{Z}$ ein Hauptidealring ist, gibt es ein $x \in \mathbb{Z}$ mit $a = (x) \subset \mathbb{Z}$. Wegen $5 \in a$ folgt $x \mid 5$. Da 5 prim ist, ist x eine Einheit oder assoziiert zu 5. Aufgrund der Annahme $a \neq \mathbb{Z}$ ist x *keine* Einheit. Also ist x assoziiert zum Primelement 5. Da $\mathbb{Z}$ ein Hauptidealring ist, ist das Ideal $a = (x) = (5)$ somit ein maximales Ideal.

3. Diese Aussage ist falsch, denn: Ist $a \subset \mathbb{Q}[T]$ ein Ideal, so erbt $\mathbb{Q}[T]/a$ von $\mathbb{Q}[T]$ eine $\mathbb{Q}$-Vektorraumstruktur. Insbesondere ist $\mathbb{Q}[T]/a$ einelementig oder unendlich. Wegen $|\mathbb{F}_5| = 5$ gilt insbesondere *nicht* $\mathbb{Q}[T]/a \cong \mathbb{F}_5$.

   [Es gibt viele Varianten dieses Arguments, die genauso gut funktionieren, zum Beispiel: *Angenommen,* $\mathbb{Q}[T]/a \cong \mathbb{F}_5$. Da jeder solche Isomorphismus die Eins auf die Eins abbildet, folgt $5 \in a$ (da $\mathbb{F}_5$ Charakteristik 5 hat). Aber in $\mathbb{Q}[T]$ ist 5 eine Einheit, und damit $\mathbb{Q}[T]/a \cong \{0\}$, im Widerspruch zur Annahme.]

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

1. Der Körper $\mathbb{F}_{1024}$ ist algebraisch abgeschlossen.
2. Es gibt einen Körper K mit $K^\times \cong \mathbb{Z}/17$.
3. Jede separable Körpererweiterung ist endlich.

Lösung:

1. Diese Aussage ist falsch, denn: Der Körper $\mathbb{F}_{1024}$ ist endlich und es gibt *keine* algebraisch abgeschlossenen endlichen Körper.
2. Diese Aussage ist falsch, denn: *Angenommen,* es gäbe einen Körper K mit der Eigenschaft $K^\times \cong \mathbb{Z}/17$. Dann folgt
$$|K| = |K^\times| + 1 = |\mathbb{Z}/17| + 1 = 17 + 1 = 18.$$
Insbesondere ist K ein endlicher Körper. Dann müsste $|K|$ aber eine Primpotenz sein, im Widerspruch dazu, dass 18 *keine* Primpotenz ist.
3. Diese Aussage ist falsch, denn: In Charakteristik 0 ist jede algebraische Körpererweiterung separabel. Ist
$$L := \{x \in \mathbb{C} \mid x \text{ ist algebraisch über } \mathbb{Q}\},$$
so ist L ein Zwischenkörper von $\mathbb{C} \mid \mathbb{Q}$ und die Körpererweiterung $L \mid \mathbb{Q}$ ist algebraisch (und damit separabel, s.o.), aber die Körpererweiterung $L \mid \mathbb{Q}$ ist bekannterweise *nicht* endlich.

Aufgabe 4 (1 + 6 + 1 + 1 = 9 Punkte)**.**

1. Wie lautet die Definition normaler Körpererweiterungen?
2. Formulieren Sie den Hauptsatz der Galoistheorie.
3. Nennen Sie ein Resultat, das im Beweis des Hauptsatzes der Galoistheorie eine wesentliche Rolle spielt.
4. Nennen Sie eine Anwendung des Hauptsatzes der Galoistheorie.

Lösung:

1. *Definition.* Eine algebraische Körpererweiterung $L \mid K$ ist *normal*, wenn für jedes $\alpha \in L$ das Minimalpolynom von α über K bereits in L in Linearfaktoren zerfällt.
2. *Hauptsatz der Galoistheorie.* Sei $L \mid K$ eine endliche Galoiserweiterung.
   (a) Dann sind
   $$\begin{aligned} \mathsf{Subext}(L,K) &\longrightarrow \mathsf{Subgroup}\,\mathrm{Gal}(L,K) \\ M &\longmapsto \mathrm{Gal}(L,M) \\ \mathsf{Subgroup}\,\mathrm{Gal}(L,K) &\longrightarrow \mathsf{Subext}(L,K) \\ H &\longmapsto L^H \end{aligned}$$
   zueinander inverse Bijektionen.
   (b) Sei M ein Zwischenkörper von $L \mid K$. Dann ist die Körpererweiterung $M \mid K$ genau dann normal, wenn $\mathrm{Gal}(L,M)$ ein Normalteiler in $\mathrm{Gal}(L,K)$ ist. In diesem Fall ist
   $$\begin{aligned} \mathrm{Gal}(L,K)/\,\mathrm{Gal}(L,M) &\longrightarrow \mathrm{Gal}(M,K) \\ [\sigma] &\longmapsto \sigma|_M \end{aligned}$$
   ein wohldefinierter Gruppenisomorphismus.
3. Der Fixkörpersatz von Artin.

   [Oder: Der Satz vom primitiven Element, das Konjugationsprinzip, ...]
4. Charakterisierung der Auflösbarkeit von polynomialen Gleichungen durch Radikale.

   [Oder: Charakterisierung von Konstruierbarkeit mit Zirkel und Lineal, ...]

Aufgabe 5 ($2+3+2+2=9$ Punkte)**.** Sei $f := T^4 - 2 \in \mathbb{Q}[T]$.

1. Zeigen Sie, dass $\mathbb{Q}[T]/(f)$ ein Körper ist.
2. Sei L ein Zerfällungskörper von f über $\mathbb{Q}$. Zeigen Sie, dass $[L : \mathbb{Q}] = 8$.
3. Bestimmen Sie die Anzahl der Körperhomomorphismen $L \longrightarrow \mathbb{C}$.
4. Zeigen Sie, dass die Operation der Galoisgruppe von f über $\mathbb{Q}$ auf der Menge der Nullstellen von f in L *nicht* frei ist.

Lösung:

1. Das Polynom $T^4 - 2 \in \mathbb{Q}[T]$ ist nach dem Eisensteinschen Irreduzibilitätskriterium irreduzibel in $\mathbb{Q}[T]$. Da $\mathbb{Q}[T]$ ein Hauptidealring ist, ist das Ideal $(f) \subset \mathbb{Q}[T]$ ein maximales Ideal. Also ist $\mathbb{Q}[T]/(f)$ ein Körper.
2. Sei $M := \mathbb{Q}(\sqrt[4]{2}, i) \subset \mathbb{C}$. Dann ist M ein Zerfällungskörper von f über $\mathbb{Q}$, denn: In M zerfällt f wegen
$$f = (X - \sqrt[4]{2}) \cdot (X + \sqrt[4]{2}) \cdot (X + i \cdot \sqrt[4]{2}) \cdot (X - i \cdot \sqrt[4]{2})$$
in Linearfaktoren. Wegen $i \cdot \sqrt[4]{2}/\sqrt[4]{2} = i$ gilt
$$\mathbb{Q}(\sqrt[4]{2}, i) = \mathbb{Q}(\sqrt[4]{2}, -\sqrt[4]{2}, i \cdot \sqrt[4]{2}, -i \cdot \sqrt[4]{2}).$$
Also ist M ein Zerfällungskörper für f über $\mathbb{Q}$. Aus der Eindeutigkeit der Zerfällungskörper folgt
$$[L : \mathbb{Q}] = [M : \mathbb{Q}].$$
Es gilt
$$[M : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(i)] \cdot [\mathbb{Q}(i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(i)] \cdot 2.$$
Mit $\mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{R}$ und $i \in \mathbb{C} \setminus \mathbb{R}$ sowie der Multiplikativität der Grade folgt aber auch $\mathbb{Q}(\sqrt[4]{2}) \cap \mathbb{Q}(i) = \mathbb{Q}$ bzw. $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(i)] = 4$.
3. Sei M wie im zweiten Teil. Dann stimmt die Anzahl der Körpermorphismen $L \longrightarrow \mathbb{C}$ mit denen vom Typ $M \longrightarrow \mathbb{C}$ überein (Eindeutigkeit von Zerfällungskörpern). Da $M \mid \mathbb{Q}$ normal ist (als Zerfällungskörper eines rationalen Polynoms), stimmt diese Anzahl mit $|\operatorname{Gal}(M, \mathbb{Q})|$ überein. Da $M \mid \mathbb{Q}$

eine Galoiserweiterung ist (die Separabilität ist wegen Charakteristik 0 gegeben), folgt somit (mit dem zweiten Teil) für die gesuchte Anzahl

$$\left|\mathrm{Gal}(M, \mathbb{Q})\right| = [M : \mathbb{Q}] = 8.$$

[Alternativ kann man auch alle Körperhomomorphismen $L \longrightarrow \mathbb{C}$ mit dem Konjugationsprinzip bestimmen.]

4. Sei $G := \mathrm{Gal}(L, \mathbb{Q})$. Dann ist G (ein Modell für) die Galoisgruppe von f über $\mathbb{Q}$. Da $L \mid \mathbb{Q}$ eine Galoiserweiterung ist, gilt (mit dem zweiten oder dritten Teil)

$$|G| = [L : \mathbb{Q}] = 8.$$

   Sei $X \subset L$ die Menge Nullstellen von f in L. Dann ist $|X| \leq \deg f = 4 < |G|$. Aus der Bahnengleichung folgt somit, dass es *keine* freie Operation von G auf X gibt. Insbesondere ist auch die Galoisoperation von G auf X *nicht* frei.

Aufgabe 6 (3 + 3 + 3 = 9 Punkte). Sei $L \mid K$ eine endliche Galoiserweiterung, sei $G := \operatorname{Gal}(L, K)$ und es gelte $|G| = 44$.

1. Bestimmen Sie die Anzahl der 11-Sylowgruppen von G.
2. Zeigen Sie, dass es einen Epimorphismus $G \longrightarrow \mathbb{Z}/2$ gibt.
3. Zeigen Sie: Es gibt einen Zwischenkörper M von $L \mid K$ mit $[M : K] = 2$.

Lösung:

1. Es gibt genau eine 11-Sylowgruppe in G, denn: Sei s_{11} die Anzahl der 11-Sylowgruppen von G. Nach den Sylowsätzen gilt
$$s_{11} \mid 44 \quad \text{und} \quad s_{11} \equiv 1 \mod 11.$$
Die einzigen (positiven) Teiler von 44 sind $1, 2, 4, 11, 22, 44$. Aus den beiden obigen Bedingungen folgt daher $s_{11} = 1$.

2. Sei $N \subset G$ die (nach dem ersten Teil eindeutig bestimmte) 11-Sylowgruppe von G. Dann ist N ein Normalteiler in G (da jede zu N konjugierte Untergruppe von G auch eine 11-Sylowgruppe in G ist, und somit wegen $s_{11} = 1$ mit N übereinstimmt). Wegen $|G/N| = |G|/|N| = 44/11 = 4$ ist (nach den Klassifikationsresultaten für „kleine" Gruppen) $G/N \cong \mathbb{Z}/4$ oder $G/N \cong \mathbb{Z}/2 \times \mathbb{Z}/2$. Sowohl $\mathbb{Z}/4$ als auch $\mathbb{Z}/2 \times \mathbb{Z}/2$ besitzen surjektive Gruppenhomomorphismen nach $\mathbb{Z}/2$. Durch Komposition mit der kanonischen Projektion $G \longrightarrow G/N$ erhalten wir so einen Epimorphismus $G \longrightarrow \mathbb{Z}/2$.

3. Sei $N' \subset G$ der Kern eines Epimorphismus $G \longrightarrow \mathbb{Z}/2$ (ein solcher Epimorphismus existiert nach dem zweiten Teil) und sei $M := L^{N'}$ der zugehörige Zwischenkörper von $L \mid K$. Da N' ein Normalteiler von G ist, ist $M \mid K$ nach dem Hauptsatz der Galoistheorie eine Galoiserweiterung und
$$[M : K] = \bigl|\operatorname{Gal}(M, K)\bigr| = \bigl|\operatorname{Gal}(L, K)/\operatorname{Gal}(L, M)\bigr| = |G/N'| = |\mathbb{Z}/2| = 2.$$

Aufgabe 7 (6 Punkte)**.** Seien $m, n \in \mathbb{N}_{>0}$ mit $\mathrm{ggT}(m,n) = 1$ und $\zeta_n := e^{2\pi i/n}$, $\zeta_m := e^{2\pi i/m} \in \mathbb{C}$. Zeigen Sie, dass

$$\big[\mathbb{Q}(\zeta_n, \zeta_m) : \mathbb{Q}\big] = \big[\mathbb{Q}(\zeta_n) : \mathbb{Q}\big] \cdot \big[\mathbb{Q}(\zeta_m) : \mathbb{Q}\big].$$

Hinweis. Zeigen Sie zunächst $\mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_{n\cdot m})$. Warum hilft das?

Lösung: Es gilt $\mathbb{Q}(\zeta_n, \zeta_m) = \mathbb{Q}(\zeta_{n\cdot m})$, denn: Wir zeigen die beiden Inklusionen einzeln:

- Wegen $\zeta_n = {\zeta_{n\cdot m}}^m$ und $\zeta_m = {\zeta_{n\cdot m}}^n$ gilt $\zeta_n, \zeta_m \in \mathbb{Q}(\zeta_{n\cdot m})$, und damit
$$\mathbb{Q}(\zeta_n, \zeta_m) \subset \mathbb{Q}(\zeta_{n\cdot m}).$$
- Wegen $\mathrm{ggT}(n,m) = 1$ gibt es $x, y \in \mathbb{Z}$ mit $x \cdot n + y \cdot m = 1$. Also ist
$$\zeta_{n\cdot m} = {\zeta_{n\cdot m}}^1 = {\zeta_{n\cdot m}}^{x\cdot n + y\cdot m} = ({\zeta_{n\cdot m}}^n)^x \cdot ({\zeta_{n\cdot m}}^m)^y = {\zeta_m}^x \cdot {\zeta_n}^y \in \mathbb{Q}(\zeta_n, \zeta_m),$$
und damit $\mathbb{Q}(\zeta_{n\cdot m}) \subset \mathbb{Q}(\zeta_n, \zeta_m)$.

Es gilt
$$\big[\mathbb{Q}(\zeta_n, \zeta_m) : \mathbb{Q}\big] = \big[\mathbb{Q}(\zeta_n) : \mathbb{Q}\big] \cdot \big[\mathbb{Q}(\zeta_m) : \mathbb{Q}\big],$$
denn: Nach der obigen Vorüberlegung und der Theorie der Kreisteilungskörper über $\mathbb{Q}$ ist
$$\big[\mathbb{Q}(\zeta_n, \zeta_m) : \mathbb{Q}\big] = \big[\mathbb{Q}(\zeta_{n\cdot m}) : \mathbb{Q}\big] = \big|\mathbb{Z}/(n\cdot m)^\times\big|.$$
Wegen $\mathrm{ggT}(n,m) = 1$ liefert der Chinesische Restsatz einen Ringisomorphismus

$$\mathbb{Z}/(n\cdot m) \cong \mathbb{Z}/(n) \times \mathbb{Z}/(m),$$

und damit

$$\big|\mathbb{Z}/(n\cdot m)^\times\big| = \big|(\mathbb{Z}/(n) \times \mathbb{Z}/(m))^\times\big| = \big|\mathbb{Z}/(n)^\times \times \mathbb{Z}/(m)^\times\big| = \big|\mathbb{Z}/(n)^\times\big| \cdot \big|\mathbb{Z}/(m)^\times\big|.$$

Die Theorie der Kreisteilungskörper über $\mathbb{Q}$ zeigt dann die gewünschte Gleichheit:

$$\big[\mathbb{Q}(\zeta_n, \zeta_m) : \mathbb{Q}\big] = \big|\mathbb{Z}/(n)^\times\big| \cdot \big|\mathbb{Z}/(m)^\times\big| = \big[\mathbb{Q}(\zeta_n) : \mathbb{Q}\big] \cdot \big[\mathbb{Q}(\zeta_m) : \mathbb{Q}\big]$$