Philipps-Universität Marburg
Fachbereich Mathematik und Informatik
Prof. Dr. Hans Peter Schlickewei
Dipl.-Math. Thomas Geiger

Klausur zur Vorlesung ALGEBRA II - GALOISTHEORIE
im Sommersemester 2012
Donnerstag, den 05.07.2012, 08.00 – 10.00 Uhr

☐ Frau ☐ Herr

Name: Muster Lösung

Vorname: ....

Matrikelnummer: ....

☐ Diese Klausur ist mein letzter Prüfungsversuch im Modul Algebra.

- Füllen Sie bitte zuerst das Deckblatt aus und versehen Sie **alle** Blätter mit Ihrem Namen!
- Bearbeiten Sie die Aufgaben auf den ausgegebenen Blättern. Es befinden sich noch leere Blätter bei der Aufsicht, falls der Platz unter der Aufgabenstellung und auf der Rückseite des Aufgabenblattes nicht ausreichen sollten.
- Es sind keine Hilfsmittel zugelassen.

VIEL ERFOLG!

A1	A2	A3	A4	$\sum$
4	4	3	4	15

Aufgabe 1. *(4 Punkte)*

Sei $K = \mathbb{Q}(\sqrt{5}, \sqrt{7})$.

(i) Zeigen Sie: $K/\mathbb{Q}$ ist eine Galoiserweiterung.

(ii) Bestimmen Sie $\mathrm{Gal}(K/\mathbb{Q})$.

(iii) Bestimmen Sie alle Zwischenkörper L mit $\mathbb{Q} \subset L \subset K$.

(i) • K ist Zerfällungskörper der Polynome

$$X^2 - 5 \quad \text{und} \quad X^2 - 7$$

über $\mathbb{Q}$ $\Rightarrow$ $K/\mathbb{Q}$ ist normale Erweiterung.

• Wegen $\chi(\mathbb{Q}) = 0$ ist $K/\mathbb{Q}$ separable Erweiterung.

$\Rightarrow$ $K/\mathbb{Q}$ ist Galoiserweiterung.

(ii) • $\mathbb{Q}(\sqrt{5})/\mathbb{Q}$ ist eine einfache Erweiterung vom Grad 2 (Minimalpolynom: $X^2 - 5$).

$$\Rightarrow \mathrm{Gal}(\mathbb{Q}(\sqrt{5})/\mathbb{Q}) = \{id, \sigma\} \simeq \mathbb{Z}/2\mathbb{Z} \quad \text{mit}$$

$$\sigma : \sqrt{5} \mapsto -\sqrt{5}.$$

• Analog ist $\mathbb{Q}(\sqrt{7})/\mathbb{Q}$ einfache Erweiterung vom Grad 2 mit

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{7})/\mathbb{Q}) = \{id, \tau\} \simeq \mathbb{Z}/2\mathbb{Z} \quad \text{und}$$

$$\tau : \sqrt{7} \mapsto -\sqrt{7}.$$

- Behauptung: $\mathbb{Q}(\sqrt{5}) \cap \mathbb{Q}(\sqrt{7}) = \mathbb{Q}$.

Dazu:

$$\mathbb{Q}(\sqrt{5}) = \{a + b\sqrt{5} \mid a,b \in \mathbb{Q}\}$$

$$\mathbb{Q}(\sqrt{7}) = \{c + d\sqrt{7} \mid c,d \in \mathbb{Q}\}$$

Gelte $a + b\sqrt{5} = c + d\sqrt{7}$ mit $a,b,c,d \in \mathbb{Q}$

$\Rightarrow b\sqrt{5} = (c-a) + d\sqrt{7}$

$\Rightarrow 5b^2 = (c-a)^2 + 2d(c-a)\sqrt{7} + 7d^2$

Koeffizientenvergleich liefert: $d(c-a) = 0$, d.h.

$d = 0$ oder $a = c$.

- Falls $d = 0$ gilt lautet die Ausgangsgleichung

$$a + b\sqrt{5} = c$$

$\Rightarrow a = c$ und $b = 0$, d.h. das Element liegt in $\mathbb{Q}$.

- Falls $a = c$ gilt erhalten wir aus der Ausgangsgleichung

$$b\sqrt{5} = d\sqrt{7}$$

b und d sind nicht Null.

Durch Erweitern können wir OE $b,d \in \mathbb{Z}$, $\operatorname{ggT}(b,d) = 1$ annehmen.

$\Rightarrow 5b^2 = 7d^2 \Rightarrow 5 \mid d$

$\Rightarrow 25 \mid 5b^2 \Rightarrow 5 \mid b^2 \Rightarrow 5 \mid b$

$\Rightarrow 5$ ist gemeinsamer Teiler von b und d $\lightning$

$\Rightarrow b = d = 0$, also lautet die Ausgangsgleichung

$$a = c$$

und das Element liegt auch in diesem Fall in $\mathbb{Q}$.

- Wegen $\mathbb{Q}(\sqrt{5}, \sqrt{7}) = \mathbb{Q}(\sqrt{5}) \cdot \mathbb{Q}(\sqrt{7})$ und $\mathbb{Q}(\sqrt{5}) \cap \mathbb{Q}(\sqrt{7}) = \mathbb{Q}$ folgt aus der Vorlesung:

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{5}, \sqrt{7}) / \mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}(\sqrt{5}) / \mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\sqrt{7}) / \mathbb{Q})$$

$$= \{id, \sigma, \tau, \sigma\tau\} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

wobei:

$\sigma: \sqrt{5} \mapsto -\sqrt{5}, \quad \sqrt{7} \mapsto \sqrt{7}$

$\tau: \sqrt{5} \mapsto \sqrt{5}, \quad \sqrt{7} \mapsto -\sqrt{7}$

$\sigma\tau: \sqrt{5} \mapsto -\sqrt{5}, \quad \sqrt{7} \mapsto -\sqrt{7}$.

(iii) Die Untergruppen von $\mathrm{Gal}(K/\mathbb{Q})$ sind

$\{id\}$, $\mathrm{Gal}(K/\mathbb{Q})$, $U_1 = \{id, \sigma\}$, $U_2 = \{id, \tau\}$, $U_3 = \{id, \sigma\tau\}$.

Fixkörper (abgelesen an expliziter Angabe der Galoisgruppe in (ii)):

$K^{\{id\}} = K, \quad K^{\mathrm{Gal}(K/\mathbb{Q})} = \mathbb{Q}, \quad K^{U_1} = \mathbb{Q}(\sqrt{7})$,

$K^{U_2} = \mathbb{Q}(\sqrt{5}), \quad K^{U_3} = \mathbb{Q}(\sqrt{35})$.

Nach dem Hauptsatz der Galoistheorie sind dies alle Zwischenkörper von $K/\mathbb{Q}$.

$\blacksquare$

Aufgabe 2. (*4 Punkte*)

Sei $\mathbb{F}_3$ der Körper mit 3 Elementen. Seien weiter $f(X) = X^3+\overline{2}X+\overline{1} \in \mathbb{F}_3[X]$ und $g(X) = X^3 + X^2 + X + \overline{2} \in \mathbb{F}_3[X]$. Mit E_f bzw. E_g bezeichnen wir den Zerfällungskörper von f bzw. g über $\mathbb{F}_3$.

(i) Bestimmen Sie die Grade $[E_f : \mathbb{F}_3]$ und $[E_g : \mathbb{F}_3]$.

(ii) Bestimmen Sie die Galoisgruppen $\mathrm{Gal}(E_f/\mathbb{F}_3)$ und $\mathrm{Gal}(E_g/\mathbb{F}_3)$.

(iii) Gibt es eine Beziehung zwischen E_f und E_g?

- f und g sind in $\mathbb{F}_3[X]$ irreduzibel, denn wegen $\operatorname{Grad} f = \operatorname{Grad} g = 3$ müsste sich ein Faktor vom Grad 1 abspalten, d.h. f bzw. g müsste in $\mathbb{F}_3$ eine Nullstelle besitzen. Wir berechnen aber:

$$f(\overline{0}) = \overline{1}, \quad f(\overline{1}) = \overline{4} = \overline{1}, \quad f(\overline{2}) = \overline{13} = \overline{1}$$
$$g(\overline{0}) = \overline{2}, \quad g(\overline{1}) = \overline{5} = \overline{2}, \quad g(\overline{2}) = \overline{16} = \overline{1} \quad \text{ok.}$$

- Adjungieren wir also eine Nullstelle von f bzw. g zu $\mathbb{F}_3$, so erhalten wir einen Erweiterungskörper vom Grad 3.

  Nach Vorlesung gibt es (bis auf Isomorphie) nur einen Erweiterungskörper von $\mathbb{F}_3$ vom Grad 3, nämlich

$$\mathbb{F}_{3^3} = \mathbb{F}_{27}.$$

- Nach Vorlesung ist $\mathbb{F}_{27}/\mathbb{F}_3$ eine Galoiserweiterung und damit insbesondere normale Körpererweiterung.

Da f und g eine Nullstelle in $\mathbb{F}_{27}$ besitzen und irreduzibel sind, zerfallen sie in $\mathbb{F}_{27}$ also vollständig in Linearfaktoren. Wir erhalten:

$$E_f = \mathbb{F}_{27} \quad \text{sowie} \quad E_g = \mathbb{F}_{27}$$

Also folgt:

$$\left.\begin{array}{l} [E_f : \mathbb{F}_3] = 3 \\ [E_g : \mathbb{F}_3] = 3 \end{array}\right\} \Rightarrow \text{(i) gelöst}$$

sowie $E_f = E_g \qquad \Rightarrow$ (iii) gelöst.

- Ebenfalls nach Vorlesung ist die Galoisgruppe von $\mathbb{F}_{27} / \mathbb{F}_3$ zyklisch von der Ordnung 3 (erzeugt vom Frobeniusautomorphismus). Es ist also

$$\mathrm{Gal}(E_f / \mathbb{F}_3) \simeq \mathrm{Gal}(E_g / \mathbb{F}_3) \simeq \mathbb{Z}/3\mathbb{Z}$$

$\Rightarrow$ (ii) gelöst.

$\blacksquare$

Aufgabe 3. *(3 Punkte)*

(i) Geben Sie zu den beiden Normalreihen

$$\mathbb{Z} \triangleright 15\mathbb{Z} \triangleright 60\mathbb{Z} \triangleright \{0\}$$

und

$$\mathbb{Z} \triangleright 12\mathbb{Z} \triangleright \{0\}$$

äquivalente Verfeinerungen und die zugehörigen Faktoren an.

(ii) Seien p eine Primzahl, n eine natürliche Zahl und G eine Gruppe der Ordnung p^n. Zeigen Sie: Jede Kompositionsreihe von G enthält genau $n+1$ Untergruppen.

(i) (Übungsaufgabe 9.2. (i))

- $\mathbb{Z} \triangleright 3\mathbb{Z} \triangleright 15\mathbb{Z} \triangleright 60\mathbb{Z} \triangleright \{0\}$

  ist eine Verfeinerung der ersten Reihe mit Faktoren

  $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}$ (bis auf Isomorphie).

- $\mathbb{Z} \triangleright 3\mathbb{Z} \triangleright 12\mathbb{Z} \triangleright 60\mathbb{Z} \triangleright \{0\}$

  ist eine Verfeinerung der zweiten Reihe mit Faktoren

  $\mathbb{Z}/3\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, $\mathbb{Z}$

Da beide Verfeinerungen dieselbe Länge und bis auf eine Permutation dieselben Faktoren besitzen, sind sie äquivalent.

(ii) (Übungsaufgabe 9.3. (i))

Sei $G = G_1 \trianglerighteq\!\!\!\!\!\!/\ G_2 \trianglerighteq\!\!\!\!\!\!/\ \ldots \trianglerighteq\!\!\!\!\!\!/\ G_m \trianglerighteq\!\!\!\!\!\!/\ G_{m+1} = \{e\}$

eine Kompositionsreihe ohne Wiederholungen.

Zu zeigen: $m = n$

Dazu:

Nach Vorlesung sind die Faktoren G_i/G_{i+1} auflösbar.

$\Longrightarrow$ Für $i \in \{1, \ldots, m\}$ ist G_i/G_{i+1} entweder abelsch oder wir können Gruppen

$$H_1^{(i)}, \ldots, H_{l_{i+1}}^{(i)}$$

finden, mit

$$G_i = H_1^{(i)} \trianglerighteq\!\!\!\!\!\!/\ H_2^{(i)} \trianglerighteq\!\!\!\!\!\!/\ \ldots \trianglerighteq\!\!\!\!\!\!/\ H_{l_{i+1}}^{(i)} = G_{i+1}$$

so dass $H_j^{(i)}/H_{j+1}^{(i)}$ für $j \in \{1, \ldots, l_i\}$ jeweils abelsch ist.

Nach dem Hauptsatz über endlich erzeugte abelsche Gruppen können wir wiederrum Gruppen

$$H_j^{(i)} = H_1^{(j,i)} \trianglerighteq\!\!\!\!\!\!/\ \ldots \trianglerighteq\!\!\!\!\!\!/\ H_{k_{ji}+1}^{(j,i)} = H_{j+1}^{(i)}$$

konstruieren, so dass die Faktoren jeweils zyklisch von der Ordnung p sind.

Also: Wenn es in der Ausgangsreihe Faktoren gibt, die nicht zyklisch von der Ordnung p sind, kann die Reihe verfeinert werden $\not\!\!\searrow$ Kompositionsreihe!

$\Rightarrow$ In unserer Ausgangsreihe sind alle Faktoren zyklisch von der Ordnung p, d.h. isomorph zu $\mathbb{Z}/p\mathbb{Z}$.

Aber: Eine Gruppe der Ordnung p^n kann in einer Normalreihe nur genau n verschiedene Faktoren der Ordnung p liefern.

$\Rightarrow$ Für die Kompositionsreihe zu Beginn gilt $m=n$

sowie $$G_i/G_{i+1} \cong \mathbb{Z}/p\mathbb{Z} \qquad i \in \{1, \dots, n\}.$$

$\blacksquare$

Aufgabe 4. *(4 Punkte)*
Seien E/K eine endliche Galoiserweiterung und $\alpha \in E$ ein Element mit $\sigma(\alpha) \neq \alpha$ für alle $\sigma \in \mathrm{Gal}(E/K) \setminus \{\mathrm{id}_E\}$. Zeigen Sie: α ist ein primitives Element der Erweiterung E/K.

Zu zeigen: $K(\alpha) = E$.

Zunächst ist $K \subset K(\alpha) \subset E$ ein Zwischenkörper.

Sei $U < \mathrm{Gal}(E/K)$ die gemäß des Hauptsatzes der Galoistheorie zu $K(\alpha)$ zugehörige Untergruppe, d.h.

$$E^U = K(\alpha)$$

und U besteht aus allen $\sigma \in \mathrm{Gal}(E/K)$, welche $K(\alpha)$ elementweise festhalten.

$$\overset{\text{insb.}}{\Longrightarrow} \quad \sigma(\alpha) = \alpha \quad \forall\ \sigma \in U$$

Nach Voraussetzung gilt also

$$U = \{\mathrm{id}_E\}$$

und damit

$$K(\alpha) = E^U = E^{\{\mathrm{id}_E\}} = E.$$

$\blacksquare$