Fachbereich Mathematik/Informatik **27. September 2011**
Prof. Dr. H. Brenner

Körper- und Galoistheorie

Klausur

Dauer: Zwei volle Stunden + 10 Minuten Orientierung, in denen noch nicht geschrieben werden darf.

Es sind keine Hilfsmittel erlaubt.

Alle Antworten sind zu begründen.

Es gibt insgesamt 64 Punkte. Es gilt die Sockelregelung, d.h. die Bewertung pro Aufgabe(nteil) beginnt bei der halben Punktzahl.

Zum Bestehen braucht man 16 Punkte, ab 32 Punkten gibt es eine Eins.

Tragen Sie auf dem Deckblatt Ihren Namen ein.

Viel Erfolg!

Name, Vorname: .....

Matrikelnummer: .....

Aufgabe:	1	2	3	4	5	6	7	8	9	10	11	12	13	$\sum$
mögl. Pkt.:	4	4	4	4	4	4	4	4	6	9	5	6	6	64
erhalt. Pkt.:														

Note:

Aufgabe 1. (4 Punkte)

Definiere die folgenden (kursiv gedruckten) Begriffe.

(1) Der *Grad* einer endlichen Körpererweiterung $K \subseteq L$.
(2) Das *Minimalpolynom* eines Elementes $x \in L$ in einer endlichen Körpererweiterung $K \subseteq L$.
(3) Die *Galoisgruppe* einer Körpererweiterung $K \subseteq L$.
(4) Eine *einfache Radikalerweiterung* (von Körpern).
(5) Eine *Radikalerweiterung* (von Körpern).
(6) Eine *auflösbare* Körpererweiterung $K \subseteq L$.
(7) Eine aus einer Teilmenge $T \subseteq E$ einer Ebene E *elementar konstruierbare* Gerade G.
(8) Eine *Fermatsche Primzahl*.

Lösung

(1) Bei einer endlichen Körpererweiterung $K \subseteq L$ nennt man die K-(Vektorraum-)Dimension von L den *Grad* der Körpererweiterung.
(2) Das *Minimalpolynom* von $x \in L$ (über K) ist das normierte Polynom $P \in K[X]$ von minimalem Grad mit $P(x) = 0$.
(3) Unter der *Galoisgruppe* versteht man die Gruppe der K-Algebra-Automorphismen
$$\mathrm{Aut}_K(L).$$
(4) Eine Körpererweiterung $K \subseteq L$ heißt eine *einfache Radikalerweiterung*, wenn es ein $b \in L$ gibt mit $L = K(b)$ und ein $n \in \mathbb{N}$ mit $b^n \in K$.
(5) Eine Körpererweiterung $K \subseteq L$ heißt eine *Radikalerweiterung*, wenn es Zwischenkörper
$$K \subseteq L_1 \subseteq \ldots \subseteq L_{n-1} \subseteq L_n = L$$
gibt derart, dass $L_i \subseteq L_{i+1}$ für jedes i eine einfache Radikalerweiterung ist.
(6) Eine Körpererweiterung $K \subseteq L$ heißt *auflösbar*, wenn es eine Radikalerweiterung $K \subseteq M$ mit $L \subseteq M$ gibt.
(7) Die Gerade G heißt aus $T \subseteq E$ *elementar konstruierbar*, wenn es zwei verschiedene Punkte $P, Q \in T$ gibt, so dass G die Verbindungsgerade dieser Punkte ist.
(8) Eine Primzahl der Form $2^s + 1$, wobei s eine positive natürliche Zahl ist, heißt *Fermatsche Primzahl*.

Aufgabe 2. (4 Punkte)

Formuliere die folgenden Sätze.

(1) Der *Fundamentalsatz der Algebra*.
(2) Der *Satz über die Galoiskorrespondenz* bei einer endlichen Galoiserweiterung $K \subseteq L$.
(3) Der *Satz von Abel-Ruffini*.
(4) Der *Satz über die Charakterisierung von konstruierbaren n-Ecken*.

Lösung

(1) Jedes nichtkonstante Polynom $P \in \mathbb{C}[X]$ über den komplexen Zahlen besitzt eine Nullstelle.
(2) Es sei $K \subseteq L$ eine endliche Galoiserweiterung mit der Galoisgruppe $G = \mathrm{Gal}\,(L|K)$. Dann sind die Zuordnungen
$$M \longmapsto \mathrm{Gal}\,(L|M) \text{ und } H \longmapsto \mathrm{Fix}\,(H)$$
zueinander inverse Abbildungen zwischen der Menge der Zwischenkörper M, $K \subseteq M \subseteq L$, und der Menge der Untergruppen von G. Bei dieser Korrespondenz werden die Inklusionen umgekehrt.
(3) Für $n \geq 5$ gibt es polynomiale Gleichungen (über $\mathbb{Q}$) vom Grad n, die nicht auflösbar sind.
(4) Ein reguläres n-Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn die Primfaktorzerlegung von n die Gestalt hat
$$n = 2^{\alpha} p_1 \cdots p_k \,,$$
wobei die p_i alle verschiedene Fermatsche Primzahlen sind.

AUFGABE 3. (4 Punkte)

Löse das folgende lineare Gleichungssystem über dem Körper $K = \mathbb{Q}[\sqrt{3}]$:

$$\begin{pmatrix} 2+\sqrt{3} & -\sqrt{3} \\ \frac{1}{2} & -2-3\sqrt{3} \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1-\sqrt{3} \\ 4-2\sqrt{3} \end{pmatrix} .$$

Lösung

Wir schreiben das Gleichungssystem als

$$(I)\ (2+\sqrt{3})x - \sqrt{3}y = 1-\sqrt{3}\,,$$

$$(II)\ \frac{1}{2}x - (2+3\sqrt{3})y = 4-2\sqrt{3}\,.$$

Wir multiplizieren die zweite Zeile mit $4+2\sqrt{3}$ und erhalten

$$(III)\ (2+\sqrt{3})x + (-26-16\sqrt{3})y = 4\,.$$

Wir nehmen die Differenz der ersten und der dritten Zeile und erhalten

$$(IV)\ (26+15\sqrt{3})y = -3-\sqrt{3}\,.$$

Das inverse Element von $(26+15\sqrt{3})$ ist $(26-15\sqrt{3})$, somit ist also

$$y = (26-15\sqrt{3})(-3-\sqrt{3}) = -33+19\sqrt{3}.$$

Aus der Gleichung (II) folgt daraus

$$\begin{aligned} x &= 2(4-2\sqrt{3}+(2+3\sqrt{3})y) \\ &= 8-4\sqrt{3}+2(2+3\sqrt{3})(-33+19\sqrt{3}) \\ &= 8-4\sqrt{3}+210-122\sqrt{3} \\ &= 218-126\sqrt{3}. \end{aligned}$$

Aufgabe 4. (4 Punkte)

Forme die Gleichung

$$x^4 + 3x^3 - 5x^2 + 2x - 7 = 0$$

in eine äquivalente Gleichung der Form

$$y^4 + b_2y^2 + b_1y + b_0 = 0$$

mit $b_i \in \mathbb{Q}$ um.

Lösung

Wir setzen $x = y - \frac{3}{4}$ an und drücken das Polynom bzw. die Gleichung in y aus. Es ist

$$\begin{aligned} x^4 &= (y - \frac{3}{4})^4 \\ &= y^4 - 4\frac{3}{4}y^3 + 6\frac{9}{16}y^2 - 4\frac{27}{64}y + \frac{81}{256} \\ &= y^4 - 3y^3 + \frac{27}{8}y^2 - \frac{27}{16}y + \frac{81}{256}, \end{aligned}$$

$$\begin{aligned} 3x^3 &= 3(y - \frac{3}{4})^3 \\ &= 3(y^3 - 3\frac{3}{4}y^2 + 3\frac{9}{16}y - \frac{27}{64}) \\ &= 3y^3 - \frac{27}{4}y^2 + \frac{81}{16}y - \frac{81}{64}, \end{aligned}$$

$$-5x^2 = -5(y - \frac{3}{4})^2 = -5(y^2 - \frac{3}{2}y + \frac{9}{16}) = -5y^2 + \frac{15}{2}y - \frac{45}{16}$$

und

$$2x = 2(y - \frac{3}{4}) = 2y - \frac{3}{2}.$$

Insgesamt ergibt sich also

$$\begin{aligned} x^4 + 3x^3 - 5x^2 + 2x - 7 &= y^4 + (\frac{27}{8} - \frac{27}{4} - 5)y^2 + (-\frac{27}{16} + \frac{81}{16} + \frac{15}{2} + 2)y \\ &\quad +(\frac{81}{256} - \frac{81}{64} - \frac{45}{16} - \frac{3}{2} - 7) \\ &= y^4 - \frac{67}{8}y^2 + \frac{103}{8}y - \frac{3139}{256}. \end{aligned}$$

Eine äquivalente Gleichung ist also

$$y^4 - \frac{67}{8}y^2 + \frac{103}{8}y - \frac{3139}{256} = 0\,.$$

Aufgabe 5. (4 Punkte)

Bestimme die Zerlegung des Polynoms $X^6 - 1$ in irreduzible Faktoren über den Körpern $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}/(7)$ und $\mathbb{Z}/(5)$.

Lösung

Es ist (über jedem Körper)

$$\begin{aligned} X^6 - 1 &= (X^2 - 1)(X^4 + X^2 + 1) \\ &= (X - 1)(X + 1)(X^4 + X^2 + 1) \\ &= (X - 1)(X + 1)(X^2 + X + 1)(X^2 - X + 1). \end{aligned}$$

Dies kann man direkt bestätigen, es ergibt sich aber auch aus der Produktzerlegung von $X^6 - 1$ mit Hilfe der Kreisteilungspolynome. Über den komplexen Zahlen ist

$$X^6 - 1 = \prod_{k=0}^{5} (X - e^{\frac{2\pi ik}{6}}) .$$

Da davon vier Nullstellen imaginär sind, müssen die beiden quadratischen Polynome von oben über $\mathbb{Q}$ und über $\mathbb{R}$ irreduzibel sein, so dass die obige Faktorzerlegung über diesen Körpern die Primfaktorzerlegung ist.

Über $\mathbb{Z}/(7)$ gilt aufgrund des kleinen Fermat für jede Einheit $x^6 = 1$. Daher ist die Faktorzerlegung

$$X^6 - 1 = (X - 1)(X - 2)(X - 3)(X - 4)(X - 5)(X - 6) .$$

Über $\mathbb{Z}/(5)$ haben die beiden Polynome $X^2 + X + 1$ und $X^2 - X + 1$ keine Nullstelle, sind also irreduzibel, und daher ist die obige Zerlegung auch die Primfaktorzerlegung über $\mathbb{Z}/(5)$.

Aufgabe 6. (4 Punkte)

Bestimme die Matrix des Frobenius-Homomorphismus

$$\Phi : \mathbb{F}_{125} \longrightarrow \mathbb{F}_{125}$$

bezüglich einer geeigneten $\mathbb{F}_5$-Basis von $\mathbb{F}_{125}$.

Lösung

Das Polynom $X^3 + X + 1 \in \mathbb{Z}/(5)[X]$ ist irreduzibel, da es Grad 3 hat und in $\mathbb{Z}/(5)$ keine Nullstelle besitzt. Daher ist

$$L = \mathbb{Z}/(5)[X]/(X^3 + X + 1)$$

ein Körper mit 125 Elementen, und die Restklassen von $1, X, X^2$ (die wir mit $1, x, x^2$ bezeichnen) bilden eine $\mathbb{Z}/(5)$-Basis von L. Wir beschreiben den Frobenius bezüglich dieser Basis unter Verwendung von $x^3 = -x - 1$. Es ist

$$1^5 = 1\,,$$

$$x^5 \;=\; x^2(-x-1) \;=\; -x^3 - x^2 \;=\; -x^2 + x + 1 \;=\; 4x^2 + x + 1$$

und

$$\begin{aligned}
(x^2)^5 &= x^{10} \\
&= (-x^2 + x + 1)^2 \\
&= x^4 + x^2 + 1 - 2x^3 - 2x^2 + 2x \\
&= x(-x-1) - 2(-x-1) - x^2 + 2x + 1 \\
&= -x^2 - x + 2x + 2 - x^2 + 2x + 1 \\
&= -2x^2 + 3x + 3 \\
&= 3x^2 + 3x + 3.
\end{aligned}$$

In den Spalten der beschreibenden Matrix stehen die Koeffizienten der Bildvektoren bezüglich der Basis, also ist die Matrix gleich

$$\begin{pmatrix} 1 & 1 & 3 \\ 0 & 1 & 3 \\ 0 & 4 & 3 \end{pmatrix}.$$

Aufgabe 7. (4 Punkte)

Es sei $K \subseteq L$ eine endliche Körpererweiterung, $x \in L$ $(x \neq 0)$ und sei $P \in K[X]$ das Minimalpolynom von x. Zeige, dass P irreduzibel ist.

Lösung

Es sei $P = P_1 P_2$ eine Faktorzerlegung des Minimalpolynoms. Dann gilt in L die Beziehung

$$0 = P(x) = P_1(x)P_2(x).$$

Da L ein Körper ist, muss ein Faktor null sein, sagen wir $P_1(x) = 0$. Da aber P unter allen Polynomen $\neq 0$, die x annullieren, den minimalen Grad besitzt, müssen P und P_1 den gleichen Grad besitzen und folglich muss P_2 konstant $(\neq 0)$, also eine Einheit sein.

Aufgabe 8. (4 Punkte)

Zeige, dass es zu jeder natürlichen Zahl n eine Körpererweiterung $\mathbb{Q} \subseteq L$ vom Grad n gibt.

Lösung

Sei n gegeben. Das Polynom $X^n - 2 \in \mathbb{Q}[X]$ ist nach dem Lemma von Eisenstein irreduzibel, da die Primzahl 2 alle Koeffizienten außer dem Leitkoeffizienten teilt und 2^2 den konstanten Koeffizienten nicht teilt. Daher ist

$$K_n = \mathbb{Q}[X]/(X^n - 2)$$

ein Körper. Der Grad von K_n über $\mathbb{Q}$ ist gleich dem Grad des definierenden Polynoms, also gleich n.

Aufgabe 9. (6 Punkte)

Sei $K \subseteq L$ eine endliche Körpererweiterung. Zeige, dass die Galoisgruppe $\mathrm{Gal}\,(L|K)$ endlich ist.

Lösung

Die Körpererweiterung besitzt ein endliches K-Algebra-Erzeugendensystem, also $L = K[x_1, \ldots, x_n]$. Nach Lemma 8.14 ist ein K-Algebra-Automorphismus

$$\varphi : L \longrightarrow L$$

durch $\varphi(x_i)$, $i = 1, \ldots, n$, eindeutig festgelegt. Da jedes x_i nach Satz 8.4 algebraisch ist, gibt es Polynome $F_i \neq 0$ mit $F_i(x_i) = 0$. Nach Lemma 8.5 ist auch $F_i(\varphi(x_i)) = 0$. Die Polynome F_i besitzen aber jeweils nur endlich viele Nullstellen, so dass nur endlich viele Werte für $\varphi(x_i)$ in Frage kommen.

Aufgabe 10. (9 Punkte)

Es sei K ein Körper, D eine endliche kommutative Gruppe und $K \subseteq L$ eine D-graduierte Körpererweiterung. Der Körper K enthalte eine m-te primitive Einheitswurzel, wobei m der Exponent von D sei. Zeige, dass es ein Element $v \in L$ gibt derart, dass die Menge

$$\{\varphi(v) |\, \varphi \in \mathrm{Gal}\,(L|K)\}$$

eine K-Basis von L bildet.

Lösung

Unter der Voraussetzung über die Einheitswurzeln ist die Körpererweiterung eine Galoiserweiterung und die Galoisgruppe ist in natürlicher Weise isomorph zur Charaktergruppe $D^\vee$. Insbesondere ist die Anzahl der Charaktere gleich dem Grad der Körpererweiterung. Ein Charakter χ schickt, als Automorphismus aufgefasst, ein homogenes Element x_d vom Grad d auf $\chi(d)x_d$.

Wir wählen in jeder Komponente L_d ein von 0 verschiedenes Element x_d und setzen

$$v = \sum_{d \in D} x_d\,.$$

Die Menge $\{\varphi(v) |\, \varphi \in \mathrm{Gal}\,(L|K)\}$ ist gleich

$$\{\varphi_\chi(v) = \sum_{d \in D} \chi(d)x_d |\, \chi \in D^\vee\}\,.$$

Da die Anzahl der Charaktere gleich dem Körpergrad ist, genügt es zu zeigen, dass diese Elemente linear unabhängig sind. Sei also

$$\sum_\chi c_\chi \varphi_\chi(v) = 0$$

mit $c_\chi \in K$. Das bedeutet

$$\sum_\chi c_\chi (\sum_{d \in D} \chi(d)x_d) \;=\; \sum_{d \in D} (\sum_\chi c_\chi \chi(d))x_d \;=\; 0.$$

Da die x_d, $d \in D$, linear unabhängig sind, folgt für jedes $d \in D$ die Beziehung

$$\sum_\chi c_\chi \chi(d) = 0\,.$$

Dies bedeutet wiederum für die Charaktere die Gleichheit

$$\sum_\chi c_\chi \chi = 0\,.$$

Nach dem Lemma von Dedekind sind aber die Charaktere linear unabhängig, sodass $c_\chi = 0$ ist.

Aufgabe 11. (5 Punkte)

Bestimme das Kreisteilungspolynom Φ_{14}.

Lösung

Es ist

$$\begin{aligned} X^{14}-1 &= \Phi_1 \cdot \Phi_2 \cdot \Phi_7 \cdot \Phi_{14} \\ &= (X-1)\cdot(X+1)\cdot(X^6+X^5+\ldots+X+1)\cdot\Phi_{14} \\ &= (X^2-1)\cdot(X^6+X^5+\ldots+X+1)\cdot\Phi_{14} \\ &= (X^8+X^7-X-1)\cdot\Phi_{14}. \end{aligned}$$

Polynomdivision ergibt

$$\Phi_{14} = X^6 - X^5 + X^4 - X^3 + X^2 - X + 1\,.$$

Aufgabe 12. (6 Punkte)

Es sei $P \in \mathbb{Q}[X]$ ein Polynom vom Grad 3. Zeige mit Mitteln der Galoistheorie, dass P auflösbar ist.

Lösung

Das Polynom P heißt auflösbar, wenn der Zerfällungskörper $\mathbb{Q} \subseteq L$ von P auflösbar ist. Dieser Zerfällungskörper ist eine Galoiserweiterung von $\mathbb{Q}$, und jeder Automorphismus von L permutiert die Nullstellen von P in L und ist dadurch festgelegt (siehe Lemma 13.1). Daher ist die Galoisgruppe der Körpererweiterung eine Untergruppe der Permutationsgruppe S_3. Nach Satz 21.6 ist eine galoissche Körpererweiterung genau dann auflösbar, wenn ihre Galoisgruppe auflösbar ist. Die Permutationsgruppe S_3 ist auflösbar, wie die zyklische alternierende Untergruppe $\mathbb{Z}/(3) \cong A_3 \subset S_3$ mit der Restklassengruppe $\mathbb{Z}/(2)$ zeigt. Nach Lemma 20.2 ist dann auch jede Untergruppe von S_3 auflösbar. Also ist die Galoisgruppe und damit die Körpererweiterung und das Polynom auflösbar.

Aufgabe 13. (6 Punkte)

Aus einer Menge $T \subseteq E$ seien „wie üblich“ Geraden und Kreise elementar konstruierbar. Als neue Punkte seien allerdings nur die Durchschnitte von einer Geraden mit einer Geraden und von einer Geraden mit einem Kreis erlaubt (also nicht der Durchschnitt von zwei Kreisen). Bestimme die Menge M der Punkte, die aus der Anfangsmenge $\{0, 1\}$ auf diese Weise konstruierbar ist.

Lösung

Wenn man, wie üblich, die durch die beiden Punkte 0 und 1 definierte Gerade mit $\mathbb{R}$ identifiziert, so ist die Menge M der auf diese Weise konstruierbaren Punkte gleich $\mathbb{Z}$.

Die Inklusion $\mathbb{Z} \subseteq M$ ergibt sich so: da 0 und 1 zu M gehören, ist die reelle Gerade konstruierbar. Damit ist der Kreis mit Mittelpunkt 1 durch 0 konstruierbar und der andere Schnittpunkt ist 2. Mit 2 als Mittelpunkt durch 1 erhält man 3 und so nach und nach alle natürlichen Zahlen. Die Kreise mit Mittelpunkt 0 durch n liefern auch die negativen Zahlen.

Die Inklusion $M \subseteq \mathbb{Z}$ beweisen wir durch Induktion über die Anzahl der Konstruktionsschritte. Der Induktionsanfang ist durch $\{0, 1\} \subseteq \mathbb{Z}$ gesichert. Sei vorausgesetzt, dass nach dem k-ten Konstruktionsschritt nur Elemente aus $\mathbb{Z}$ konstruiert wurden. Dann kann man daraus überhaupt nur eine Gerade konstruieren, nämlich die reelle Gerade. Daher können sich keine neuen Punkte über den Schnitt von zwei Geraden ergeben und es steht lediglich der Durchschnitt der reellen Geraden mit Kreisen als Konstruktionsverfahren zur Verfügung. Die elementar konstruierbaren Kreise besitzen als Mittelpunkt eine ganze Zahl und gehen ebenfalls durch eine ganze Zahl. Also ist der andere Schnittpunkt auch eine ganze Zahl, so dass man innerhalb von $\mathbb{Z}$ bleibt.