Fachbereich Mathematik/Informatik **21. Mai 2011**
Prof. Dr. H. Brenner

Körper- und Galoistheorie

Testklausur mit Lösungen

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. Die Gesamtpunktzahl geht doppelt in Ihre Übungspunktzahl ein.

Zur Orientierung: 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	14	$\sum$
mögl. Pkt.:	4	4	3	4	3	4	4	3	6	7	8	5	4	5	64
erhalt. Pkt.:															

Note:

Aufgabe 1. (4 Punkte)

Definiere die folgenden (kursiv gedruckten) Begriffe.

(1) Eine *endliche* Körpererweiterung $K \subseteq L$.
(2) Der *Grad* einer endlichen Körpererweiterung $K \subseteq L$.
(3) Eine *Einheit* u in einem kommutativen Ring R.
(4) Eine *n-te Einheitswurzel* z in einem Körper K ($n \in \mathbb{N}_+$).
(5) Die *Charakteristik* eines Körpers K.
(6) Ein *innerer Automorphismus* einer Gruppe G.
(7) Eine *algebraische Zahl* $z \in \mathbb{C}$.
(8) Die *Galoisgruppe* einer Körpererweiterung $K \subseteq L$.

Lösung

(1) Eine Körpererweiterung $K \subseteq L$ heißt *endlich*, wenn L ein endlichdimensionaler Vektorraum über K ist.
(2) Bei einer endlichen Körpererweiterung $K \subseteq L$ nennt man die K-(Vektorraum-)Dimension von L den *Grad* der Körpererweiterung.
(3) Ein Element u in einem kommutativen Ring R heißt *Einheit*, wenn es ein Element $v \in R$ mit $uv = 1$ gibt.
(4) Ein Element $z \in K$ heißt n-te *Einheitswurzel*, wenn $z^n = 1$ ist.
(5) Die *Charakteristik* eines Körpers K ist die kleinste positive natürliche Zahl n mit der Eigenschaft $n \cdot 1_K = 0$. Die Charakteristik ist 0, falls keine solche Zahl existiert.
(6) Ein Automorphismus
$$G \longrightarrow G$$
der Form $x \mapsto gxg^{-1}$ zu einem festen Element $g \in G$ heißt *innerer Automorphismus*.
(7) Eine Zahl $z \in \mathbb{C}$ heißt *algebraisch*, wenn es ein von 0 verschiedenes Polynom $P \in \mathbb{Q}[X]$ gibt mit $P(z) = 0$.
(8) Unter der *Galoisgruppe* versteht man die Gruppe aller K-Algebra-Automorphismen von L, also
$$\mathrm{Aut}_K(L).$$

Aufgabe 2. (4 Punkte)

Formuliere die folgenden Sätze bzw. Formeln.

(1) Die *Gradformel* für zwei endliche Körpererweiterungen $K \subseteq L$ und $L \subseteq M$.
(2) Die *trigonometrische Darstellung* der n-ten komplexen Einheitswurzeln ($n \in \mathbb{N}_+$).
(3) Der *Satz von Lagrange* über die Ordnung eines Gruppenelementes $g \in G$ in einer endlichen Gruppe G.
(4) Der *Satz über den Einsetzungshomomorphismus* zu einer R-Algebra A und einem Element $f \in A$.

Lösung

(1) Die Gradformel besagt, dass $K \subseteq M$ eine endliche Körpererweiterung ist und dass
$$\operatorname{grad}_K M = \operatorname{grad}_K L \cdot \operatorname{grad}_L M$$
gilt.
(2) Die n-ten komplexen Einheitswurzeln besitzen die Darstellung
$$\cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n}, k = 0, 1, \ldots, n-1.$$
(3) Die Ordnung von g teilt die Ordnung der Gruppe.
(4) Es gibt einen eindeutig bestimmten R-Algebra-Homomorphismus
$$\psi : R[X] \longrightarrow A$$
mit $\psi(X) = f$.

Aufgabe 3. (3 Punkte)

Bestimme eine ganze Zahl n derart, dass die Lösungen der quadratischen Gleichung

$$x^2 + 3x + \frac{7}{3} = 0$$

in $\mathbb{Q}[\sqrt{n}]$ liegen.

Lösung

Wir schreiben die Gleichung als

$$(x + \frac{3}{2})^2 = -\frac{7}{3} + \frac{9}{4} = \frac{-28 + 27}{12} = \frac{-1}{12}.$$

Daher ist

$$x + \frac{3}{2} = \pm\sqrt{\frac{-1}{12}} = \pm\frac{1}{2}\sqrt{-\frac{1}{3}} = \pm\frac{1}{6}\sqrt{-3}.$$

Also liegen die Lösungen in $\mathbb{Q}[\sqrt{-3}]$.

AUFGABE 4. (4 Punkte)

Forme die Gleichung

$$x^5 + 10x^4 + x - 5 = 0$$

in eine äquivalente Gleichung der Form

$$y^5 + b_3y^3 + b_2y^2 + b_1y + b_0 = 0$$

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

Lösung

Wir machen den Ansatz $x = y + c$. Einsetzen ergibt

$$(y + c)^5 + 10(y + c)^4 + y + c - 5 = 0\,,$$

wobei der Koeffizient zu y^4 gleich 0 werden soll. Dieser Koeffizient ist $5c+10$, also muss man

$$c = -2$$

wählen. Damit wird das Polynom zu

$$\begin{aligned}
&= (y + c)^5 + 10(y + c)^4 + y + c - 5\\
&= (y - 2)^5 + 10(y - 2)^4 + y - 2 - 5\\
&= y^5 - 5 \cdot 2y^4 + 10(-2)^2y^3 + 10(-2)^3y^2 + 5(-2)^4y - 2^5\\
&\quad +10(y^4 + 4(-2)y^3 + 6(-2)^2y^2 + 4(-2)^3y + 16) + y - 7\\
&= y^5 + 40y^3 - 80y^2 + 80y - 32 - 80y^3 + 240y^2 - 320y + 160 + y - 7\\
&= y^5 - 40y^3 + 160y^2 - 239y + 121
\end{aligned}$$

und die äquivalente Gleichung ist

$$y^5 - 40y^3 + 160y^2 - 239y + 121 \;=\; 0.$$

Aufgabe 5. (3 Punkte)

Bestimme das Minimalpolynom der komplexen Zahl $2+5i$ über $\mathbb{Q}$.

Lösung

Es ist

$$(2+5i)^2 = 4-25+20i = -21+20i.$$

Dies ist eine $\mathbb{Q}$-Linearkombination von 1 und $2+5i$, nämlich

$$-21+20i = -29 \cdot 1 + 4(2+5i).$$

Daher ist

$$Z^2 - 4Z + 29$$

ein annullierendes Polynom von $2+5i$. Wegen $2+5i \notin \mathbb{Q}$ kann es kein annullierendes Polynom von einem kleineren Grad geben, also handelt es sich um das Minimalpolynom.

Aufgabe 6. (4 Punkte)

Betrachte den Körper $K = \mathbb{F}_4 = \mathbb{Z}/(2)[U]/(U^2+U+1)$. Führe im Polynomring $K[X]$ die Polynomdivision

$$X^4 + uX^3 + (u+1)X + 1 \text{ durch } uX^2 + X + u + 1$$

aus, wobei u die Restklasse von U in K bezeichnet.

Lösung

Die Division mit Rest ergibt

$X^4+uX^3+(u+1)X+1 = (uX^2+X+u+1)((u+1)X^2+(u+1)X+(u+1))+uX+u+1\,.$

Aufgabe 7. (4 Punkte)

Finde im Polynomring $\mathbb{Z}/(2)[X]$ ein irreduzibles Polynom vom Grad vier.

Lösung

Wir betrachten das Polynom

$$F = X^4 + X + 1\,.$$

Da weder 0 noch 1 eine Nullstelle von F sind, besitzt es keinen Linearfaktor. Die einzige verbleibende Faktorzerlegung wäre als ein Produkt von zwei irreduziblen Polynomen vom Grad zwei. Das einzige irreduzible Polynom vom Grad zwei ist $X^2 + X + 1$. Wegen

$$(X^2 + X + 1)^2 \;=\; X^4 + X^2 + 1 \;\neq\; F$$

ist F irreduzibel.

Aufgabe 8. (3 Punkte)

Berechne in

$$\mathbb{Z}/(7)[X]/(X^3+4X^2+X+5)$$

das Produkt

$$(2x^2+5x+3)\cdot(3x^2+x+6)$$

(x bezeichne die Restklasse von X).

Lösung

Es ist

$$x^3 = 3x^2+6x+2$$

und

$$\begin{aligned} x^4 &= x(3x^2+6x+2) \\ &= 3x^3+6x^2+2x \\ &= 3(3x^2+6x+2)+6x^2+2x \\ &= x^2+6x+6. \end{aligned}$$

Daher ist

$$\begin{aligned} (2x^2+5x+3)\cdot(3x^2+x+6) &= 6x^4+3x^3+5x^2+5x+4 \\ &= 6(x^2+6x+6)+3(3x^2+6x+2)+5x^2+5x+4 \\ &= 6x^2+3x+4. \end{aligned}$$

Aufgabe 9. (6 Punkte)

Beweise die „Gradformel“ für eine Folge von endlichen Körpererweiterungen $K \subseteq L \subseteq M$.

Lösung

Wir setzen $\operatorname{grad}_K L = n$ und $\operatorname{grad}_L M = m$. Es sei $x_1, \ldots, x_n \in L$ eine K-Basis von L und $y_1, \ldots, y_m \in M$ eine L-Basis von M. Wir behaupten, dass die Produkte

$$x_i y_j, 1 \leq i \leq n, 1 \leq j \leq m,$$

eine K-Basis von M bilden. Wir zeigen zuerst, dass diese Produkte den Vektorraum M über K aufspannen. Sei dazu $z \in M$. Wir schreiben

$$z = b_1 y_1 + \ldots + b_m y_m \text{ mit Koeffizienten } b_j \in L.$$

Wir können jedes b_j als $b_j = a_{1j} x_1 + \ldots + a_{nj} x_n$ mit Koeffizienten $a_{ij} \in K$ ausdrücken. Das ergibt

$$\begin{aligned} z &= b_1 y_1 + \ldots + b_m y_m \\ &= (a_{11} x_1 + \ldots + a_{n1} x_n) y_1 + \ldots + (a_{1m} x_1 + \ldots + a_{nm} x_n) y_m \\ &= \sum_{1 \leq i \leq n,\, 1 \leq j \leq m} a_{ij} x_i y_j. \end{aligned}$$

Daher ist z eine K-Linearkombination der Produkte $x_i y_j$. Um zu zeigen, dass diese Produkte linear unabhängig sind, sei

$$0 = \sum_{1 \leq i \leq n,\, 1 \leq j \leq m} c_{ij} x_i y_j$$

angenommen mit $c_{ij} \in K$. Wir schreiben dies als $0 = \sum_{j=1}^{m} (\sum_{i=1}^{n} c_{ij} x_i) y_j$. Da die y_j linear unabhängig über L sind und die Koeffizienten der y_j zu L gehören folgt, dass $\sum_{i=1}^{n} c_{ij} x_i = 0$ ist für jedes j. Da die x_i linear unabhängig über K sind und $c_{ij} \in K$ ist folgt, dass $c_{ij} = 0$ ist für alle i, j.

Aufgabe 10. (7 Punkte)

Es seien k und n ganze Zahlen. Zeige, dass die folgenden Aussagen äquivalent sind.

(1) k teilt n.
(2) Es ist $\mathbb{Z}n \subseteq \mathbb{Z}k$.
(3) Es gibt einen Ringhomomorphismus
$$\mathbb{Z}/(n) \longrightarrow \mathbb{Z}/(k).$$
(4) Es gibt einen surjektiven Gruppenhomomorphismus
$$\mathbb{Z}/(n) \longrightarrow \mathbb{Z}/(k)$$

Lösung

(1) $\Rightarrow$ (2). Wenn k ein Teiler von n ist, so ist $n = ak$ mit einem $a \in \mathbb{Z}$ und daher ist $n \in \mathbb{Z}k$. Somit gilt die Idealinklusion $\mathbb{Z}n \subseteq \mathbb{Z}k$. (2) $\Rightarrow$ (3). Wegen der Idealinklusion $\mathbb{Z}n \subseteq \mathbb{Z}k$ wird unter dem Restklassen-Ringhomomorphismus
$$\mathbb{Z} \longrightarrow \mathbb{Z}/(k)$$
das Ideal $\mathbb{Z}n$ auf 0 abgebildet. Daher gibt es aufgrund des Satzes über die induzierte Abbildung einen Ringhomomorphismus
$$\mathbb{Z}/(n) \longrightarrow \mathbb{Z}/(k).$$
(3) $\Rightarrow$ (4). Es sei
$$\varphi : \mathbb{Z}/(n) \longrightarrow \mathbb{Z}/(k)$$
der gegebene Ringhomomorphismus. Dieser ist insbesondere ein Gruppenhomomorphismus, und es gilt $\varphi(1) = 1$. Da die $1 \in \mathbb{Z}/(k)$ diese Gruppe erzeugt, ist φ surjektiv. (4) $\Rightarrow$ (1). Es sei
$$\varphi : \mathbb{Z}/(n) \longrightarrow \mathbb{Z}/(k)$$
ein surjektiver Gruppenhomomorphismus. Bei $n = 0$ ist die Aussage richtig. Sei also $n \neq 0$, so dass die angegebenen Gruppen die endlichen Ordnungen n bzw. k besitzen. Dabei ist nach dem Isomorphiesatz die Gruppe $\mathbb{Z}/(k)$ isomorph zu einer Restklassengruppe von $\mathbb{Z}/(n)$ und aufgrund der Indexformel ist k (die Anzahl der Nebenklassen) ein Teiler von n.

Aufgabe 11. (8 Punkte)

Es sei $n \in \mathbb{N}_+$ und es sei $\mu_n \subseteq \mathbb{C}$ die Menge der n-ten komplexen Einheitswurzeln. Es sei $F \in \mathbb{C}[X]$ ein Polynom. Zeige, dass $F \in \mathbb{C}[X^n]$ (d.h., dass F als Polynom in X^n geschrieben werden kann) genau dann gilt, wenn für jedes $z \in \mu_n$ die Gleichheit

$$F(zX) = F(X)$$

gilt.

Lösung

Sei zunächst $F \in \mathbb{C}[X^n]$. Dann schreiben wir $F = \sum_{i=0}^{k} a_i (X^n)^i$. Für $z \in \mu_n$ ist somit

$$F(zX) = \sum_{i=0}^{k} a_i ((zX)^n)^i = \sum_{i=0}^{k} a_i (z^n X^n)^i = \sum_{i=0}^{k} a_i (X^n)^i = F(X).$$

Für die Umkehrung sei

$$F = \sum_{i=0}^{k} c_i X^i .$$

Es sei z eine primitive n-te Einheitswurzel, so dass man alle Einheitswurzeln eindeutig als z^j, $j = 0, \ldots, n-1$, schreiben kann. Es ist

$$\begin{aligned} nF(X) &= \sum_{j=0}^{n-1} F(z^j X) \\ &= \sum_{j=0}^{n-1} (\sum_{i=0}^{k} c_i (z^j)^i X^i) \\ &= \sum_{i=0}^{k} (c_i \sum_{j=0}^{n-1} (z^i)^j) X^i. \end{aligned}$$

Wir zeigen, dass die Koeffizienten zu X^i, wenn i kein Vielfaches von n ist, gleich 0 sind. Dies gilt dann auch für F.

Sei also i kein Vielfaches von n. Da z primitiv ist, ist $w = z^i$ eine n-te Einheitswurzel, aber nicht 1. Wegen der Faktorisierung

$$X^n - 1 = (X-1)(X^{n-1} + \ldots + X + 1)$$

ist daher $\sum_{j=0}^{n-1} w^j = 0$.

Aufgabe 12. (5 Punkte)

Sei K ein Körper und $K[X]$ der Polynomring über K. Zeige unter Verwendung der Division mit Rest, dass $K[X]$ ein Hauptidealbereich ist.

Lösung

Sei I ein von null verschiedenes Ideal in $K[X]$. Betrachte die nichtleere Menge

$$\{\operatorname{grad}(P) |\, P \in I,\, P \neq 0\}\,.$$

Diese Menge hat ein Minimum $m \in \mathbb{N}$, das von einem Element $F \in I$, $F \neq 0$, herrührt, sagen wir $m = \operatorname{grad}(F)$. Wir behaupten, dass $I = (F)$ ist. Sei hierzu $P \in I$ gegeben. Aufgrund der Division mit Rest gilt

$$P = FQ + R \text{ mit } \operatorname{grad}(R) < \operatorname{grad}(F) \text{ oder } R = 0\,.$$

Wegen $R \in I$ und der Minimalität von $\operatorname{grad}(F)$ kann der erste Fall nicht eintreten. Also ist $R = 0$ und P ist ein Vielfaches von F.

Aufgabe 13. (4 Punkte)

Bestimme die Galoisgruppe (einschließlich der Gruppenstruktur) der Körpererweiterung $\mathbb{Q} \subseteq \mathbb{Q}[i]$.

Lösung

Es ist $\mathbb{Q}[i] \cong \mathbb{Q}[X]/(X^2+1)$. Ein $\mathbb{Q}$-Algebra-Homomorphismus muss i auf eine Nullstelle von X^2+1 schicken, also auf i oder auf $-i$. Die dadurch definierten surjektiven Einsetzungshomomorphismen

$$\mathbb{Q}[X] \longrightarrow \mathbb{Q}[i]$$

legen nach dem Isomorphiesatz einen $\mathbb{Q}$-Algebra-Automorphismus

$$\mathbb{Q}[i] \longrightarrow \mathbb{Q}[i]$$

fest. Die Galoisgruppe besteht also aus der Identität und der Konjugation $a+bi \mapsto a-bi$. Die Identität ist das neutrale Element dieser Gruppe und die Hintereinanderausführung der Konjugation ist die Identität, was die Gruppenstruktur festlegt.

Aufgabe 14. (5 (3+2) Punkte)

Es seien D_1 und D_2 kommutative Gruppen und seien $D_1^\vee$ und $D_2^\vee$ die zugehörigen Charaktergruppen zu einem Körper K.

(1) Zeige, dass zu einem Gruppenhomomorphismus
$$\varphi : D_1 \longrightarrow D_2$$
durch die Zuordnung $\chi \mapsto \chi \circ \varphi$ ein Gruppenhomomorphismus
$$\varphi^\vee : D_2^\vee \longrightarrow D_1^\vee$$
definiert wird.

(2) Es sei D_3 eine weitere kommutative Gruppe und sei
$$\psi : D_2 \longrightarrow D_3$$
ein Gruppenhomomorphismus. Zeige die Gleichheit
$$(\psi \circ \varphi)^\vee = \varphi^\vee \circ \psi^\vee.$$

Lösung

(1) Ein Charakter $\chi \in D_2^\vee$ ist ein Gruppenhomomorphismus
$$D_2 \longrightarrow K^\times,$$
daher ist die Verknüpfung
$$\chi \circ \varphi : D_1 \longrightarrow K^\times$$
ein Element aus $D_1^\vee$, die Abbildung ist also wohldefiniert. Zu zwei Charakteren $\chi_1, \chi_2 \in D_2^\vee$ und einem beliebigen Element $d \in D_1$ ist
$$\begin{aligned} ((\chi_1 \cdot \chi_2) \circ \varphi)(d) &= (\chi_1 \cdot \chi_2)(\varphi(d)) \\ &= \chi_1(\varphi(d)) \cdot \chi_2(\varphi(d)) \\ &= ((\chi_1 \circ \varphi)(d)) \cdot ((\chi_2 \circ \varphi)(d)) \\ &= ((\chi_1 \circ \varphi) \cdot (\chi_2 \circ \varphi))(d). \end{aligned}$$
Also ist
$$\varphi^\vee(\chi_1 \cdot \chi_2) = (\chi_1 \cdot \chi_2) \circ \varphi = (\chi_1 \circ \varphi) \cdot (\chi_2 \circ \varphi) = \varphi^\vee(\chi_1) \cdot \varphi^\vee(\chi_2)$$
und die Zuordnung ist ein Gruppenhomomorphismus.

(2) Dies ergibt sich für $\chi \in D_3^\vee$ direkt aus
$$(\psi \circ \varphi)^\vee(\chi) = \chi \circ (\psi \circ \varphi) = (\chi \circ \psi) \circ \varphi = \varphi^\vee(\chi \circ \psi) = \varphi^\vee(\psi^\vee(\chi)) = (\varphi^\vee \circ \psi^\vee)(\chi).$$