Fachbereich Mathematik/Informatik **2. Juli 2011**
Prof. Dr. H. Brenner

Körper- und Galoistheorie

Testklausur II 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	4	3	5	4	3	3	5	5	10	7	64
erhalt. Pkt.:															

Note:

AUFGABE 1. (4 Punkte)

Definiere die folgenden (kursiv gedruckten) Begriffe.

(1) Ein *Normalteiler* N in einer Gruppe G.
(2) Eine *auflösbare* Gruppe G.
(3) Eine *n-te primitive* Einheitswurzel ζ in einem Körper K ($n \in \mathbb{N}_+$).
(4) Der *Grad* einer endlichen Körpererweiterung $K \subseteq L$.
(5) Ein *separables* Polynom $P \in K[X]$ über einem Körper K.
(6) Die *Galoisgruppe* einer Körpererweiterung $K \subseteq L$.
(7) Eine (endliche) *Galoiserweiterung* $K \subseteq L$.
(8) Der n-te *Kreisteilungskörper* (über $\mathbb{Q}$).

Lösung

(1) Ein Untergruppe $H \subseteq G$ ist ein *Normalteiler*, wenn
$$xH = Hx$$
ist für alle $x \in G$.
(2) Eine Gruppe G heißt *auflösbar*, wenn es eine Filtrierung
$$\{e\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq \ldots \subseteq G_{k-1} \subseteq G_k = G$$
gibt derart, dass G_i ein Normalteiler in G_{i+1} ist und die Restklassengruppe G_{i+1}/G_i abelsch ist (für jedes $i = 0, \ldots, k-1$).
(3) Eine n-te Einheitswurzel heißt *primitiv*, wenn sie die Ordnung n besitzt.
(4) Bei einer endlichen Körpererweiterung $K \subseteq L$ nennt man die K-(Vektorraum-)Dimension von L den *Grad* der Körpererweiterung.
(5) Ein Polynom $P \in K[X]$ heißt *separabel*, wenn es über keinem Erweiterungskörper $K \subseteq L$ mehrfache Nullstellen besitzt.
(6) Unter der *Galoisgruppe* versteht man die Gruppe der K-Algebra-Automorphismen
$$\mathrm{Aut}_K(L).$$
(7) Eine endliche Körpererweiterung $K \subseteq L$ heißt eine *Galoiserweiterung*, wenn
$$\#(\mathrm{Gal}(L|K)) = \mathrm{grad}_K L$$
gilt.
(8) Der n-te *Kreisteilungskörper* ist der Zerfällungskörper des Polynoms
$$X^n - 1$$
über $\mathbb{Q}$.

Aufgabe 2. (4 Punkte)

Formuliere die folgenden Sätze bzw. Formeln.

(1) Das *Lemma von Dedekind* für Charaktere auf einem Monoid M in einen Körper K.
(2) Der *Satz über die Galoiskorrespondenz* bei einer endlichen Galoiserweiterung $K \subseteq L$.
(3) Das *Eisensteinsche Irreduzibilitätskriterium* (über $\mathbb{Z}$ bzw. $\mathbb{Q}$).
(4) Der *Satz über den Grad der Kreisteilungskörper* (über $\mathbb{Q}$).

Lösung

(1) Es sei G ein Monoid, K ein Körper und $\chi_1, \ldots, \chi_n \in \operatorname{Char}(G, K)$ seien n Charaktere. Dann sind diese Charaktere linear unabhängig (als Elemente in $\operatorname{Hom}_K(G, K)$).
(2) Es sei $K \subseteq L$ eine endliche Galoiserweiterung mit der Galoisgruppe $G = \operatorname{Gal}(L|K)$. Dann sind die Zuordnungen
$$M \longmapsto \operatorname{Gal}(L|M) \text{ und } H \longmapsto \operatorname{Fix}(H)$$
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) Es sei $F = \sum_{i=0}^{n} c_i X^i \in \mathbb{Z}[X]$ ein Polynom. Es sei $p \in \mathbb{Z}$ eine Primzahl mit der Eigenschaft, dass p den Leitkoeffizienten c_n nicht teilt, aber alle anderen Koeffizienten teilt, aber dass p^2 nicht den konstanten Koeffizienten c_0 teilt. Dann ist F irreduzibel in $\mathbb{Q}[X]$.
(4) Der Kreisteilungskörper K_n besitzt über $\mathbb{Q}$ den Grad $\varphi(n)$ (φ die eulersche φ-Funktion).

Aufgabe 3. (3 Punkte)

Bestimme das Minimalpolynom der komplexen Zahl $\pi + ei$ über $\mathbb{R}$.

Lösung

Wegen $e \neq 0$ gehört diese Zahl nicht zu $\mathbb{R}$, daher besitzt das Minimalpolynom den Grad 2. Es ist

$$(\pi+ei)^2 = \pi^2-e^2+2\pi ei = \pi^2-e^2+2\pi(\pi+ei)-2\pi^2 = 2\pi(\pi+ei)-\pi^2-e^2.$$

Daher ist

$$X^2 - 2\pi X + \pi^2 + e^2$$

das Minimalpolynom.

Aufgabe 4. (4 (1+1+2) Punkte)

a) Zeige, dass durch

$$K = \mathbb{Z}/(7)[T]/(T^3 - 2)$$

ein Körper mit 343 Elementen gegeben ist.

b) Berechne in K das Produkt $(T^2 + 2T + 4)(2T^2 + 5)$.

c) Berechne das (multiplikativ) Inverse zu $T + 1$.

Lösung

a) Es ist

$$1^3 = 1,\ 2^3 = 1,\ 3^3 = 6,\ 4^3 = 1,\ 5^3 = 6,\ 6^3 = 6\,.$$

Also besitzt das Polynom $T^3 - 2$ keine Nullstelle in $\mathbb{Z}/(7)$ und ist somit irreduzibel, also ist $\mathbb{Z}/(7)[T]/(T^3-2)$ ein Körper. Die Restklassen von $1, T, T^2$ bilden eine $\mathbb{Z}/(7)$-Basis, so dass dieser Körper $7^3 = 343$ Elemente besitzt.

b) Es ist

$$\begin{aligned}(T^2 + 2T + 4)(2T^2 + 5) &= 2T^4 + 4T^3 + 6T^2 + 3T + 6\\ &= 4T + 1 + 6T^2 + 3T + 6\\ &= 6T^2.\end{aligned}$$

c) Polynomdivision liefert

$$T^3 - 2 = (T^2 + 6T + 1)(T + 1) + 4\,.$$

In K gilt somit $(T + 1)(T^2 + 6T + 1) = 3$. Das Inverse von 3 in $\mathbb{Z}/(7)$ ist 5, also ist $5T^2 + 2T + 5$ das Inverse von $T + 1$.

Aufgabe 5. (4 (1+1+1+1) Punkte)

Wir betrachten das Polynom

$$P = X^{7129} + 105X^{103} + 15X + 45\,.$$

Bestimme für die folgenden Körper K, ob P irreduzibel in $K[X]$ ist.

a) $K = \mathbb{Q}$.

b) $K = \mathbb{R}$.

c) $K = \mathbb{Z}/(2)$.

d) $K = \mathbb{Q}[T]/(T^{7129} + 105T^{103} + 15T + 45)$.

Lösung

a) Wir können das Eisenstein-Kriterium mit der Primzahl 5 anwenden. Die 5 teilt alle Koeffizienten von P außer dem Leitkoeffizienten, und 5^2 teilt nicht den konstanten Term. Also ist P irreduzibel in $\mathbb{Q}[X]$.

b) Das Polynom hat ungeraden Grad, daher besitzt es aufgrund des Zwischenwertsatzes eine reelle Nullstelle und ist daher nicht irreduzibel in $\mathbb{R}[X]$.

c) Über $K = \mathbb{Z}/(2)$ wird das Polynom zu $X^{7129} + X^{103} + X + 1$, das die Nullstelle 1 besitzt. Also ist P nicht irreduzibel in $\mathbb{Z}/(2)[X]$.

d) Zunächst ist K ein Körper aufgrund von Teil (a). Es sei t die Restklasse von T. In K ist nach Konstruktion $P(t) = 0$, also ist t eine Nullstelle von P und P ist nicht irreduzibel in $K[X]$.

Aufgabe 6. (3 (1+2) Punkte)

Sei $\mathbb{Q} \subseteq K$ eine endliche normale Körpererweiterung und sei

$$\kappa : \mathbb{C} \longrightarrow \mathbb{C}$$

die komplexe Konjugation.

a) Zeige, dass $\kappa(K) \subseteq K$ gilt.

b) Zeige, dass $\kappa|_K = \mathrm{id}_K$ genau dann gilt, wenn $K \subseteq \mathbb{R}$ ist.

Lösung

a) Die Verknüpfung $K \xrightarrow{\iota} \mathbb{C} \xrightarrow{\kappa} \mathbb{C}$ (ι die Inklusion) ist ein $\mathbb{Q}$-Algebra-Homomorphismus, daher ist das Bild dieser Abbildung nach Satz 14.3 gleich K.

b) Bei $K \subseteq \mathbb{R}$ ist natürlich $\kappa|_K = \mathrm{id}_K$, da die komplexe Konjugation auf $\mathbb{R}$ die Identität ist und sich diese Eigenschaft auf eine Teilmenge überträgt. Wenn andererseits $K \not\subseteq \mathbb{R}$ ist, so gibt es (wegen $K \subseteq \mathbb{C}$) ein $a + bi \in K$ mit $b \neq 0$. Für dieses Element ist $\kappa(a+bi) = a-bi \neq a+bi$, so dass die komplexe Konjugation nicht die Identität auf K ist.

Aufgabe 7. (5 Punkte)

Es sei K ein Körper. Beweise die Produktregel für das formale Ableiten

$$D : K[X] \longrightarrow K[X],\ F \longmapsto F'.$$

Lösung

Die Produktregel besagt

$$(F \cdot G)' = F \cdot G' + F' \cdot G\,.$$

Nach Definition ist die Ableitung $F \mapsto F'$ eine K-lineare Abbildung. Deshalb und aufgrund des Distributivgesetzes sind für festes G die Abbildungen

$$F \longmapsto F \cdot G \longmapsto (F \cdot G)'\,,$$

$$F \longmapsto F \cdot G'$$

und

$$F \longmapsto F' \cdot G$$

K-linear. Da jedes F eine eindeutige Darstellung als K-Linearkombination mit den Potenzen X^n, $n \in \mathbb{N}$, besitzt, genügt es, die Aussage für $F = X^n$ zu zeigen. Die gleiche Überlegung zeigt, dass man lediglich $G = X^m$ betrachten muss. Dann gilt einerseits

$$(X^n \cdot X^m)' \;=\; (X^{n+m})' \;=\; (n+m)X^{n+m-1}$$

und andererseits

$$\begin{aligned} X^n \cdot (X^m)' + (X^n)' \cdot X^m &= mX^nX^{m-1} + nX^{n-1}X^m \\ &= mX^{n+m-1} + nX^{n+m-1} \\ &= (n+m)X^{n+m-1}, \end{aligned}$$

so dass Gleichheit gilt.

Aufgabe 8. (4 Punkte)

Beweise das Lemma von Dedekind für zwei Charaktere

$$\chi_1, \chi_2 : G \longrightarrow K$$

auf einem Monoid G in einen Körper K.

Lösung

Wir müssen zeigen, dass χ_1 und χ_2 als Abbildungen von G nach K linear unabhängig sind. Das bedeutet, dass sie sich nicht um einen konstanten Faktor unterscheiden. Wir nehmen $\chi_2 = a \cdot \chi_1$ mit $a \in K^\times$ an. Wegen $\chi_1(e) = \chi_2(e) = 1$ für das neutrale Element $e \in G$ muss $a = 1$ sein. Dann ist aber $\chi_2 = \chi_1$ und es würden nicht zwei verschiedene Charaktere vorliegen.

Aufgabe 9. (3 Punkte)

Bestimme die Matrix des Frobenius-Homomorphismus

$$\Phi : \mathbb{F}_{25} \longrightarrow \mathbb{F}_{25}$$

bzgl. einer geeigneten $\mathbb{F}_5$-Basis von $\mathbb{F}_{25}$.

Lösung

Wegen $1^2 = (-1)^2 = 1$ und $2^2 = 3^2 = 4$ in $\mathbb{F}_5 = \mathbb{Z}/(5)$ ist $X^2 - 2$ irreduzibel über $\mathbb{F}_5$. Daher ist $\mathbb{F}_{25} = \mathbb{Z}/(5)[X]/(X^2 - 2)$. Wir betrachten den Frobenius-Homomorphismus bzgl. der Basis 1 und x (x sei die Restklasse von X). Dabei ist $1^5 = 1$ und

$$x^5 \;=\; x^2 \cdot x^2 \cdot x \;=\; 2 \cdot 2 \cdot x \;=\; 4x.$$

Also ist

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

die beschreibende Matrix.

Aufgabe 10. (3 Punkte)

Wie viele Unterkörper besitzt der endliche Körper $\mathbb{F}_{625}$?

Lösung

Wegen $625 = 5^4$ ist die Galoisgruppe der Körpererweiterung $\mathbb{F}_5 \subset \mathbb{F}_{625}$ zyklisch der Ordnung 4, also isomorph zu $\mathbb{Z}/(4)$. Diese Gruppe besitzt drei Untergruppen, nämlich 0, die durch 2 erzeugte Untergruppe und sich selbst. Nach dem Satz über die Galoiskorrespondenz besitzt daher $\mathbb{F}_{625}$ drei Zwischenkörper.

Aufgabe 11. (5 Punkte)

Sei $D = \mathbb{Z}/(n)$ und sei K ein Körper, der eine n-te primitive Einheitswurzel ζ enthält. Es sei L eine D-graduierte Körpererweiterung von K. Beschreibe die Matrizen der K-Algebra-Automorphismen auf L (also die Elemente der Galoisgruppe $\mathrm{Gal}\,(L|K)$) bezüglich einer geeigneten K-Basis von L.

Lösung

Die Automorphismen auf L entsprechen den Charakteren auf $D = \mathbb{Z}/(n)$. Diese entsprechen wiederum eindeutig dem Bild der 1, welches eine n-te Einheitswurzel sein muss, also sich mittels der gegebenen primitiven Einheitswuzel als ζ^i mit einem eindeutigen i zwischen 0 und $n-1$ schreiben lässt. Es sei $x \in L_1$ ein von 0 verschiedenes Element der ersten Stufe. Dann bilden die x^d, $0 \leq d \leq n-1$, eine K-Basis von L. Der zu einem Charakter χ gehörende Automorphismus wirkt dabei in der d-ten Stufe durch Multiplikation mit $\chi(d)$. Daher besitzt der Automorphismus zum Charakter χ mit $\chi(1) = \zeta^i$ bzgl. dieser Basis die Matrixdarstellung

$$\begin{pmatrix} \zeta^0 & 0 & \dots & \dots & 0 \\ 0 & \zeta^i & 0 & \dots & 0 \\ 0 & 0 & \zeta^{2i} & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \dots & 0 & \zeta^{i(n-1)} \end{pmatrix}.$$

Aufgabe 12. (5 Punkte)

Es sei $K \subseteq L$ eine endliche Galoiserweiterung mit Galoisgruppe G und es seien $H_1, H_2 \subseteq G$ Untergruppen mit den zugehörigen Fixkörpern $K_1 = \mathrm{Fix}\,(H_1)$ und $K_2 = \mathrm{Fix}\,(H_2)$. Zeige, dass der Durchschnitt $K_1 \cap K_2$ gleich dem Fixkörper zu H ist, wobei H die von H_1 und H_2 erzeugte Untergruppe bezeichnet (das ist die kleinste Untergruppe von G, die sowohl H_1 als auch H_2 enthält).

Lösung

Es sei zuerst $x \in \mathrm{Fix}\,(H)$. Wegen $H_1, H_2 \subseteq H$ ist insbesondere $x \in \mathrm{Fix}\,(H_1)$ und $x \in \mathrm{Fix}\,(H_2)$, also auch $x \in \mathrm{Fix}\,(H_1) \cap \mathrm{Fix}\,(H_2) = K_1 \cap K_2$.

Aufgrund der Galoiskorrespondenz können wir die andere Inklusion $K_1 \cap K_2 \subseteq \mathrm{Fix}\,(H)$ dadurch zeigen, dass wir die umgekehrte Inklusion der Galoisgruppen nachweisen. D.h. wir müssen $H \subseteq \mathrm{Gal}\,(L|K_1 \cap K_2)$ zeigen. Da rechts eine Gruppe steht und H die von H_1 und H_2 erzeugte Untergruppe ist, müssen wir lediglich $H_1, H_2 \subseteq \mathrm{Gal}\,(L|K_1 \cap K_2)$ zeigen. Wegen $K_1 \cap K_2 \subseteq K_1$ ist aber $H_1 \subseteq \mathrm{Gal}\,(L|K_1 \cap K_2)$ (ebenso für H_2).

Aufgabe 13. (10 (4+6) Punkte)

Es sei $\mathbb{Q} \subseteq K_n$ (in $\mathbb{C}$) der n-te Kreisteilungskörper und sei ζ eine n-te primitive Einheitswurzel. Wir betrachten die Elemente ζ^i, $i \in (\mathbb{Z}/(n))^\times$.

a) Zeige, dass für eine Primzahl $n = p$ diese Elemente eine $\mathbb{Q}$-Basis von K_n bilden.

b) Sei p eine Primzahl und $n = p^2$. Zeige, dass diese Elemente keine $\mathbb{Q}$-Basis von K_n bilden.

Lösung

a) Der Kreisteilungskörper K_n wird beschrieben als $K_n = \mathbb{Q}[X]/(\Phi_n)$ mit dem n-ten Kreisteilungspolynom Φ_n. Dieses hat den Grad $\varphi(n)$ (mit der eulerschen φ-Funktion), und X wird durch ζ ersetzt. Daher ist $\zeta^0, \zeta^1, \ldots, \zeta^{\varphi(n)-1}$ eine $\mathbb{Q}$-Basis von K_n. Bei $n = p$ ist $\varphi(p) = p - 1$ und wir betrachten die Elemente ζ^i, $i = 1, \ldots, p-1$. Das p-te Kreisteilungspolynom ist $X^{p-1} + X^{p-2} + \ldots + X + 1$. Daher ist

$$1 \;=\; -\zeta^{p-1} - \zeta^{p-2} - \ldots - \zeta,$$

so dass man die 1 als Linearkombination der angegebenen Elemente darstellen kann. Daher bilden sie ein Erzeugendensystem und somit auch eine Basis, da es sich um $\varphi(p)$ Elemente handelt.

b) Die Einheiten in $\mathbb{Z}/(p^2)$ sind alle Zahlen, die keine Vielfachen von p sind. Es gilt

$$0 = 1 + \zeta + \zeta^2 + \ldots + \zeta^{n-1}\,.$$

Wir schreiben diese Summe als

$$0 \;=\; \sum_{i=0}^{n-1} \zeta^i \;=\; \sum_{i=0,\, p|i}^{n-1} \zeta^i + \sum_{i=0,\, p\not|\, i}^{n-1} \zeta^i \;=\; \sum_{j=0}^{p-1} \zeta^{pj} + \sum_{i=0,\, p\not|\, i}^{n-1} \zeta^i.$$

Da ζ eine p^2-te primitive Einheitswurzel ist, ist ζ^p eine p-te primitive Einheitswurzel. Die linke Summe ist daher

$$\sum_{j=0}^{p-1} \zeta^{pj} \;=\; \sum_{j=0}^{p-1} (\zeta^p)^j \;=\; 0.$$

Also ist auch die rechte Summe

$$\sum_{i=0,\, p\not|\, i}^{n-1} \zeta^i \;=\; 0.$$

Dies ist aber die Summe über alle Elemente aus unserer Familie, so dass diese Familie linear abhängig ist.

Aufgabe 14. (7 Punkte)

Es sei G eine auflösbare Gruppe und

$$q : G \longrightarrow H$$

ein surjektiver Gruppenhomomorphismus. Zeige, dass auch H auflösbar ist.

Lösung

Wir fixieren eine auflösende Filtrierung

$$\{e\} = G_0 \subseteq G_1 \subseteq G_2 \subseteq \ldots \subseteq G_{k-1} \subseteq G_k = G$$

und setzen $H_i = q(G_i)$, dies ist eine Filtrierung von H mit Untergruppen. Wir betrachten das kommutative Diagramm

$$\begin{array}{ccc} G_i & \longrightarrow & G_{i+1} \\ \downarrow & & \downarrow \\ H_i & \longrightarrow & H_{i+1} \end{array} ,$$

wobei die vertikalen Homomorphismen surjektiv sind. Wir behaupten, dass H_i ein Normalteiler in H_{i+1} ist, und ziehen dazu Lemma 5.4 heran. Sei also $h \in H_i$ und $x \in H_{i+1}$, die wir durch $\tilde{h} \in G_i$ bzw. $\tilde{x} \in G_{i+1}$ repräsentieren. Dann ist $xhx^{-1} = q(\tilde{x}\tilde{h}\tilde{x}^{-1})$ und wegen der Normalität von G_i ist $\tilde{x}\tilde{h}\tilde{x}^{-1} \in G_i$ und somit $xhx^{-1} \in H_i$. Wir betrachten die zusammengesetzte surjektive Abbildung

$$G_{i+1} \longrightarrow H_{i+1} \longrightarrow H_{i+1}/H_i \, .$$

Da G_i zum Kern dieser Abbildung gehört, gibt es aufgrund von Satz 5.10 eine surjektive Abbildung

$$G_{i+1}/G_i \longrightarrow H_{i+1}/H_i,$$

weshalb H_{i+1}/H_i ebenfalls kommutativ ist.