Fachbereich Mathematik/Informatik **14. Januar 2012**
Prof. Dr. H. Brenner

Körper- und Galoistheorie

Nachklausur 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.

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: .....

Ich erkäre mich durch meine Unterschrift einverstanden, dass mein Klausurergebnis mit meiner Matrikelnummer im Internet bekanntgegeben wird.

Unterschrift: .....

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

Note:

AUFGABE 1. (4 Punkte)

Definiere die folgenden (kursiv gedruckten) Begriffe.

(1) Eine *n-te* Einheitswurzel ζ in einem Körper K ($n \in \mathbb{N}_+$).
(2) Der *Grad* einer endlichen Körpererweiterung $K \subseteq L$.
(3) Eine *algebraische Zahl* $z \in \mathbb{C}$.
(4) Zwei *konjugierte* Elemente $x, y \in L$ in einer endlichen Körpererweiterung $K \subseteq L$.
(5) Die *Galoisgruppe* einer Körpererweiterung $K \subseteq L$.
(6) Eine (endliche) *Galoiserweiterung* $K \subseteq L$.
(7) Eine *auflösbare* Gruppe G.
(8) Ein *konstruierbares* n-Eck ($n \in \mathbb{N}_+$).

Lösung

(1) Ein Element $\zeta \in K$ heißt n-te *Einheitswurzel*, wenn $\zeta^n = 1$ ist.
(2) Bei einer endlichen Körpererweiterung $K \subseteq L$ nennt man die K-(Vektorraum-)Dimension von L den *Grad* der Körpererweiterung.
(3) Eine Zahl $z \in \mathbb{C}$ heißt *algebraisch*, wenn es ein von 0 verschiedenes Polynom $P \in \mathbb{Q}[X]$ gibt mit $P(z) = 0$.
(4) Die zwei Elemente $x, y \in L$ heißen *konjugiert*, wenn ihre Minimalpolynome übereinstimmen.
(5) Unter der *Galoisgruppe* versteht man die Gruppe aller K-Algebra-Automorphismen von L, also
$$\mathrm{Aut}_K(L).$$
(6) Eine endliche Körpererweiterung $K \subseteq L$ heißt eine *Galoiserweiterung*, wenn
$$\#(\mathrm{Gal}(L|K)) = \mathrm{grad}_K L$$
gilt.
(7) 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 $i = 0, \ldots, k-1$).
(8) Man sagt, dass *das regelmäßige n-Eck mit Zirkel und Lineal konstruierbar* ist, wenn die komplexe Zahl
$$e^{2\pi i/n} = \cos(\frac{2\pi}{n}) + i \sin(\frac{2\pi}{n})$$
eine konstruierbare Zahl ist.

Aufgabe 2. (4 Punkte)

Formuliere die folgenden Sätze.

(1) Das *Lemma von Bezout* für Hauptidealbereiche.
(2) Der *Satz über den Zusammenhang zwischen Charakteren von D und Automorphismen von D-graduierten Körpererweiterungen $K \subseteq L$.*
(3) Der *Hauptsatz über endliche Körper.*
(4) Der *Satz über konjugierte Elemente bei einer normalen Körpererweiterung.*

Lösung

(1) Sei R ein Hauptidealbereich und seien $a, b \in R$ zwei teilerfremde Elemente. Dann kann man die 1 als Linearkombination von a und b darstellen, d.h. es gibt Elemente $r, s \in R$ mit $ra + sb = 1$.
(2) Bei einer D-graduierten Körpererweiterung $K \subseteq L$ gibt es einen injektiven Gruppenhomomorphismus
$$D^\vee = \mathrm{Char}\,(D, K) \longrightarrow \mathrm{Gal}\,(L|K),\ \chi \longmapsto (a_d \mapsto \chi(d)a_d),$$
der Charaktergruppe von D in die Galoisgruppe der Körpererweiterung.
(3) Zu jeder echten Primzahlpotenz p^e gibt es bis auf Isomorphie genau einen endlichen Körper mit p^e Elementen.
(4) Bei einer endlichen normalen Körpererweiterung sind zwei Elemente $x, y \in L$ genau dann konjugiert, wenn es einen K-Automorphismus $\varphi : L \to L$ mit $\varphi(x) = y$ gibt.

AUFGABE 3. (4 Punkte)

Löse das folgende lineare Gleichungssystem über dem Körper $K = \mathbb{F}_9 = \mathbb{Z}/(3)[U]/(U^2+1)$, wobei die Restklasse von U mit u bezeichnet sei.

$$\begin{pmatrix} 1+2u & 2 \\ 2+u & 2+2u \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1+u \\ 1+2u \end{pmatrix}.$$

Lösung

Wir berechnen die neue Gleichung $II' = II - (1+u)I$, dies ist

$$\begin{aligned} (2+u-(1+u)(1+2u))x &= (1+2u)-(1+u)(1+u) \\ &= 1+2u-1-2u-u^2 \\ &= 1. \end{aligned}$$

Der Vorfaktor ist

$$2+u-(1+u)(1+2u) = 2+u-1-2u^2 = 1+u+u^2 = u.$$

Daher ist

$$x = u^{-1} = -u = 2u.$$

Aus der ersten Gleichung folgt

$$2y = 1+u-(1+2u)x = 1+u-(1+2u)2u = 1-u-u^2 = 2+2u,$$

also ist $y = 1+u$.

AUFGABE 4. (3 Punkte)

Bestimme in $\mathbb{Q}[X]/(X^3+4X^2-7)$ das Inverse von $\frac{1}{3}x+5$ (x bezeichnet die Restklasse von X).

Lösung

Wir machen Division mit Rest von X^3+4X^2-7 durch $\frac{1}{3}X+5$. Das ergibt

$$X^3+4X^2-7=\left(\frac{1}{3}X+5\right)(3X^2-33X+495)-2482\,.$$

Also ist

$$\left(\frac{1}{3}x+5\right)(3x^2-33x+495)=2482 \mod X^3+4X^2-7$$

und daher ist das Inverse von $\frac{1}{3}X+5$ gegeben durch

$$\frac{1}{2482}(3x^2-33x+495) = \frac{3}{2482}x^2-\frac{33}{2482}x+\frac{495}{2482}.$$

Aufgabe 5. (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 nicht-leere 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 6. (9 (1+1+2+2+3) Punkte)

Wir betrachten die Körpererweiterung

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}, i) = L\,.$$

a) Bestimme den Grad der Körpererweiterung $\mathbb{Q} \subseteq L$.

b) Beschreibe eine möglichst einfache $\mathbb{Q}$-Basis von L.

c) Zeige, dass eine graduierte Körpererweiterung vorliegt. Was ist die graduierende Gruppe?

d) Bestimme die $\mathbb{Q}$-Automorphismen von L.

e) Bestimme das Minimalpolynom von $\sqrt{3} + i$.

Lösung

a) Die Körpererweiterung kann man schreiben als

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt{3}] = M \subseteq M[i] = L\,.$$

Da $\sqrt{3}$ irrational ist, hat die erste Körpererweiterung den Grad 2 und wegen $M \subseteq \mathbb{R}$ ist $i \notin M$, so dass auch die hintere Körpererweiterung den Grad 2 besitzt. Nach der Gradformel liegt insgesamt der Grad 4 vor.

b) Eine $\mathbb{Q}$-Basis ist

$$1, \sqrt{3}, i, \sqrt{3}i\,.$$

Wegen $\sqrt{3}^2, i^2 \in \mathbb{Q}$ ist dies offensichtlich ein Erzeugendensystem, und da es sich um 4 Elemente handelt und der Grad 4 ist, muss es eine Basis sein.

c) Mit der Basis aus Teil (b) können wir

$$L = \mathbb{Q} \cdot 1 \oplus \mathbb{Q} \cdot \sqrt{3} \oplus \mathbb{Q} \cdot i \oplus \mathbb{Q} \cdot \sqrt{3}i$$

schreiben. Sei $D = \mathbb{Z}/(2) \times \mathbb{Z}/(2)$. Die Festlegungen $L_{(0,0)} = \mathbb{Q} \cdot 1$, $L_{(1,0)} = \mathbb{Q} \cdot \sqrt{3}$, $L_{(0,1)} = \mathbb{Q} \cdot i$ und $L_{(1,1)} = \mathbb{Q} \cdot \sqrt{3}i$ liefern eine durch D indizierte Summenzerlegung von L. Die Eigenschaft $L_d \cdot L_e \subseteq L_{d+e}$ folgt unmittelbar aus Eigenschaften der gewählten Basiselemente.

d) Da eine graduierte Körpererweiterung vorliegt, liefern die Charaktere die vier Automorphismen id,

$$a + b\sqrt{3} + ci + d\sqrt{3}i \longmapsto a - b\sqrt{3} + ci - d\sqrt{3}i\,,$$

$$a + b\sqrt{3} + ci + d\sqrt{3}i \longmapsto a + b\sqrt{3} - ci - d\sqrt{3}i$$

und

$$a + b\sqrt{3} + ci + d\sqrt{3}i \longmapsto a - b\sqrt{3} - ci + d\sqrt{3}i\,.$$

Mehr Automorphismen kann es aufgrund von Satz 13.5 nicht geben.

e) Wir berechnen

$$(\sqrt{3}+i)^2 \;=\; 2+2\sqrt{3}i,$$

$$(\sqrt{3}+i)^3 \;=\; (2+2\sqrt{3}i)(\sqrt{3}+i) \;=\; 2\sqrt{3}+2i+6i-2\sqrt{3} \;=\; 8i$$

und

$$(\sqrt{3}+i)^4 \;=\; (2+2\sqrt{3}i)^2 \;=\; 4-12+8\sqrt{3}i \;=\; -8+8\sqrt{3}i.$$

Daraus folgt einerseits, dass $\sqrt{3}+i$ ein erzeugendes Element der Körpererweiterung sein muss und dass das Minimalpolynom den Grad 4 hat. Andererseits sieht man aus diesen Rechnungen direkt

$$(\sqrt{3}+i)^4 - 4(\sqrt{3}+i)^2 \;=\; -16$$

und somit ist

$$X^4 - 4X^2 + 16$$

das Minimalpolynom von $\sqrt{3}+i$.

Aufgabe 7. (3 Punkte)

Bestimme die Matrix des Frobenius-Homomorphismus

$$\Phi : \mathbb{F}_{49} \longrightarrow \mathbb{F}_{49}$$

bezüglich einer geeigneten $\mathbb{F}_7$-Basis von $\mathbb{F}_{49}$.

Lösung

Wegen $1^2 = (-1)^2 = 1$, $2^2 = (-2)^2 = 4$ und $3^2 = (-3)^2 = 2$ in $\mathbb{F}_7 = \mathbb{Z}/(7)$ besitzt das Polynom $X^2 + 1$ keine Nullstelle in $\mathbb{F}_7$. Daher ist dieses Polynom irreduzibel und

$$\mathbb{F}_{49} = \mathbb{F}_7[X]/(X^2 + 1)$$

ist eine Darstellung des Körpers mit 49 Elementen. Eine Basis über $\mathbb{F}_7$ wird durch 1 und x gegeben, wobei x die Restklasse von X bezeichne. Unter dem Frobenius-Homomorphismus ist

$$\Phi(1) = 1^7 = 1 \text{ und } \Phi(x) = x^7 = (x^2)^3 x = -x = 6x\,.$$

Bezüglich dieser Basis hat die beschreibende Matrix die Gestalt

$$\begin{pmatrix} 1 & 0 \\ 0 & 6 \end{pmatrix}\,.$$

Aufgabe 8. (6 Punkte)

Sei $\mathbb{F}_q$ ein endlicher Körper der Charakteristik ungleich 2. Zeige unter Verwendung der Isomorphiesätze, dass genau die Hälfte der Elemente aus $\mathbb{F}_q^\times$ ein Quadrat in $\mathbb{F}_q$ ist.

Lösung

Wir betrachten die Abbildung

$$\mathbb{F}_q^\times \longrightarrow \mathbb{F}_q^\times,\, x \longmapsto x^2,$$

der Einheitengruppe in sich. Diese schickt 1 auf 1 und wegen $(xy)^2 = x^2y^2$ handelt es sich um einen Gruppenhomomorphismus. Der Kern dieser Abbildung besteht aus den $x \in \mathbb{F}_q^\times$ mit $x^2 = 1$, also aus den Nullstellen des Polynoms $X^2 - 1$. Dessen Nullstellen sind gerade 1 und -1, weitere Nullstellen kann es nicht geben, da die Anzahl der Nullstellen durch den Grad des Polynoms beschränkt ist. Bei $1 = -1$ wäre $2 = 0$, was aufgrund der Charakteristik ausgeschlossen ist. Also besteht der Kern genau aus zwei Elementen. Nach dem Isomorphiesatz ist das Bild isomorph zum Urbild modulo Kern. Das Bild ist genau die Menge der Quadrate in der Einheitengruppe, und diese ist isomorph zu $\mathbb{F}_q^\times/\{+1, -1\}$. Jede Nebenklasse besitzt daher zwei Elemente und die Anzahl der Nebenklassen ist daher $\frac{q-1}{2}$. Die Hälfte der Einheiten sind also Quadrate.

Aufgabe 9. (7 Punkte)

Es sei $a \in \mathbb{N}$ eine Primzahl. Zeige, dass $\mathbb{Q} \subseteq \mathbb{Q}[\sqrt[3]{a}]$ eine Körpererweiterung ist, die keine Galoiserweiterung ist.

Lösung

Nach dem Lemma von Eisenstein (angewendet mit der Primzahl a) ist das Polynom $X^3 - a$ irreduzibel über $\mathbb{Q}$, und daher ist

$$\mathbb{Q} \subseteq \mathbb{Q}[\sqrt[3]{a}] = \mathbb{Q}[X]/(X^3 - a) = L$$

eine Körpererweiterung vom Grad 3. Wir zeigen, dass diese Körpererweiterung nicht normal ist, woraus nach Satz 15.6 folgt, dass sie keine Galoiserweiterung ist. Nehmen wir an, dass $\mathbb{Q} \subseteq L$ normal ist. Das Polynom $X^3 - a$ besitzt in L die Restklasse x von X als Nullstelle. Wegen der Normalität muss das Polynom über L vollständig in Linearfaktoren zerfallen, d.h. die anderen Nullstellen (aus $\mathbb{C}$) des Polynoms müssen ebenfalls zu L gehören. Die anderen Nullstellen sind $\zeta \cdot x$ mit einer dritten Einheitswurzel $\zeta \neq 1$. Aus $x, \zeta \cdot x \in L$ folgt aber sofort, dass $\zeta \in L$ ist, d.h. L enthält die dritten Einheitswurzeln. Die dritten Einheitswurzeln erzeugen eine Körpererweiterung K_3 vom Grad 2 über $\mathbb{Q}$. Daher widerspricht die Inklusion $\mathbb{Q} \subseteq K_3 \subseteq L$ der Gradformel.

Aufgabe 10. (5 Punkte)

Bestimme das Kreisteilungspolynom Φ_{15}.

Lösung

Es ist

$$\begin{aligned} X^{15}-1 &= \Phi_1 \cdot \Phi_3 \cdot \Phi_5 \cdot \Phi_{15} \\ &= (X-1)\cdot(X^2+X+1)\cdot(X^4+X^3+X^2+X+1)\cdot\Phi_{15} \\ &= (X^5-1)\cdot(X^2+X+1)\cdot\Phi_{15}. \end{aligned}$$

Wir führen zuerst die Polynomdivision $X^{15}-1$ durch X^5-1 durch, dies ergibt den Quotienten $X^{10}+X^5+1$. Eine weitere Polynomdivision ergibt

$$X^{10}+X^5+1 = (X^2+X+1)\cdot(X^8-X^7+X^5-X^4+X^3-X+1)\,.$$

Somit ist

$$\Phi_{15} = X^8-X^7+X^5-X^4+X^3-X+1\,.$$

Aufgabe 11. (4 Punkte)

Wie viele Unterkörper besitzt der Kreisteilungskörper K_{13}?

Lösung

Jeder Unterkörper von K_{13} enthält $\mathbb{Q}$, daher ist jeder Unterkörper ein Zwischenkörper der Körpererweiterung $\mathbb{Q} \subseteq K_{13}$. Dies ist eine Galoiserweiterung nach Satz 19.1 und die Galoisgruppe ist isomorph zu $\mathbb{Z}/(12)$. Über die Galoiskorrespondenz stehen die Unterkörper in Bijektion zu den Untergruppen von $\mathbb{Z}/(12)$. Die Untergruppen entsprechen eindeutig den Teilern von 12, daher gibt es 6 Untergruppen und 6 Unterkörper des dreizehnten Kreisteilungskörpers.

Aufgabe 12. (7 Punkte)

Es sei G eine auflösbare Gruppe und $H \subseteq G$ eine Untergruppe. Zeige, dass auch H auflösbar ist.

Lösung

Wir gehen von einer auflösenden Filtrierung

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

aus, d.h., dass die G_i Normalteiler in G_{i+1} und die Restklassengruppen G_{i+1}/G_i kommutativ sind. Die Untergruppe $H \subseteq G$ besitzt durch $H_i = H \cap G_i$ eine induzierte Filtrierung. Dabei liegt das kommutative Diagramm

$$\begin{array}{ccc} H \cap G_i & \longrightarrow & H \cap G_{i+1} \\ \downarrow & & \downarrow \\ G_i & \longrightarrow & G_{i+1} \end{array}$$

vor. Wir betrachten den Homomorphismus

$$f : H \cap G_{i+1} \longrightarrow G_{i+1}/G_i.$$

Der Kern von f ist offenbar $H \cap G_i$. Daher ist H_i nach Lemma 5.6 ein Normalteiler in H_{i+1}, und der Quotient H_{i+1}/H_i ist nach Satz 5.12 eine Untergruppe von G_{i+1}/G_i und damit kommutativ. Also bilden die H_i eine auflösende Filtrierung von H.

Aufgabe 13. (3 Punkte)

Beschreibe die wesentlichen mathematischen Schritte, mit denen man beweisen kann, dass die „Quadratur des Kreises“ nicht möglich ist.

Lösung

Das Problem der Quadratur des Kreises bedeutet die Fragestellung, ob man aus einem durch den Radius gegebenen Kreis ein flächengleiches Quadrat mit Hilfe von Zirkel und Lineal konstruieren kann. Den Radius kann man dabei zu 1 normieren und durch zwei Punkte 0 und 1 repräsentieren. Da der Kreisinhalt π ist, muss die Seitenlänge des zu konstruierenden Quadrates $\sqrt{\pi}$ sein. Damit ist die Frage äquivalent dazu, ob man aus zwei Punkten mit Abstand 1 mittels Zirkel und Lineal den Abstand $\sqrt{\pi}$ konstruieren kann.

Der entscheidende Schritt ist, die Menge aller aus 0 und 1 konstruierbaren Punkte in der Ebene mathematisch zu erfassen. Dabei ergibt sich, dass bei jedem elementaren Schritt (wie dem Durchschnitt von einem Kreis und einer Geraden) der neue Punkt in einer quadratischen Körpererweiterung der schon konstruierten Punkte liegt. Daraus ergibt sich induktiv, dass jeder konstruierbare Punkt eine algebraische Zahl ist. Der Satz von Lindemann besagt allerdings, dass π und damit auch $\sqrt{\pi}$ keine algebraische Zahl ist, und damit auch nicht konstruierbar.