Algebra (V4, Ü 2)
Wintersemester 1997/98
Universität Stuttgart

Auf den nächsten Seiten finden Sie die Übungsblätter zur Vorlesung.

Dozent:	Prof. Dr. **Jörg Brüdern**
Übungen:	Dipl. Math. **Rainer Dietmann** und
	Dipl. Math. **Christian Elsholtz**.
Zielgruppe	Studenten ab dem 5. Semester

Die Vorlesungen wurde von etwa 50-60 Studenten im Hauptstudium besucht. Etwa die Hälfte von ihnen gab regelmäßig Übungsaufgaben ab und erwarb einen Übungsschein. Die Aufgaben wurden von den Studenten als schwer eingestuft. Auf den Aufgabenblättern sind die Aufgaben in etwa nach dem (vermuteten) Schwierigkeitsgrad sortiert, d.h. Aufgaben 1 und 2 sind eher leicht, Aufgaben 4 und besonders 5 sind eher schwer.

Blatt 1
16.10.1997

Algebra

WS 1997/98
Prof. Brüdern
Dipl. Math. Dietmann
Dipl. Math. Elsholtz

Aufgabe 1. Man bestimme (bis auf Isomorphie) alle Gruppen mit höchstens 5 Elementen.

Aufgabe 2.
(a) Sei G eine endliche abelsche Gruppe mit neutralem Element e. Man zeige:

$$\prod_{x \in G} x^2 = e \ .$$

(b) Gegeben sei eine Gruppe G mit folgender Eigenschaft: Für alle $x \in G$ gilt $x^2 = e$, wobei e das neutrale Element in G bezeichne. Man zeige: G ist abelsch.

Aufgabe 3. Man gebe eine vollständige Liste aller Untergruppen der symmetrischen Gruppe S_3 an. Welche davon sind Normalteiler?

Aufgabe 4. Man beweise den *dritten Isomorphiesatz:*
Sei G eine Gruppe. Ferner seien A_1, A, B_1 und B Untergruppen von G mit $A_1 \lhd A$ und $B_1 \lhd B$. Dann gilt:

(i) $A_1(A \cap B_1) \lhd A_1(A \cap B)$

(ii) $B_1(A_1 \cap B) \lhd B_1(A \cap B)$

(iii) $A_1(A \cap B)/A_1(A \cap B_1) \cong B_1(A \cap B)/B_1(A_1 \cap B)$

Aufgabe 5. Man zeige für $n \geq 3$, daß die alternierende Gruppe A_n von den Zyklen $(1,2,3), (1,2,4), \ldots, (1,2,n)$ erzeugt wird. Hieraus folgere man, daß ein Normalteiler $N \lhd A_n$, welcher einen 3-Zyklus enthält, bereits mit A_n übereinstimmt.

Abgabe der Lösungen: Donnerstag, den 23. Oktober nach der Vorlesung.

Die ersten Übungen finden am Montag, den 27. Oktober bzw. am Dienstag, den 28. Oktober jeweils um 15.45 Uhr in Raum 8.141 statt.

Blatt 2
23.10.1997

Algebra

WS 1997/98
Prof. Brüdern
Dipl. Math. Dietmann
Dipl. Math. Elsholtz

Aufgabe 1
Gibt es p-Gruppen mit unendlich vielen Elementen? (Begründung !)

Aufgabe 2
Es sei G eine Gruppe und X die Menge aller Untergruppen von G. Man zeige:

(i) $G \times X \longrightarrow X$, $(g, H) \mapsto gHg^{-1}$, definiert eine Operation von G auf X.

(ii) Die Bahn eines Elements $H \in X$ besteht genau dann nur aus H, wenn H ein Normalteiler von G ist.

(iii) Ist die Ordnung von G Potenz einer Primzahl p, so unterscheidet sich die Anzahl der Untergruppen von G von der Anzahl der Normalteiler von G um ein Vielfaches von p.

Aufgabe 3
Es sei G eine endliche Gruppe und $H \subset G$ eine p-Untergruppe für eine Primzahl p. Man zeige: Ist H ein Normalteiler in G, so ist H in jeder p-Sylow-Gruppe von G enthalten.

Aufgabe 4
(a) Sei $\sigma = (x_1, \ldots, x_r) \in S_n$ ein r-Zykel. Für beliebiges $\tau \in S_n$ zeige

$$\tau\sigma\tau^{-1} = (\tau(x_1), \ldots, \tau(x_r)).$$

(b) Die „Kleinsche Vierergruppe“ V_4 ist gegeben als Untergruppe der S_4, bestehend aus den Permutationen

$$\mathrm{id},\ (1,2)(3,4),\ (1,3)(2,4),\ (1,4)(2,3).$$

Man zeige $V_4 \lhd S_4$.

Aufgabe 5
Sei G eine endliche Gruppe mit $n = \#G$. Sei p prim mit $p^r \,||\, \#G$. Man zeige:

$$(a)\ \#\mathrm{Syl}_p(G) \,|\, \frac{n}{p^r},\ \ (b)\ p \,|\, (\#\mathrm{Syl}_p(G) - 1).$$

Hinweis: Für (a) betrachte man die durch $(g, H) \mapsto gHg^{-1}$ auf $\mathrm{Syl}_p(G)$ definierte Operation von G. Für ein $H \in \mathrm{Syl}_p(G)$ betrachte man $\mathrm{Stab}(H)$ unter dieser Operation. Warum gilt $p^r \,|\, \mathrm{Stab}(H)$? Man wende nun die Bahnengleichung an. Für (b) verwende man die Operation einer festen p-Sylow-Gruppe H auf $\mathrm{Syl}_p(G)$, gegeben durch $(h, P) \mapsto hPh^{-1}$ für $h \in H, P \in \mathrm{Syl}_p(G)$. Anschließend zeige man, daß es genau eine Bahn der Länge 1 gibt und schließe dann mit der Bahnengleichung.

Abgabe der Lösungen: Donnerstag, den 30. Oktober nach der Vorlesung.

Blatt 3 30.10.1997	ALGEBRA	WS 1997/98 Prof. Brüdern Dipl. Math. Dietmann Dipl. Math. Elsholtz

Aufgabe 1

(i) Man zeige, daß $\mathbb{Z}[\sqrt{-5}] := \{a + b\sqrt{-5} \mid a, b \in \mathbb{Z}\}$ ein Ring ist.

(ii) Man zeige, daß es in diesem Ring Elemente gibt, die zwar unzerlegbar, aber nicht prim sind. Ist hier die Zerlegung in „unzerlegbare Elemente“ eindeutig?

Aufgabe 2

Wir untersuchen den Ring der ganzen GAUSSschen Zahlen:
$\mathbb{Z}[i] := \{a + bi \mid a, b \in \mathbb{Z}, i^2 = -1\}$.

(i) Man bestimme die Einheitengruppe von $\mathbb{Z}[i]$.

(ii) Man beweise, daß dieser Ring mit der Norm $N(a+bi) = a^2 + b^2$ euklidisch ist. Ist $\mathbb{Z}[i]$ faktoriell ?

(iii) Sei $p \in \mathbb{N}$ eine Primzahl. Man zeige:

$$p \text{ ist prim in } \mathbb{Z}[i] \quad \Leftrightarrow \quad \begin{array}{l} p \text{ kann nicht in der Form} \\ p = a^2 + b^2, a, b \in \mathbb{Z} \text{ geschrieben werden.} \end{array}$$

(iv) Man zerlege 210 in Primelemente aus $\mathbb{Z}[i]$.

(v) Der Quotientenkörper von $\mathbb{Z}[i]$ ist isomorph zu $\mathbb{Q}[i] := \{a + bi \mid a, b \in \mathbb{Q}\}$.

Aufgabe 3

Sei I ein Integritätsbereich mit endlich vielen Elementen. Man beweise, daß I dann sogar ein Körper ist.

Aufgabe 4

Zeige, daß alle ganzzahligen Lösungen der Gleichung

$$x^2 + y^2 = z^2 \tag{1}$$

mit $x, y, z > 0$ und $\mathrm{ggT}(x, y, z) = 1$ („Pythagoräische Tripel“) durch

$$x = u^2 - v^2, \quad y = 2uv, \quad z = u^2 + v^2$$

gegeben sind, mit $u, v \in \mathbb{N}, u > v$, u und v teilerfremd und nicht beide ungerade, und durch die Tripel, die man hieraus durch Vertauschung von x und y erhält.
Hinweis: Man zerlege die linke Seite von (1) in ein Produkt und zeige unter Ausnutzung der eindeutigen Primfaktorzerlegung in $\mathbb{Z}[i]$, daß $x + iy = \epsilon\alpha^2$ für eine Einheit $\epsilon \in \mathbb{Z}[i]$ und ein $\alpha \in \mathbb{Z}[i]$ gelten muß.

Aufgabe 5

Man bestimme alle ganzzahligen Lösungen der Gleichung

$$x^3 + y^3 = 3z^3.$$

Abgabe der Lösungen: Donnerstag, den 6. November nach der Vorlesung.

Blatt 4
6.11.1997

Algebra

WS 1997/98
Prof. Brüdern
Dipl. Math. Dietmann
Dipl. Math. Elsholtz

Aufgabe 1
(a) Man bestimme alle Ringhomomorphismen $\varphi : \mathbb{Z} \to \mathbb{Z}$ und alle Ringhomomorphismen $\varphi : \mathbb{Q} \to \mathbb{Q}$.
(b) Sei n eine natürliche Zahl. Man zeige, daß $\mathbb{Z}/n\mathbb{Z}$ genau dann ein Körper ist, wenn n eine Primzahl ist.

Aufgabe 2
Sei I_1 das im Ring $\mathbb{Z}[i]$ von 2 und $i-1$ erzeugte Ideal und I_2 das von $1+3i$ und $3+7i$ erzeugte Ideal. Man zeige $I_1 = I_2$, begründe, daß es sich um ein Hauptideal handelt und finde einen Erzeuger.

Aufgabe 3
Ein Ring R heißt einfach, wenn R außer $\{0\}$ und R keine weiteren Ideale enthält. Man zeige:
(a) Schiefkörper sind einfache Ringe.
(b) Kommutative einfache Ringe sind Körper.
(c) Ist die Voraussetzung „kommutativ“ notwendig, um in (b) wenigstens einen Schiefkörper zu erhalten?
Hinweis für (c): Man denke an Matrizenringe.

Aufgabe 4 (Sehr leicht)
Es seien I und J Ideale eines Ringes R, mit

$$I + J = \{i + j | i \in I \text{ und } j \in J\} = R.$$

Man zeige, daß es für alle $a, b \in R$ ein $x \in R$ gibt, so daß gilt:

$$\begin{aligned} x &\equiv a \bmod I \\ x &\equiv b \bmod J. \end{aligned}$$

Aufgabe 5
Sei R ein faktorieller Ring. Man zeige:
(a) Jedes Element $x \in R\backslash\{0\}$ ist nur in endlich vielen Hauptidealen enthalten.
(b) Jede aufsteigende Folge $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots \subseteq R$ von Hauptidealen I_i in R wird stationär, d.h. es gibt ein $n \in \mathbb{N}$ mit $I_i = I_n$ für alle $i \geq n$.
Hinweis: In der Vorlesung wurde gezeigt, daß in Integritätsringen Erzeuger von Hauptidealen bis auf Multiplikation mit Einheiten eindeutig sind.

Abgabe der Lösungen: Donnerstag, den 13. November nach der Vorlesung.

Blatt 5
13.11.1997

Algebra

WS 1997/98
Prof. Brüdern
Dipl. Math. Dietmann
Dipl. Math. Elsholtz

Aufgabe 1
Man zerlege die folgenden Polynome in irreduzible Faktoren, oder beweise, daß das betreffende Polynom bereits irreduzibel ist.
(a) $X^2 + 5X + 1$ in $\mathbb{Z}[X]$,
(b) $X^2 + 1$ in $(\mathbb{Z}/5\mathbb{Z})[X]$ und $(\mathbb{Z}/7\mathbb{Z})[X]$,
(c) $X^5 - kX + 1$ ($k \in \mathbb{Z}$ ein Parameter) in $\mathbb{Q}[X]$,
(d) $X^3 - 3$ in $K[X]$ mit $K = \{a + b\sqrt{2} \,:\, a, b \in \mathbb{Q}\}$,
(e) $X^2 + Y^2 - 1$ in $\mathbb{C}[X, Y]$,
(f) $X^4 + 4Y^4$ in $\mathbb{Z}[i][X, Y]$ und in $\mathbb{Z}[X, Y]$.
Hinweis: Es reicht die Angabe der wesentlichen Zwischenschritte!

Aufgabe 2
(a) Sei R ein Hauptidealring und $x, y \in R\backslash\{0\}$. Man zeige: $\mathrm{GGT}(x, y)$ existiert und läßt sich in der Form

$$\mathrm{GGT}(x, y) = ax + by$$

für geeignete $a, b \in R$ darstellen.
(b) Man betrachte die beiden Polynome $f(X) = X^5 + X^4 + X^3 + X^2 + X + 1$ und $g(X) = X^4 + X^3 + X + 1$ in $(\mathbb{Z}/2\mathbb{Z})[X]$, bestimme ihren GGT und drücke diesen als Linearkombination von f und g aus.

Aufgabe 3
Man zeige: Zwei verschiedene Polynome $f, g \in \mathbb{Q}[X]$ mit ganzzahligen Koeffizienten sind in $\mathbb{Z}[X]$ genau dann teilerfremd, wenn das von ihnen erzeugte Ideal (f, g) eine ganze Zahl $z \neq 0$ enthält.

Aufgabe 4
Sei R ein Integritätsbereich. Man zeige: $R[X]$ ist genau dann ein Hauptidealring, wenn R ein Körper ist (siehe Satz 6 der Vorlesung). (Die Voraussetzung, sei R ein Integritätsbereich, wird gar nicht benötigt.)

Aufgabe 5
(a) Man zeige: Ein kommutativer Ring R ist genau dann noethersch, wenn jedes Ideal I in R endlich erzeugt ist, d.h. von einer Teilmenge $X \subset R$ mit $\#X < \infty$ erzeugt wird.
(b) Man beweise mit Hilfe von (a) den Hilbertschen Basissatz: Ist R ein kommutativer noetherscher Ring, so ist auch der Polynomring $R[X]$ noethersch.
Möglicher Lösungsweg für (b): Ist I ein beliebiges Ideal in $R[X]$, so sei

$$J_n = \{r \in R \,:\, \text{es gibt ein } f \in I \text{ mit } \deg f = n \text{ und höchstem Koeffizient } r\}.$$

Die Kette $J_1 \subset J_2 \subset \ldots \subset R$ wird für einen Index m stationär (warum ?). Seien $r_{n1}, \ldots, r_{ns_n}$ Erzeuger für J_n (warum gibt es diese?). Man finde nun eine endliche Menge $F \subset R[X]$ mit $(F) = I$. Zum Nachweis von $(F) = I$ verwende man Induktion nach dem Grad der Polynome in I.

Abgabe der Lösungen: Donnerstag, den 20. November nach der Vorlesung.

Blatt 6
20.11.1997

Algebra

WS 1997/98
Prof. Brüdern
Dipl. Math. Dietmann
Dipl. Math. Elsholtz

Aufgabe 1
Man untersuche folgende Polynome in $\mathbb{Q}[X]$ auf Irreduzibilität:

(a) $f(X) = \frac{2}{15}X^5 + \frac{4}{5}X^4 - X^3 + \frac{6}{5}X^2 - 3X + \frac{1}{5}$

(b) $f(X) = X^3 + 2X^2 + 4X + 4$

(c) $f(X) = X^3 + 2X^2 + 2X + 4$

(d) $f(x) = 4X^3 + 4X^2 + 2X + 1$

(e) $f(X) = X^4 + 6X^3 + 12X^2 + 12X + 7$

(f) $f(X) = X^4 + 6X^3 + 12X^2 + 12X + 5$

(g) $f(X) = X^4 + 15X^3 + 7$

(h) $f(X) = 2X^4 + 11X^3 + 20X^2 + 14X + 3$

(i) $f(X) = X^{500} + X^{375} + X^{250} + X^{125} + 1$

Aufgabe 2 (Eisenstein rückwärts)

(a) Man beweise: Sei $f \in \mathbb{Z}[X]$ mit $f(x) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_1X + a_0$. Sei $p \nmid a_0, p|a_1, \ldots, p|a_n$ aber $p^2 \nmid a_n$, dann ist f irreduzibel über $\mathbb{Q}[X]$.

(b) Man beweise oder widerlege: Sei $f \in \mathbb{Z}[x]$. Wenn es keine Primzahl p gibt, so daß die Koeffizienten von f die Eisensteinbedingungen für p erfüllen, dann ist f reduzibel.

Aufgabe 3
Sei p eine Primzahl. Man bestimme die Anzahl der irreduziblen Polynome vom Grad 2 und Grad 3 in $(\mathbb{Z}/p\mathbb{Z})[X]$.

Aufgabe 4 (Satz von Newton)
Seien $s_1, \ldots, s_n$ die elementarsymmetrischen Polynome in den Variablen $X_1, \ldots, X_n$. Man zeige: $R[X_1, \ldots, X_n] \cong R[s_1, \ldots, s_n]$; dabei ist $R[s_1, \ldots, s_n]$ der kleinste Ring, der R und $s_1, \ldots, s_n$ enthält.

Aufgabe 5
Sei R ein kommutativer Ring. Man zeige: Die Diskriminante eines kubischen Polynoms der Bauart $f(X) = X^3 + aX + b \in R[X]$ ist durch $\Delta_f = -4a^3 - 27b^2$ gegeben.

Abgabe der Lösungen: Donnerstag, den 27. November nach der Vorlesung.

Blatt 7
27.11.1997

Algebra

WS 1997/98
Prof. Brüdern
Dipl. Math. Dietmann
Dipl. Math. Elsholtz

Aufgabe 1
Sei K ein Körper und $n \in \mathbb{N}$. Man zeige: Die Determinante

$$\Delta(X_{11}, \ldots, X_{nn}) = \begin{vmatrix} X_{11} & \cdots & X_{1n} \\ \vdots & & \vdots \\ X_{n1} & \cdots & X_{nn} \end{vmatrix}$$

ist irreduzibel in $K[X_{11}, \ldots, X_{nn}]$.

Aufgabe 2
Seien a und b teilerfremde natürliche Zahlen und $x, y \in \mathbb{C}$ mit $x^a = 2$, $y^b = 3$. Man zeige $\mathbb{Q}(x, y) = \mathbb{Q}(x \cdot y)$ und bestimme das Minimalpolynom von $x \cdot y$ über $\mathbb{Q}$.

Aufgabe 3
Sei L/K eine endliche Körpererweiterung, so daß der Grad $[L : K]$ prim ist. Man zeige, daß dann ein $\alpha \in L$ mit $L = K(\alpha)$ existiert.

Aufgabe 4
Man betrachte

$$A = \{a \in \mathbb{R} : a \text{ ist algebraisch über } \mathbb{Q}\}.$$

Es ist zu zeigen: A ist eine algebraische Erweiterung von $\mathbb{Q}$ und es gilt $[A : \mathbb{Q}] = \infty$. Ist A abzählbar? Gibt es $\alpha \in \mathbb{R}$, die transzendent über $\mathbb{Q}$ sind? Man zeige: Jedes $\alpha \in \mathbb{R} \backslash A$ ist transzendent über A.

Aufgabe 5
Sei L/K eine Körpererweiterung, $a \in L$ algebraisch mit $r = \deg(a)$ und n eine beliebige natürliche Zahl. Man versuche, eine Formel für $[K(a^n) : K]$ anzugeben, die nur von r und n abhängt.

Aufgabe 6
(a) Sei L/K eine Körpererweiterung, und seien $\alpha, \beta \in L$, so daß $\alpha + \beta$ und $\alpha \cdot \beta$ algebraisch über K sind. Man zeige: Dann sind auch α und β algebraisch über K.
(b) Sei L/K eine Körpererweiterung, $n \in \mathbb{N}$ und $\alpha_1, \ldots, \alpha_n \in L$, so daß $\sigma_1(\alpha_1, \ldots, \alpha_n)$, $\ldots, \sigma_n(\alpha_1, \ldots, \alpha_n)$ algebraisch über K sind. Dabei sind σ_i $(1 \leq i \leq n)$ die elementarsymmetrischen Funktionen in n Variablen. Man zeige: Unter diesen Voraussetzungen sind auch $\alpha_1, \ldots, \alpha_n$ algebraisch über K.

Abgabe der Lösungen: Donnerstag, den 4. Dezember nach der Vorlesung.

Algebra

WS 1997/98
Prof. Brüdern
Dipl. Math. Dietmann
Dipl. Math. Elsholtz

Aufgabe 1
Man gebe die Kreisteilungspolynome $\Phi_n \in \mathbb{Z}[x]$ für $1 \leq n \leq 20$ explizit an.

Aufgabe 2
Sei L/K eine Körpererweiterung und $f \in L[X]$ ein Polynom mit $\deg f < \#K$.
Man zeige: Ist $f(a) \in K$ für alle $a \in K$, so ist $f \in K[X]$.

Aufgabe 3
Sei K Körper, $p \in K[X]$ irreduzibel und $F = K[X]/(p)$. Weiter sei L/K eine Körpererweiterung. Man zeige:

(i) Die Anzahl der K-Einbettungen von F in L ist höchstens $\deg p$.

(ii) Seien $a, b \in L$ mit $p(a) = p(b) = 0$. Dann gibt es einen Isomorphismus $\varphi : K(a) \to K(b)$ mit $\varphi \mid K = id$.

Aufgabe 4

(i) Sei $\mathrm{ggT}(r, p^n - 1) = 1$. Dann gibt es zu jedem $a \in \mathbb{F}_{p^n}$ ein $x \in \mathbb{F}_{p^n}$ mit $x^r = a$.

(ii) Gelte $r | p^n - 1$. Dann gilt $\#\{a^r : a \in \mathbb{F}_{p^n}\} = 1 + \dfrac{p^n - 1}{r}$.

(iii) Sei F ein endlicher Körper. Zu jedem $a \in F$ gibt es $x, y \in F$ mit $a = x^2 + y^2$.

Aufgabe 5
Man zeige: $\mu_n^*(\mathbb{Q})$ ist genau dann eine Basis von $\mathbb{Q}(\mu_n)/\mathbb{Q}$, wenn n quadratfrei ist.
(Eine Zahl n heißt quadratfrei, wenn für alle Primzahlen p gilt: $p^2 \nmid n$.)

Nikolaus

Die erste korrekte Lösung der folgenden Aufgabe wird mit einem Nikolaus belohnt!

Aufgabe 6
Sei R ein Integritätsbereich, der nicht nur aus 0 und den Einheiten besteht. Untersuche folgende Argumentation:
„Angenommen, R enthalte nur endlich viele irreduzible Elemente, z.B. $p_1, \ldots, p_r$. Dann muß $1 + (p_1 p_2 \ldots p_r)$ einen irreduziblen Faktor q haben. Dieser kann aber mit keinem der $p_1, \ldots, p_r$ übereinstimmen. Also gibt es stets unendlich viele irreduzible Elemente.“

(a) Ist diese Argumentation korrekt?

(b) Wenn nicht, ist zumindest die Aussage korrekt, daß R stets unendlich viele irreduzible Elemente enthält?

Abgabe der Lösungen: Donnerstag, den 11. Dezember nach der Vorlesung. Lösungen der Nikolaus-aufgabe können jederzeit (mit Datum und Uhrzeit versehen) abgegeben werden. Bei mehreren korrekten Lösungen entscheidet der Zeitpunkt der Abgabe.

ALGEBRA

WS 1997/98
Prof. Brüdern
Dipl. Math. Dietmann
Dipl. Math. Elsholtz

Aufgabe 1
Man konstruiere einen Zerfällungskörper von $X^4 - 2$ über $\mathbb{Q}$ und gebe seinen Grad und ein primitives Element an.

Aufgabe 2
Seien $p_1, \dots, p_n$ verschiedene Primzahlen aus $\mathbb{N}$. Man zeige

$$[\mathbb{Q}(\sqrt{p_1}, \dots, \sqrt{p_n}) : \mathbb{Q}] = 2^n$$

und folgere

$$[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty;$$

dabei bezeichnet $\overline{\mathbb{Q}}$ den algebraischen Abschluß von $\mathbb{Q}$.

Aufgabe 3
In dieser Aufgabe soll gezeigt werden, daß eine algebraische Körpererweiterung L/K genau dann einfach ist, wenn sie nur endlich viele Zwischenkörper enthält. Man beweise diese Aussage in folgenden Schritten:

(i) Man diskutiere zuerst den Fall $\#K < \infty$. Im folgenden kann dann $\#K = \infty$ angenommen werden.

(ii) Sei $L = K(\alpha)$ und $f \in K[X]$ das Minimalpolynom von α über K. Die Menge der Zwischenkörper von L/K läßt sich identifizieren mit einer Teilmenge der Teiler von f, aufgefaßt als Polynom in $L[X]$.

(iii) Es möge L/K nur endlich viele Zwischenkörper zulassen. Um zu zeigen, daß L/K einfach ist, reduziere man auf den Fall, wo L über K von zwei Elementen erzeugt wird. Für $L = K(\alpha, \beta)$ schließlich betrachte man zu Konstanten $c \in K$ die Körper $K(\alpha + c\beta)$.

Aufgabe 4
Sei p prim und $L = \mathbb{F}_p(X, Y) := \mathbb{F}_p(X)(Y)$. Man zeige:

(i) $\sigma : L \to L$; $a \mapsto a^p$ ist ein Körperhomomorphismus.

(ii) Gilt $K = \sigma(L)$, so ist die Körpererweiterung L/K weder einfach noch separabel.

Aufgabe 5
Man konstruiere einen algebraischen Abschluß für einen endlichen Körper $\mathbb{F}_p$.
Anleitung: Zunächst zeige man, daß ein irreduzibles $f \in \mathbb{F}_p[X]$ ein Teiler von $X^{p^r} - X$ ist, falls $\deg f \mid r$ gilt. Weiterhin gebe man dem Ausdruck $\bigcup_{n=1}^{\infty} \mathbb{F}_{p^{n!}}$ einen Sinn und zeige, daß dies ein Abschluß für $\mathbb{F}_p$ ist.

Abgabe der Lösungen: Donnerstag, den 18. Dezember nach der Vorlesung.

ALGEBRA

WS 1997/98
Prof. Brüdern
Dipl. Math. Dietmann
Dipl. Math. Elsholtz

Aufgabe 1
Sei $\alpha \in \mathbb{C}$ algebraisch über $\mathbb{Q}$. Man zeige: α ist genau dann separabel, wenn die Anzahl der verschiedenen $\mathbb{Q}$-Einbettungen von $\mathbb{Q}(\alpha)$ nach $\mathbb{C}$ gleich $|\mathbb{Q}(\alpha) : \mathbb{Q}|$ ist.

Aufgabe 2
Es seien K/L und L/M jeweils normale Körpererweiterungen. Folgt dann, daß auch K/M normal sein muß?

Aufgabe 3
Es sei $f = X^4 - 2$.

(i) Man gebe den Zerfällungskörper L von f über $\mathbb{Q}$ an.

(ii) Man bestimme die Automorphismen von L und berechne die Galois-Gruppe $G = Gal\, L/\mathbb{Q}$.

(iii) Man gebe alle Untergruppen der Galois-Gruppe G und alle Unterkörper des Zerfällungskörpers L in einem Diagramm an.

(iv) Welche der Untergruppen sind Normalteiler von G und welche Zwischenkörper sind normal über Q?

Aufgabe 4
Sei $\zeta_n = e^{\frac{2\pi i}{n}}$ für $n \in \mathbb{N}$. Man beweise, daß $\mathbb{Q}(\zeta_n) \cap \mathbb{R} = \mathbb{Q}(\zeta_n + \overline{\zeta_n})$ und bestimme $[\mathbb{Q}(\zeta_n + \overline{\zeta_n}) : \mathbb{Q}]$.

Aufgabe 5
Sei L/F eine endliche, normale und separable Körpererweiterung. Sei F_i der Zwischenkörper, der nach dem Hauptsatz der Galois-Theorie mit der Untergruppe G_i der Galois-Gruppe $Gal\, L/F$ korrespondiert. Man beweise: Zum Durchschnitt zweier Untergruppen $G_1 \cap G_2$ korrespondiert der von F_1 und F_2 erzeugte Vereinigungskörper: $< F_1 \cup F_2 >$. Umgekehrt korrespondiert der Schnittkörper $F_1 \cap F_2$ zu der von G_1 und G_2 erzeugten Vereinigungsgruppe.

Aufgabe 6
Sei M/K eine endliche, normale und separable Körpererweiterung. Sei $Gal\, M/K$ die zyklische Gruppe der Ordnung n. Dann gibt es zu jedem Teiler d von n genau einen Zwischenkörper L mit $[L : K] = d$. Ein Zwischenkörper L_1 vom Grad d_1 (über K) ist genau dann in einem Zwischenkörper L_2 vom Grad d_2 enthalten, wenn $d_1 \mid d_2$ gilt.

Abgabe der Lösungen: Donnerstag, den 8. Januar 1998 nach der Vorlesung.

Fröhliche Weihnachten und ein gutes neues Jahr 1998 wünschen

Blatt 11
8.1.1998

Algebra

WS 1997/98
Prof. Brüdern
Dipl. Math. Dietmann
Dipl. Math. Elsholtz

Aufgabe 1

(i) Ist die Körpererweiterung $\mathbb{Q}(\sqrt{2+\sqrt{2}})/\mathbb{Q}$ galoissch? Wenn ja, berechne man die Galois-Gruppe der Körpererweiterung.

(ii) Man untersuche analog die Körpererweiterung $\mathbb{Q}\left(\sqrt{1+\sqrt{2}}\right)/\mathbb{Q}$.

Aufgabe 2

Es sei K ein Körper, $f \in K[X]$ ein irreduzibles und separables Polynom. L sei der Zerfällungskörper von f über K. Die Erweiterung L/K ist also galoissch. Man zeige: Ist $Gal(L/K)$ abelsch, so gilt $L = K(\alpha)$ für jede Nullstelle $\alpha \in L$ von f.

Aufgabe 3

(i) Man berechne die Galois-Gruppen $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ bzw. $Gal(\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})/\mathbb{Q})$ und gebe alle Untergruppen bzw. alle Zwischenkörper an. Weiterhin stelle man die Beziehungen der Untergruppen bzw. Zwischenkörper in einem Diagramm dar.

(ii) Seien $p_1, \ldots, p_n$ verschiedene Primzahlen. Man zeige, daß $Gal(\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})/\mathbb{Q})$ eine Gruppe mit 2^n Elementen ist, wobei für jedes Element a gilt: $a^2 = id$. Ist die Galois-Gruppe abelsch? (Es kann Blatt 9, Aufgabe 2 benutzt werden. Es ist aber auch möglich, hier einen (einfacheren) Beweis zu finden.)

Aufgabe 4

Sei L/K galoissch. Sei $f \in K[X]$ irreduzibel und normiert und $g \in L[X]$ irreduzibel und normiert mit $g|f$. Dann ist die Primfaktorzerlegung von f in $L[X]$ das Produkt der Elemente der Bahn $\{\sigma(g) : \sigma \in Gal(L/K)\}$. Insbesondere haben die Primteiler von f in $L[X]$ denselben Grad.

Aufgabe 5

Sei $f = X^5 - 6X + 3 \in \mathbb{Q}[X]$.

- Man zeige: f ist irreduzibel und separabel. Wieviele reelle Nullstellen hat f?
- Sei L der Zerfällungskörper von f über $\mathbb{Q}$. Man zeige $G = Gal(L/\mathbb{Q}) \cong S_5$.

  Ein möglicher Lösungsweg: Um Automorphismen zu finden, betrachte man die Nullstellen von f. Man zeige, daß G eine Transposition und einen 5-Zykel enthält. Man zeige weiter, daß eine Transposition und ein 5-Zykel bereits S_5 erzeugen. (Vergleiche auch Blatt 1, Aufgabe 5.)

Abgabe der Lösungen: Donnerstag, den 15. Januar 1998 nach der Vorlesung.

Algebra

WS 1997/98
Prof. Brüdern
Dipl. Math. Dietmann
Dipl. Math. Elsholtz

Aufgabe 1

(i) Man gebe eine explizite Vorschrift an, um das regelmäßige Fünfeck mit Zirkel und Lineal zu konstruieren.

(ii) Sei $p > 2$ prim. Man zeige: Ist das regelmäßige p-Eck mit Zirkel und Lineal konstruierbar, so hat p die Form $p = 2^{2^k} + 1$.

(iii) Man beweise, daß $2^{2^5} + 1$ durch 641 teilbar ist, ohne diese Division explizit auszuführen.

(iv) Man versuche, möglichst viele ungerade n anzugeben, so daß das regelmäßige $n-$Eck mit Zirkel und Lineal konstruierbar ist.

Aufgabe 2

Sei K ein Körper der Charakteristik 0. Weiter sei $a_1, \ldots, a_n$ eine Basis der Galois-Erweiterung $L/K, U$ eine Untergruppe von $\mathrm{Gal}(L/K)$ und $c_i = \mathrm{Sp}_U a_i := \sum_{\sigma \in U} \sigma(a_i)$ $(1 \leq i \leq n)$. Dann ist der zu U gehörende Fixkörper $\Phi(U)$ durch $K(c_1, \ldots, c_n)$ gegeben.

Aufgabe 3

Sei L/K eine Galoiserweiterung und U eine Untergruppe von $\mathrm{Gal}(L/K)$. Man zeige: Es ist genau dann $\Phi(U) = K(c)$, wenn $\sigma(c) = c$ für alle $\sigma \in U$ und $\sigma(c) \neq c$ für alle $\sigma \in \mathrm{Gal}(L/K) \backslash U$ gilt.

Aufgabe 4

Sei p eine Primzahl, $\zeta = e^{2\pi i/p}$, φ ein Erzeuger der zyklischen Gruppe $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ und $\zeta_i := \varphi^i(\zeta)$. Dann gibt es zu jedem Teiler d von $p - 1 = dm$ genau einen Zwischenkörper M des $p-$ten Kreisteilungskörpers $\mathbb{Q}(\zeta)/\mathbb{Q}$ mit $|M : \mathbb{Q}| = m$. Man erhält M durch Adjunktion eines Elementes der Form

$$\eta_i = \sum_{k=0}^{d-1} \zeta_{i+km} \; (0 \leq i \leq m-1) \; ;$$

d.h. $M = \mathbb{Q}(\eta_0) = \ldots = \mathbb{Q}(\eta_{m-1})$. Auf diese Weise erhält man eine vollständige Übersicht über die Zwischenkörper von $Q(\zeta)/\mathbb{Q}$.

Abgabe der Lösungen: Donnerstag, den 22. Januar nach der Vorlesung.

Blatt 13
22.1.1998

ALGEBRA

WS 1997/98
Prof. Brüdern
Dipl. Math. Dietmann
Dipl. Math. Elsholtz

Aufgabe 1
Man beweise, daß die alternierende Gruppe A_5 nur die trivialen Normalteiler $\{e\}$ und A_5 hat. (Vergleiche Blatt 1, Aufgabe 5.)

Aufgabe 2

(i) Seien p und q verschiedene Primzahlen und G eine Gruppe mit $\#G = pq$. Man beweise, daß G auflösbar ist. Weiterhin gebe man alle Gruppen mit 15 Elementen an. (Hinweis: Man kann die SYLOW-Sätze verwenden.)

(ii) Seien p und q verschiedene Primzahlen und G eine Gruppe mit $\#G = p^2q$. Man beweise, daß G auflösbar ist.

Aufgabe 3
Sei K ein Körper mit Charakteristik 0 und $f \in K[x]$ irreduzibel. Sei r eine Nullstelle von f. Sei $K_n/K_{n-1}/\ldots/K_2/K_1/K$ eine Radikal-Erweiterung von K mit $r \in K_n$. Man zeige, daß f durch Radikale ausgedrückt werden kann. Insbesondere gilt: Wenn *eine* Nullstelle von f durch Radikale ausgedrückt werden kann, dann auch alle anderen.

Aufgabe 4

(i) Sei p prim. Sei $f \in \mathbb{Q}[x]$ ein irreduzibles Polynom vom Grad p mit genau $p-2$ reellen Nullstellen. Man zeige, daß $Gal(f,\mathbb{Q}) = S_p$ ist. (Vergleiche Blatt 11, Aufgabe 5.)

(ii) Man konstruiere für jede Primzahl p ein Polynom mit den Eigenschaften aus (i). (Tip: Man denke an gerade Koeffizienten.)

(iii) Sei n ungerade und $g \in \mathbb{Q}[x]$ ein irreduzibles Polynom vom Grad n. Man beweise, daß alle Nullstellen reell sind, wenn die Galois-Gruppe $Gal(g,\mathbb{Q})$ zyklisch ist.

Aufgabe 5
Sei p eine Primzahl. Sei a eine quadratfreie Zahl mit $a \neq -1, 0, 1$. Sei K_p der Zerfällungskörper des Polynoms $f = X^p - a$ über $\mathbb{Q}$. Man beweise, daß $[K_p : \mathbb{Q}] = p(p-1)$ gilt. Ist $Gal(K_p/\mathbb{Q})$ auflösbar?

Abgabe der Lösungen: Donnerstag, den 29. Januar 1998 nach der Vorlesung.

Blatt 14
29.1.1998

Algebra

WS 1997/98
Prof. Brüdern
Dipl. Math. Dietmann
Dipl. Math. Elsholtz

Aufgabe 1
Sei p eine Primzahl. Man bestimme (bis auf Isomorphie) alle Gruppen der Ordnung p^2.

Aufgabe 2
Sei R ein Ring und $M \neq \{0\}$ ein torsionsfreier R-Modul. Dann ist R nullteilerfrei.

Aufgabe 3
Sei R ein Integritätsbereich und K sein Quotientenkörper. Sei M ein torsionsfreier R-Modul. Man zeige: Es gibt einen K-Vektorraum V und einen injektiven Modulhomomorphismus $\varphi : M \to V$, so daß V über K von $\varphi(M)$ erzeugt wird.

Aufgabe 4
Sei K ein Körper, $V = K^\infty$ der Vektorraum der Polynome mit Koeffizienten in K und $R = End(V)$ der Ring der Endomorphismen. Zeige: Für alle $n, m \in \mathbb{N}$ gilt $R^m \cong R^n$.

Aufgabe 5
Sei K ein Körper mit char $K \neq 2, 3$. Weiter sei $f \in K[X]$ irreduzibel, L der Zerfällungskörper von f über K und Δ die Diskriminante von f. Dann gilt $Gal(L/K) \cong S_3$, falls Δ kein Quadrat in K ist; andernfalls ist $Gal(L/K) \cong A_3$.

Abgabe der Lösungen: Donnerstag, den 5. Februar 1998 nach der Vorlesung.