M E T U
Department of Mathematics

	Field Extensions and Galois Theory Midterm I	
Code : *Math 368* Acad. Year : *2017-2018* Semester : *Spring* Instructor : *Karayayla* Date : *28.03.2018* Time : *17.40* Duration : *120 minutes*	Last Name : Name : Student No : Department : Signature : **7** Questions on **5** Pages SHOW DETAILED WORK!	

1	2	3	4	5		

1.(16 pts.) For $f \in \mathbb{R}[x]$ of degree 4, let x_1, x_2, x_3 and x_4 be the four roots of f in $\mathbb{C}$. Express the discriminant Δ of f in terms of the roots of f, and show that $\Delta < 0$ if exactly two of the roots of f are real and distinct. $\Delta(f) = \prod_{1\le i<j\le 4} (\alpha_i-\alpha_j)^2 = (x_1-x_2)^2 \cdot (\alpha_1-\alpha_3)^2 \cdot (\alpha_1-\alpha_4)^2 \cdot (\alpha_2-\alpha_3)^2 \cdot (\alpha_2-\alpha_4)^2 \cdot (\alpha_3-\alpha_4)^2$

Let $\alpha_1 \neq \alpha_2 \in \mathbb{R}$ and $\alpha_3, \alpha_4 \in \mathbb{C}-\mathbb{R}$, then $\bar{\alpha_3} = \alpha_4$ so $\alpha_3 \neq \alpha_4$, $\alpha_3 = a+bi$, $b \neq 0$

$\alpha_1 = c, \alpha_2 = d$ $c \neq d \in \mathbb{R}$ $\alpha_1, \dots, \alpha_4$ aredisthct so $\Delta(f) \neq 0$.

We know $\Delta(f) \in \mathbb{R}$ since $f \in \mathbb{R}[x]$.

$$\Delta(f) = (\underbrace{c-d}_{>0})^2 (\underbrace{2bi}_{<0})^2 \underbrace{((c-a-bi)(c-a+bi))^2}_{|z_1|^4 > 0} \cdot \underbrace{((d-a-bi)(d-a+bi))^2}_{|z_2|^4 > 0} \Rightarrow \Delta(f) < 0$$

$(z_1 \cdot \bar{z_1})^2 = (|z_1|^2)^2$ $\qquad$ $(z_2 \cdot \bar{z_2})^2 = (|z_2|^2)^2$

$z_1 = c-a+bi$ $\qquad$ $z_2 = d-a+bi$

$c-a \in \mathbb{R}, b \in \mathbb{R}$ $\qquad$ $d-a \in \mathbb{R}, b \in \mathbb{R}$

2.(16 pts.) Let $f = x^3 + 2x^2 + 3x + 5$ and α, β, γ be its roots in $\mathbb{C}$. Find a polynomial g of degree 3 whose roots are $\alpha\beta$, $\alpha\gamma$ and $\beta\gamma$. $g = (x-\alpha\beta)\cdot(x-\alpha\gamma)\cdot(x-\beta\gamma)$

$= x^3 - (\alpha\beta+\alpha\gamma+\beta\gamma)x^2 + (\alpha^2\beta\gamma + \alpha\beta^2\gamma + \alpha\beta\gamma^2)x - \alpha^2\beta^2\gamma^2$

$f = (x-\alpha)(x-\beta)(x-\gamma)$

$= x^3 - (\alpha+\beta+\gamma)x^2 + (\alpha\beta+\alpha\gamma+\beta\gamma)x - \alpha\beta\gamma$

$= x^3 + 2x^2 + 3x + 5 \Rightarrow \alpha+\beta+\gamma = -2,\ \alpha\beta+\alpha\gamma+\beta\gamma = 3,\ \alpha\beta\gamma = -5$

coefficients of g:

$-\alpha^2\beta^2\gamma^2 = -(\alpha\beta\gamma)^2 = -(-5)^2 = -25$

$\alpha^2\beta\gamma + \alpha\beta^2\gamma + \alpha\beta\gamma^2 = \alpha\beta\gamma(\alpha+\beta+\gamma) = (-5)\cdot(-2) = 10$

$-(\alpha\beta+\alpha\gamma+\beta\gamma) = -3$

So $g(x) = x^3 - 3x^2 + 10x - 25$

3.(2 × 9 pts.) a) Assume $f \in F[x]$ is irreducible where F is a field and f does not divide $g \in F[x]$. Show that there are $A, B \in F[x]$ such that $Af + Bg = 1$. (Hint: Consider the ideal $\langle f, g\rangle$ generated by f and g in $F[x]$ and use the fact that $F[x]$ is a PID.)

$\langle f,g\rangle = \langle h\rangle$ for some $h \in F[x]$ since $F[x]$ is a PID.

so $h \mid f$ and $h \mid g$.

$h \mid f$ and f is irreducible, so $f = h \cdot k$ for some $k \in F[x]$

$f = hk$ and f is irreducible $\Rightarrow$ h is a unit or k is a unit in $F[x]$
(by definition of irreducibility).

units in $F[x]$ are constants, so $h = c$ or $k = c$ for some $c \in F$

$k = c \Rightarrow h = c^{-1} \cdot f$ so $g = h \cdot l$ for some $l \in F[x]$ (because $h \mid g$ from above)

$\Rightarrow g = c^{-1} f \cdot l \Rightarrow f \mid g$ (contradiction) $f \nmid g$ is given.

Thus k is not a constant, therefore $h = c$. (we had $h = c$ or $k = c$).

We get $\langle f,g\rangle = \langle c\rangle$ for some $c \in F$.

$c \neq 0$, $c = 0 \Rightarrow \langle c\rangle = \{0\} \neq \langle f,g\rangle$

$\langle f,g\rangle = \langle c\rangle \Rightarrow c \in \langle f,g\rangle$, so $Af + Bg = c$ for $A, B \in F[x]$

Note: $\langle f,g\rangle = \{Af + Bg \mid A, B \in F[x]\}$

$(c^{-1}A) \cdot f + (c^{-1}B) \cdot g = 1$ $\left.\begin{matrix} c^{-1}A \\ c^{-1}B \end{matrix}\right\} \in F[x]$

b) For f, g, A, B as in part (a), show that $B + \langle f\rangle$ is the multiplicative inverse of $g + \langle f\rangle$ in the field $\frac{F[x]}{\langle f\rangle}$.

$f \nmid g$ in $F[x] \Leftrightarrow g \notin \langle f\rangle \Leftrightarrow g + \langle f\rangle \neq 0 + \langle f\rangle$ in $\frac{F[x]}{\langle f\rangle}$ - field since f is irreduc.

$(g + \langle f\rangle)(B + \langle f\rangle) = Bg + \langle f\rangle$
$= 1 + \langle f\rangle$

since $1 - Bg = Af + Bg - Bg = Af \in \langle f\rangle$

$1 + \langle f\rangle$ is multiplicative identity of the field $\frac{F[x]}{\langle f\rangle}$

Thus $(g + \langle f\rangle) \cdot (B + \langle f\rangle) = 1 + \langle f\rangle \Rightarrow (g + \langle f\rangle)^{-1} = B + \langle f\rangle$

4.(3×6 pts.) Let $F \subset L$ be a field extension and $\alpha \neq 0$, $\alpha \in L$ be algebraic over F.

a) Show that $1/\alpha$ is also algebraic over F.

α is alg. ov. $F \Rightarrow f(\alpha)=0$ for some $f \in F[x]$

$f = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, $f(\alpha)=0$

$a_n \alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 = 0$ (Divide by α^n (multiply by $\frac{1}{\alpha^n}$)):

$a_n + a_{n-1}\frac{1}{\alpha} + \cdots + a_{n-2}\frac{1}{\alpha^{n-2}} + a_{n-1}\frac{1}{\alpha^{n-1}} + a_0 \cdot \frac{1}{\alpha^n} = 0$

$\frac{1}{\alpha}$ is a root of $g(x) = a_n + a_{n-1}x + a_{n-2}x^2 + \cdots + a_2 x^{n-2} + a_1 x^{n-1} + a_0 x^n$

$g(1/\alpha)=0$, $g \in F[x] \Rightarrow 1/\alpha$ is alg. ov. F.

b) Show that $[F(\alpha):F] = [F(1/\alpha):F]$.

$F(\alpha)$ is a field, $\alpha \neq 0 \Rightarrow 1/\alpha = \alpha^{-1} \in F(\alpha)$

$F \subseteq F(\alpha)$ and $\alpha^{-1} \in F(\alpha) \Rightarrow F(\alpha^{-1}) \subseteq F(\alpha)$ ($F(\alpha^{-1})$: smallest subfield in L containing F and α^{-1})

similarly

$\left.\begin{array}{l}\alpha^{-1} \in F(\alpha^{-1}) \\ \alpha^{-1} \neq 0\end{array}\right\} \Rightarrow \alpha \in F(\alpha^{-1})$

thus $F(\alpha) \subseteq F(\alpha^{-1})$

Therefore $F(\alpha) = F(\alpha^{-1})$

Hence $[F(\alpha):F] = [F(\alpha^{-1}):F]$

c) If $f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in F[x]$ is the minimal polynomial of α over F, what is the minimal polynomial of $1/\alpha$ over F?

As in part a, we got $1/\alpha$ is a root of

$g(x) = 1 + a_{n-1}x + a_{n-2}x^2 + \cdots + a_2 x^{n-2} + a_1 x^{n-1} + a_0 x^n$, $g \in F[x]$

$a_0 \neq 0$ unless $f(x) = x$ since if $a_0 = 0$, $x \mid f$ and f is irred.

But $f = x \Rightarrow \alpha = 0$ (contradicting $\alpha \neq 0$)

So, $a_0 \neq 0$, hence $\deg(g) = n = \deg(f) = [F(\alpha):F] = [F(\alpha^{-1}):F]$

$a_0^{-1} \cdot g \in F[x]$ satisfies $a_0^{-1} g(\frac{1}{\alpha}) = 0$, $a_0^{-1} g$ is monic and

$\deg(a_0^{-1} g) = [F(\frac{1}{\alpha}):F] = \deg$ of min pol. h of $1/\alpha$ ov. F.

so $h \mid a_0^{-1} g$, $\deg h = \deg a_0^{-1} g$ and they are both monic

implies $h = a_0^{-1} \cdot g$.

5.(2 × 7 pts.) a) Show that $f = \frac{1}{3}x^4 + \frac{2}{5}x^3 + \frac{7}{2}x^2 + x + 2 \in \mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$.

$30 \cdot f = 10x^4 + 12x^3 + 105x^2 + 30x + 60 \in \mathbb{Z}[x]$

$30f$ is irreducible in $\mathbb{Q}[x]$ by Eiseinstein's criterion (choose $p=3$

$p \nmid 10,\ p \mid 12,\ p \mid 105,\ p \mid 30$

$p \mid 60,\ p^2 \nmid 60$)

so $30^{-1} \cdot 30f = f$ is irred. ov $\mathbb{Q}$.

b) If $a \in \mathbb{Z}$ is the product of distinct primes, then show that $f = x^n - a \in \mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$.

$a = p_1 p_2 \cdots p_k$ where p_i are distinct primes.

$x^n - a = x^n - p_1 p_2 \cdots p_k \in \mathbb{Z}[x]$ is irred ov. $\mathbb{Q}$ by Eiseinstein's Criterion

(take $p = p_1$)

$p_1 \nmid 1,\ p \mid \underset{a_{n-1}}{0},\ p \mid \underset{a_{n-2}}{0}, \cdots, p \mid \underset{a_0}{a},\ p^2 \nmid a$.

6.(Bonus, 10 pts.) For a field extension $F \subset L$, assume that $\alpha \in L$ is algebraic over F such that the degree of its minimal polynomial over F is odd. Prove that $F(\alpha^2) = F(\alpha)$.

$F \subseteq F(\alpha^2) \subseteq F(\alpha)$ field extensions ($\alpha \in F(\alpha) \Rightarrow \alpha^2 \in F(\alpha) \Rightarrow F(\alpha^2) \subseteq F(\alpha)$)

$\underset{\text{odd}}{[F(\alpha):F]} = \underset{\text{At most } 2}{[F(\alpha):F(\alpha^2)]} \cdot [F(\alpha^2):F]$

since α is a root of $g(x) = x^2 - \alpha^2 \in F(\alpha^2)[x]$

$\deg(g) = 2$

$2 \nmid$ odd number

g irred ov. $F(\alpha) \Rightarrow [F(\alpha):F(\alpha^2)] = 2$

so $[F(\alpha):F(\alpha^2)] = 1$

g reducible $\Rightarrow [F(\alpha):F(\alpha^2)] \leq 2$

Hence $F(\alpha^2) = F(\alpha)$.

so is 1.

(Note $F(\alpha^2)(\alpha) = F(\alpha^2, \alpha) = F(\alpha)$)

7.(10 + 8 pts.) a) Let $[F(\alpha):F]=r$ and $[F(\beta):F]=s$ for two elements $\alpha,\beta\in L$ for an extension field L over F. Show that $lcm(r,s)\le[F(\alpha,\beta):F]\le rs$ where $lcm(r,s)$ is the least common multiple of r and s.

consider $F\subseteq F(\alpha)\subseteq F(\alpha)(\beta)=F(\alpha,\beta)$

By Tower Thm, $\underbrace{[F(\alpha):F]}_{=r}\cdot\underbrace{[F(\alpha)(\beta):F(\alpha)]}_{\le s}=[\underbrace{F(\alpha)(\beta)}_{=F(\alpha,\beta)}:F]$

so $r\mid[F(\alpha,\beta):F]$

and $[F(\alpha,\beta):F]\le r\cdot s$

(since $[F(\beta):F]=s \Rightarrow g(\beta)=0$
$\deg(g)=s$
$g\in F[x]$
g: irred. poly of β over F
$g\in F[x]\subseteq F(\alpha)[x]$
so if h is irred poly of β over $F(\alpha)$, $h\mid g$, hence
$\deg h\le\deg g=s$
$[F(\alpha)(\beta):F(\alpha)]\le s$

similarly, considering

$F\subseteq F(\beta)\subseteq F(\beta)(\alpha)=F(\alpha,\beta)$

we get $s=[F(\beta):F]\mid[F(\alpha,\beta):F]$

$r\mid[F(\alpha,\beta):F]\wedge s\mid[F(\alpha,\beta):F]$

$\Rightarrow$ l.c.m.$(r,s)\mid[F(\alpha,\beta):F]$

$\Rightarrow$ l.c.m$(r,s)\le[F(\alpha,\beta):F]$

combining the results, l.c.m$(r,s)\le[F(\alpha,\beta):F]\le rs$

b) If $\zeta_5=e^{\frac{2\pi i}{5}}$, what is $[\mathbb{Q}(\zeta_5,\sqrt[3]{2}):\mathbb{Q}]$?

$[\mathbb{Q}(\zeta_5):\mathbb{Q}]=4$ – min. pol. of ζ_5 ov. $\mathbb{Q}$ is $x^4+x^3+x^2+x+1$ – We had proved this is irred ov. $\mathbb{Q}$ and ζ_5 is a root since
$\zeta_5^5-1=0$
$(\zeta_5-1)(\zeta_5^4+\zeta_5^3+\zeta_5^2+\zeta_5+1)=0$

$[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$ – min poly of $\sqrt[3]{2}$ ov. $\mathbb{Q}$ is x^3-2 (irred by Eiseinstein's Cr.)

Using part a:

$r=4, s=3$

l.c.m.$(r,s)=12$

l.c.m$(4,3)\le[\mathbb{Q}(\zeta_5,\sqrt[3]{2}):\mathbb{Q}]\le 4\cdot 3$ $\ne 0$.

$12\le$ " ≤ 12

so $[\mathbb{Q}(\zeta_5,\sqrt[3]{2}):\mathbb{Q}]=12$