# M E T U
# Department of Mathematics

| | Field Extensions and Galois Theory<br>Midterm II | |
|---|---|---|
| Code : *Math 368*<br>Acad. Year : *2017-2018*<br>Semester : *Spring*<br>Instructor : *Karayayla*<br><br>Date : *02.05.2018*<br>Time : *17.40*<br>Duration : *150 minutes* | Last Name :<br>Name : Student No :<br>Department :<br>Signature :<br><br>7 Questions on 5 Pages<br>SHOW DETAILED WORK! | |

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | | |
|---|---|---|---|---|---|---|---|---|---|
| S | O | L | U | T | I | O | N | S | |

1.(12 pts.) Write down the definitions of a splitting field, a normal field extension, and a separable element of an algebraic field extension.

splitting field: $F \subseteq L$ a field extension, $L$ is a splitting field of a polynomial $f \in F[x]$ if for

1) $f(x)$ splits completely in $L[x]$ as $f = c(x-\alpha_1)(x-\alpha_2) \cdots (x-\alpha_n)$, $\alpha_i \in L$, $c \in F$

and 2) $L = F(\alpha_1, \alpha_2, \ldots, \alpha_n)$

Normal Extension: $L$ is a normal extension over $F$ (where $F \subseteq L$ is a field ext.) if every irreducible $f \in F[x]$ which has a root in $L$ splits completely over $L$

Separable Element:

For an algebraic extension $F \subseteq L$, $\alpha \in L$ is called a separable element of $L$ over $F$ if the minimal polynomial $f$ of $\alpha$ over $F$ is separable over $F$, that is all roots of $f$ in a splitting field of $f$ over $F$ have multiplicity 1.

2.(12 pts.) Let $\alpha \in L$ be a root of $x^7 + \sqrt[5]{3}x^4 + ix^3 + \sqrt[3]{5} + 2$ where $L$ is a field extension of $\mathbb{Q}$. Show that $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq 210$.

Let $M = \mathbb{Q}(\sqrt[5]{3}, i, \sqrt[3]{5})$

Minimal polynomial of $\sqrt[5]{3}$ over $\mathbb{Q}$: $x^5 - 3$ $\Rightarrow [\mathbb{Q}(\sqrt[5]{3}) : \mathbb{Q}] = 5$

$i$ : $x^2 + 1$ $\Rightarrow [\mathbb{Q}(\sqrt[5]{3}, i) : \mathbb{Q}(\sqrt[5]{3})] \leq 2$

$\sqrt[3]{5}$ : $x^3 - 5$ $\Rightarrow [\mathbb{Q}(\sqrt[5]{3}, i, \sqrt[3]{5}) : \mathbb{Q}(\sqrt[5]{3}, i)] \leq 3$

Then by Tower Theorem, we get $[\mathbb{Q}(\sqrt[5]{3}, i, \sqrt[3]{5}) : \mathbb{Q}] \leq 5 \cdot 2 \cdot 3 = 30$

($[M:\mathbb{Q}] \leq 30$, indeed, we can show that $[M:\mathbb{Q}] = 30$ )

$f = x^7 + \sqrt[5]{3}x^4 + ix^3 + \sqrt[3]{5} + 2 \in M[x]$, $f(\alpha) = 0$

Thus $[M(\alpha) : M] \leq \deg(f) = 7$ (since minimal polynomial h of $\alpha$ over $M$ divides $f$)

Hence, by Tower Thm. $[M(\alpha) : \mathbb{Q}] = [M(\alpha) : M] \cdot [M : \mathbb{Q}] \leq 7 \cdot 30 = 210$

Since $\alpha \in M(\alpha)$, we have extensions $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq M \subseteq M(\alpha)$

$[\mathbb{Q}(\alpha) : \mathbb{Q}] \mid [M(\alpha) : \mathbb{Q}] \Rightarrow [\mathbb{Q}(\alpha) : \mathbb{Q}] \leq [M(\alpha) : \mathbb{Q}] \leq 210$

Therefore, $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq 210$.

3.(2 × 7 pts.) a) Let $\beta = \sqrt{2+\sqrt{2}} \in \mathbb{R}$. Find the minimal polynomial $f$ of $\beta$ over Q .

$\beta^2 = 2+\sqrt{2} \Rightarrow \beta^2 - 2 = \sqrt{2} \Rightarrow (\beta^2-2)^2 = 2$

$\beta^4 - 4\beta^2 + 4 = 2$

$\beta^4 - 4\beta^2 + 2 = 0$

$f(x) = x^4 - 4x^2 + 2 \in \mathbb{Q}[x] \Rightarrow f(\beta) = 0$

$f$ is irreducible, over $\mathbb{Q}$ by Schönemann-Eiseinstein Criterion (take $p=2$)

$f$ is monic. Thus, $f$ is the minimal polynomial of $\beta$ over $\mathbb{Q}$.

b) Show that $L = \mathbb{Q}(\beta)$ is a splitting field of $f$ over $\mathbb{Q}$.

$f = x^4 - 4x^2 + 2 = 0 \Rightarrow x^2 = \frac{4 \mp \sqrt{16-8}}{2} = 2 \mp \sqrt{2} \Rightarrow x = \mp\sqrt{2\mp\sqrt{2}}$ (4 distinct roots, call them $\beta_1, \beta_2, \beta_3, \beta_4$)

$\beta \in \mathbb{Q}(\beta)$, $-\beta = -\sqrt{2+\sqrt{2}} \in \mathbb{Q}(\beta)$

$\beta^2 = 2+\sqrt{2} \in \mathbb{Q}(\beta) \Rightarrow (2+\sqrt{2}) - 2 = \sqrt{2} \in \mathbb{Q}(\beta)$

$\beta \cdot \sqrt{2-\sqrt{2}} = \sqrt{2+\sqrt{2}} \cdot \sqrt{2-\sqrt{2}} = \sqrt{4-2} = \sqrt{2} \in \mathbb{Q}(\beta)$ so $\sqrt{2-\sqrt{2}} = \frac{\sqrt{2}}{\beta} \in \mathbb{Q}(\beta)$

$\sqrt{2-\sqrt{2}} \in \mathbb{Q}(\beta) \Rightarrow -\sqrt{2-\sqrt{2}} \in \mathbb{Q}(\beta)$.

All 4 distinct roots $\beta = \beta_1, \beta_2, \beta_3$ and $\beta_4$ are in $\mathbb{Q}(\beta) \Rightarrow \mathbb{Q}(\beta_1, \beta_2, \beta_3, \beta_4) \subseteq \mathbb{Q}(\beta)$

And since $\beta = \beta_1$, $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\beta_1, \beta_2, \beta_3, \beta_4)$

Thus, $\mathbb{Q}(\beta) = \mathbb{Q}(\beta_1, \beta_2, \beta_3, \beta_4)$ = splitting field of $\beta$ over $\mathbb{Q}$.

4. (14 pts.) Show that $\mathbb{Q}(\sqrt{3}, \sqrt[3]{5})$ is not a splitting field of any $f \in \mathbb{Q}[x]$ over $\mathbb{Q}$.

$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}, \sqrt[3]{5}) \subseteq \mathbb{R} \subseteq \mathbb{C}$

$x^3 - 5$ has one root, namely $\sqrt[3]{5}$ in $\mathbb{Q}(\sqrt{3}, \sqrt[3]{5})$

$x^3 - 5$ has 2 non-real roots in $\mathbb{C}$ thus the only root of $x^3 - 5$ in $\mathbb{Q}(\sqrt{3}, \sqrt[3]{5})$ is $\sqrt[3]{5}$, so $x^3 - 5$ does not split completely in $\mathbb{Q}(\sqrt{3}, \sqrt[3]{5})$

Since $x^3 - 5$ is irreducible over $\mathbb{Q}$ (3 is prime, there is no root in $\mathbb{Q}$), this means that the extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{3}, \sqrt[3]{5})$ is not a normal extension.

But if it were a splitting field of some polynomial, it would be a normal extension (splitting fields are normal extensions)

Then, $\mathbb{Q}(\sqrt{3}, \sqrt[3]{5})$ is not a splitting field over $\mathbb{Q}$ of any $f \in \mathbb{Q}[x]$.

5.(6 + 10 pts.) a) Write down a basis of $L = \mathbb{Q}(\sqrt{2}, i)$ over $\mathbb{Q}$ considering it as a vector space.

Minimal polynomial of $\sqrt{2}$ over $Q$: $x^2-2 \Rightarrow$ A basis of $Q(\sqrt{2})$ over $Q$ is $\{1, \sqrt{2}\}$

$g = x^2+1 \in Q[x] \subseteq Q(\sqrt{2})[x]$, $g(i)=0$, $g$ is monic

$\deg(g)=2$ and $g$ has no root in $Q(\sqrt{2}) \subseteq \mathbb{R}$ (since in $\mathbb{C}$ all roots are $\mp i \notin \mathbb{R}$)

Therefore, $g$ is irreducible over $Q(\sqrt{2})$, hence $[Q(\sqrt{2},i):Q(\sqrt{2})]=2$

Thus a basis of $Q(\sqrt{2},i)=Q(\sqrt{2})(i)$ over $Q(\sqrt{2})$ is $\{1,i\}$

Then, a basis of $Q(\sqrt{2},i)$ over $Q$ is

$B=\{1\cdot 1, 1\cdot i, \sqrt{2}\cdot 1, \sqrt{2}\cdot i\}=\{1, i, \sqrt{2}, \sqrt{2}\cdot i\}$

and $[Q(\sqrt{2},i):Q]=2\cdot 2=4$.

b) What is the condition on $k \in Q$ such that $\alpha = k\sqrt{2}+i$ is a primitive element of the extension $\mathbb{Q} \subset L$ (that is, $L = \mathbb{Q}(\alpha)$). (Hint: Use the basis from part a and use linear algebra.)

Let $\alpha = k\sqrt{2}+i$ where $k \in Q$, then $\alpha \in L$,

$Q \subseteq Q(\alpha) \subseteq L$. $\quad [L:Q]=[L:Q(\alpha)]\cdot[Q(\alpha):Q]$

$4 = [L:Q(\alpha)]\cdot[Q(\alpha):Q]$

$L=Q(\alpha) \Leftrightarrow [L:Q(\alpha)]=1 \Leftrightarrow [Q(\alpha):Q]=4 \Leftrightarrow$ Minimal polynomial of $\alpha$ over $Q$ has degree 4

$\Leftrightarrow \{1, \alpha, \alpha^2, \alpha^3\}$ is a basis of $Q(\alpha)=L=Q(\sqrt{2},i)$

So, $L=Q(\alpha) \Leftrightarrow \{1,\alpha,\alpha^2,\alpha^3\}$ is a linearly independent set over $Q$

Since $1, \alpha, \alpha^2, \alpha^3$ are in $L=Q(\sqrt{2},i)$, we can use the basis $B$ from part a, and check for linear independence of $1, \alpha, \alpha^2$ and $\alpha^3$:

$1$ is written as $(1,0,0,0)$ with respect to the basis $B=\{1, i, \sqrt{2}, \sqrt{2}i\}$

$\alpha = k\sqrt{2}+i$ " $(0,1,k,0)$

$\alpha^2=(2k^2-1)\cdot 1+2k\cdot(\sqrt{2}i)$ is written as $(2k^2-1,0,0,2k)$

$\alpha^3=[k\cdot(2k^2-1)-2k]\cdot\sqrt{2}+[(2k^2-1)+4k^2]i=(2k^3-3k)\cdot\sqrt{2}+(6k^2-1)\cdot i$

so $\alpha^3$ is written as the tuple $(0, 6k^2-1, 2k^3-3k, 0)$ w.r.to the basis $B$.

Then the condition that $L=Q(\alpha)$ is $\{1,\alpha,\alpha^2,\alpha^3\}$ is linearly indep. over $Q$, which is equivalent to

$$\begin{vmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & k & 0 \\ 2k^2-1 & 0 & 0 & 2k \\ 0 & 6k^2-1 & 2k^3-3k & 0 \end{vmatrix} \neq 0 \quad (4\times 4 \text{ determinant is nonsingular})$$

6.(4 + 6 + 6 pts.) Let $F$ be a field of characteristic $p > 0$ and assume that $f = x^p - x + c \in F[x]$ is irreducible over $F$.

a) Show that $f$ is separable over $F$.

$f'(x) = p \cdot x^{p-1} - 1 = -1$ since $\mathrm{char}(F) = p$ hence $p \cdot x^{p-1} = p \cdot 1 \cdot x^{p-1} = 0 x^{p-1} = 0$

Then $\mathrm{g.c.d.}(f, f') = \mathrm{g.c.d.}(f, -1) = 1$

Hence $f$ is separable over $F$.

b) Show that if $\alpha$ is a root of $f$ in some extension field $L$ over $F$, then $\alpha + 1$ is also a root of $f$.

$f(\alpha) = 0 \iff \alpha^p - \alpha + c = 0$

Then $f(\alpha+1) = (\alpha+1)^p - (\alpha+1) + c$

$= \alpha^p + 1^p - \alpha - 1 + c$ (since $\mathrm{char}(F) = p$, $(\alpha+1)^p = \alpha^p + 1^p$)

$= \alpha^p - \alpha + c = f(\alpha) = 0$

c) Show that $F(\alpha)$ is a normal extension field over $F$.

This follows if we can show that $F(\alpha)$ is a splitting field of a polynomial over $F$.

From part (b), $f(\alpha) = 0 \Rightarrow f(\alpha+1) = 0$ so $f(\alpha+2) = 0$, $f(\alpha+3) = 0$ ...

Since $\mathrm{char}(F) = p$ $1 + 1 + 1 + \cdots + 1 = 0$ if there are $p$ 1's.

Hence $\alpha, \alpha+1, \alpha+2, \ldots, \alpha+p-2, \alpha+p-1$ are $p$ distinct roots of $f$.

Since $\deg(f) = p$, these must be all roots, and each has multiplicity 1.

So, splitting field of $f$ over $F$ is

$F(\alpha, \alpha+1, \alpha+2, \ldots, \alpha+p-1) = F(\alpha)$

(since $\alpha \in F(\alpha) \Rightarrow \alpha + k \in F(\alpha)$ for any $k \in \mathbb{Z}$ ($k$ means $k \cdot 1_F$))

so $F(\alpha, \alpha+1, \ldots, \alpha+p-1) \subseteq F(\alpha)$ )

(The other inclusion is obvious )

7.($2 \times 8$ pts.) Let $L = \mathbb{Q}(\sqrt[5]{3}, \zeta_5)$ where $\zeta_5 = e^{\frac{2\pi i}{5}} \in \mathbb{C}$.

a) For a $\sigma \in Gal(L/\mathbb{Q})$, list the possible values of $\sigma(\sqrt[5]{3})$ and $\sigma(\zeta_5)$.

$f = x^5 - 3$ is minimal polynomial of $\sqrt[5]{3}$ over $\mathbb{Q}$ ($f$ is irred over $\mathbb{Q}$ since 5 is prime and $f$ has no root in $\mathbb{Q}$)

$\zeta_5$ is a root of $x^5 - 1 = (x-1)(x^4+x^3+x^2+x+1)$ hence of $x^4+x^3+x^2+x+1 = g(x)$ and we know (proved as a Thm) that $g(x)$ is irred over $\mathbb{Q}$. so minimal poly. of $\zeta_5$ over $\mathbb{Q}$ is $g(x)$.

Let $\sigma \in Gal(L/\mathbb{Q})$, $\sqrt[5]{3}$ is a root of $f \in \mathbb{Q}[x] \Rightarrow \sigma(\sqrt[5]{3})$ is a root of $f$ in $L$

$\zeta_5$ is a root of $g \in \mathbb{Q}[x] \Rightarrow \sigma(\zeta_5)$ is a root of $g$ in $L$

All roots of $f$ in $L$ are $\{\sqrt[5]{3} \cdot \zeta_5^k \mid k = 0,1,2,3,4\}$

All roots of $g$ in $L$ are $\{\zeta_5^k \mid k = \cancel{0},1,2,3,4\}$

Therefore

$\sigma(\sqrt[5]{3}) \in \{\sqrt[5]{3} \cdot \zeta_5^k \mid k = 0,1,2,3,4\}$ (5 choices) and $\sigma(\zeta_5) \in \{\zeta_5^k \mid k = 1,2,3,4\}$ (4 choices)

b) How many elements does the Galois group $Gal(L/\mathbb{Q})$ have?

$L$ is a splitting field of $x^5 - 3$ over $\mathbb{Q}$ since

splitting field of $x^5 - 3$ over $\mathbb{Q}$ : $\mathbb{Q}(\sqrt[5]{3}, \sqrt[5]{3}\zeta_5, \sqrt[5]{3}\zeta_5^2, \sqrt[5]{3}\zeta_5^3, \sqrt[5]{3}\zeta_5^4) = \mathbb{Q}(\sqrt[5]{3}, \zeta_5) = L$.

$x^5 - 3$ is separable over $\mathbb{Q}$ (all of the 5 distinct roots have multiplicity 1)

Thus, $L$ is a splitting field of a separable polynomial $f$ over $\mathbb{Q}$ ($f = x^5 - 3$)

, hence by a Theorem, $|Gal(L/\mathbb{Q})| = [L:\mathbb{Q}]$

$[\mathbb{Q}(\zeta_5):\mathbb{Q}] = 4 = \deg(x^4+x^3+x^2+x+1)$

$[\mathbb{Q}(\sqrt[5]{3}):\mathbb{Q}] = 5 = \deg(x^5 - 3)$

$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[5]{3}) \subseteq L$, $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_5) \subseteq L$ $\Rightarrow$ $4 = [\mathbb{Q}(\zeta_5):\mathbb{Q}] \mid [L:\mathbb{Q}]$, $5 = [\mathbb{Q}(\sqrt[5]{3}):\mathbb{Q}] \mid [L:\mathbb{Q}]$

so $\mathrm{l.c.m}(4,5) \mid [L:\mathbb{Q}]$

Also $[L:\mathbb{Q}] = \underbrace{[\mathbb{Q}(\zeta_5)(\sqrt[5]{3}):\mathbb{Q}(\sqrt[5]{3})]}_{\leq 4 \text{ since } g(\zeta_5) = 0} \cdot \underbrace{[\mathbb{Q}(\sqrt[5]{3}):\mathbb{Q}]}_{= 5} \Rightarrow [L:\mathbb{Q}] \leq 20$

~~[illegible]~~ $g \in \mathbb{Q}[x] \subseteq \mathbb{Q}(\sqrt[5]{3})[x]$

$20 = \mathrm{l.c.m}(4,5) \leq [L:\mathbb{Q}] \leq 20 \Rightarrow [L:\mathbb{Q}] = 20$

$|Gal(L/\mathbb{Q})| = 20$ so all possible choices in part a come from some $\sigma \in Gal(L/\mathbb{Q})$

8. (Bonus: 10 pts.) For a field $F$ of characteristic $p > 0$, the Frobeneous map $\varphi : F \to F$ is defined by $\varphi(x) = x^p$, and it is a field homomorphism.
Assuming that $\varphi : F \to F$ is onto, prove that any irreducible polynomial $f \in F[x]$ is separable over $F$.

Assume $\varphi : F \to F$ is onto and $f \in F[x]$ is not separable over $F$ for an irreduc. $f$ over $F$.

$f' \neq 0 \Rightarrow \deg(f') < \deg(f)$ and $f$ is irred. $\Rightarrow f \nmid f'$, hence $g.c.d(f, f') = 1$

(since only irred. factors of $f$ are constant ($\neq 0$) multiples of $1$ and $f$).

But since we assumed that $f$ is not separable, we cannot have

$g.c.d.(f, f') = 1$. Thus, $f' = 0$.

$$f(x) = \sum_{i=0}^{d} a_i x^i \quad , a_d \neq 0, \ d = \deg(f)$$

$$f'(x) = \sum_{i=0}^{d} a_i \cdot i \cdot x^{i-1} \quad , f'(x) = 0 \in F[x] \Leftrightarrow p \mid i \text{ whenever } a_i \neq 0 \in F.$$

Therefore, in $f$, only terms of the form $x^{p \cdot m_j}$ have nonzero coefficients in order to have $f'(x) = 0 \in F[x]$.

Thus, $f(x) = \sum_{j=0}^{e} b_j \cdot x^{p \cdot m_j} = \sum_{j=0}^{e} b_j (x^p)^{m_j} = g(x^p)$ for some $g(x) \in F[x]$

(Indeed $g = \sum_{j=0}^{e} b_j x^{m_j}$)

Then, $b_j = (c_j)^p$ for some $c_j \in F$

(since we assume $\varphi : F \to F$ is onto, $\exists c_j \in F \ni \varphi(c_j) = b_j$
$(c_j)^p = b_j$)

Thus,

$$f(x) = \sum_{j=0}^{e} b_j (x^p)^{m_j} = \sum_{j=0}^{e} (c_j)^p (x^{m_j})^p$$

$$= \left( \sum_{j=0}^{e} c_j x^{m_j} \right)^p = (h(x))^p \quad \text{for some } h \in F[x]$$

since $char(F) = p$

So, we obtained: $\cancel{F}$

$$f(x) = (h(x))^p \quad \text{for some } h(x) \in F[x]$$

This contradicts $f$ being irreducible since $p > 1$ ($p$ is a prime being $p = char(F)$)

Therefore, $f$ is separable over $F$.