M E T U
Department of Mathematics

Group	Field Extensions and Galois Theory Final	List No.
Code : *Math 368* Acad. Year : *2011* Semester : *Spring* Instructor : *Küçüksakallı*	Last Name : Name : Department : Signature :	Student No. : Section :
Date : *June 3, 2011* Time : *9:30* Duration : *120 minutes*	6 QUESTIONS ON 4 PAGES 80 TOTAL POINTS	

1	2	3	4	5	6		

1. (18pts) True or false? Justify your answers.

- **(6pts)** Let K be a subfield of $\mathbb{C}$. An element α is algebraic over K if and only if $K[\alpha] = K(\alpha)$.

If $K(\alpha)=K[\alpha]$, then $\frac{1}{\alpha}=a_n\alpha^n+\dots+a_1\alpha+a_0$. This gives us $a_n\alpha^{n+1}+\dots+a_1\alpha^2+a_0\alpha-1=0$. Thus α is algebraic. For converse assume α is algebraic and let f be its minimal polynomial. For any $g\in K[x]$ with $g(\alpha)\neq 0$, there exist h_i s.t. $fh_1+gh_2=1$. Thus $\frac{1}{g(\alpha)}\in K[\alpha]$. So $K(\alpha)=K[\alpha]$.

$\boxed{\text{TRUE}}$

- **(6pts)** Let $f \in K[x]$ be a polynomial of degree n. If L is the splitting field of f over K, then the degree of the extension L/K is less than or equal to $n!$.

Suppose $f(x)=(x-\alpha_0)\cdots(x-\alpha_{n-1})$ and consider $K_i=K(\alpha_0,\dots,\alpha_i)$. We have a chain of field extensions

$$K\subseteq K_0\subseteq K_1\subseteq\dots\subseteq K_{n-1}=L$$

Note that $[K_{i+1}:K_i]\le n$. By tower law, $[L:K]\le n!$

$\boxed{\text{TRUE}}$

- **(6pts)** The extension $\mathbb{Q}(\sqrt[3]{2},\zeta_3)/\mathbb{Q}$ is not simple. (An extension L/K is called simple if there exists $\alpha\in L$ such that $L=K(\alpha)$.)

Let $L=\mathbb{Q}(\sqrt[3]{2},\zeta_3)$. We know $L/\mathbb{Q}$ is normal and $Aut(L/\mathbb{Q})\cong S_3$. Consider $M=\mathbb{Q}(\underbrace{\sqrt[3]{2}+\zeta_3}_{\alpha})$. It is clear that $M\neq\mathbb{Q}(\zeta_3)$, otherwise $\sqrt[3]{2}=a+b\zeta_3$ for $a,b\in\mathbb{Q}$. Thus $[M:\mathbb{Q}]\neq 2$ by Galois correspondence. Moreover $M\neq\mathbb{Q}(\sqrt[3]{2}\zeta_3^i)$ for any integer i. Otherwise, for $\sigma:\sqrt[3]{2}\mapsto\sqrt[3]{2}\zeta_3$, we should have $\alpha+\sigma(\alpha)+\sigma^2(\alpha)=3\zeta_3\in\mathbb{Q}$ ↯

Thus $[M:\mathbb{Q}]=6$ and the extension $L/\mathbb{Q}$ is simple

$\boxed{\text{FALSE}}$

2. (12pts) Let p be an odd prime and let α be a root of $x^p - p$. Suppose that $K = \mathbb{Q}(\zeta_p)$ and $L = K(\alpha)$. Show that $\mathrm{Aut}(L/K)$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

The polynomial $f(x) = x^p - p$, is irreducible over $\mathbb{Q}$ by Eisenstein's criterion. Clearly $L = \Sigma_{f,\mathbb{Q}}$, the splitting field of f over $\mathbb{Q}$. Note that $[\mathbb{Q}(\zeta_p):\mathbb{Q}] = p-1$ and $[\mathbb{Q}(\alpha):\mathbb{Q}] = p$. Tower law implies that $[L:\mathbb{Q}] = p \cdot (p-1)$ and $[L:K] = p$.

Choose $\sigma : \alpha \mapsto \alpha \cdot \zeta_p$ in $\mathrm{Aut}(L/\mathbb{Q})$. Then $\sigma(\zeta_p) = \zeta_p^i$ for some integer i. Define $\tau = \sigma \cdot \gamma$ where $\gamma(\zeta_p) = \zeta_p^{-i}$ and $\gamma(\alpha) = \alpha$ (we can choose such $\gamma \in \mathrm{Aut}(L/\mathbb{Q})$ because $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is normal)

Now $\tau \in \mathrm{Aut}(L/\mathbb{Q})$ and $\tau(\alpha) = \alpha\zeta_p$, $\tau(\zeta_p) = \zeta_p$. Thus $\tau \in \mathrm{Aut}(L/K)$

Consider $\varphi : \mathbb{Z} \longrightarrow \mathrm{Aut}(L/K)$ which maps n to $\underbrace{\tau \circ \tau \circ \cdots \circ \tau}_{n \text{ times}}$.

This map is surjective with $\mathrm{Ker}(\varphi) = p\mathbb{Z}$. Thus $\mathrm{Aut}(L/K)$ is isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

3. (10pts) Let $L = \mathbb{Q}(\zeta_7)$ be the 7-th cyclotomic field. Let K be its unique subfield such that $[L:K] = 3$. Does there exist an element $\alpha \in L \setminus K$ such that $\alpha^3 \in K$?

Assume there exists such $\alpha \in L \setminus K$. Then $\alpha^3 - k = 0$ for some $k \in K$. The polynomial $f(x) = x^3 - k \in K[x]$ is irreducible over K and splits in L. (To see this observe that $L/\mathbb{Q}$ is a normal extension with an abelian Galois group. As a result the extension L/K must be normal).

Since $f(x)$ splits in L, the elements $\alpha, \alpha\zeta_3, \alpha\zeta_3^2$ are contained in L. Therefore $\zeta_3 \in L$. It follows that $\zeta_3\zeta_7$, a primitive 21^{st} root of unity, is in L. Thus

$$12 = \varphi(21) \mid [L:\mathbb{Q}] = 6$$

and it is a contradiction.

4. **(12pts)** Let L/K be a radical extension in $\mathbb{C}$ and let N be the normal closure of this extension. Prove that N/K is a radical extension.

This is Lemma 15.4 in your textbook.

5. **(10pts)** Find all irreducible polynomials of degrees 1, 2 and 4 in $\mathbb{F}_2[x]$ and prove that their product is $x^{16} - x$.

degree 1 $\rightsquigarrow$ $\boxed{x}$ and $\boxed{x+1}$

degree 2 $\rightsquigarrow$ $ax+bx+c$ with $a,b,c \in \mathbb{F}_2$. The coefficients a and c must be 1. Only possibility is $\boxed{x^2+x+1}$.

degree 4 $\rightsquigarrow$ $ax^4+bx^3+cx^2+dx+e$. Note that $a=e=1$. Moreover $b+c+d=1$ (otherwise 1 would be a root) Possibilities are $\boxed{x^4+x^3+x^2+x+1}$

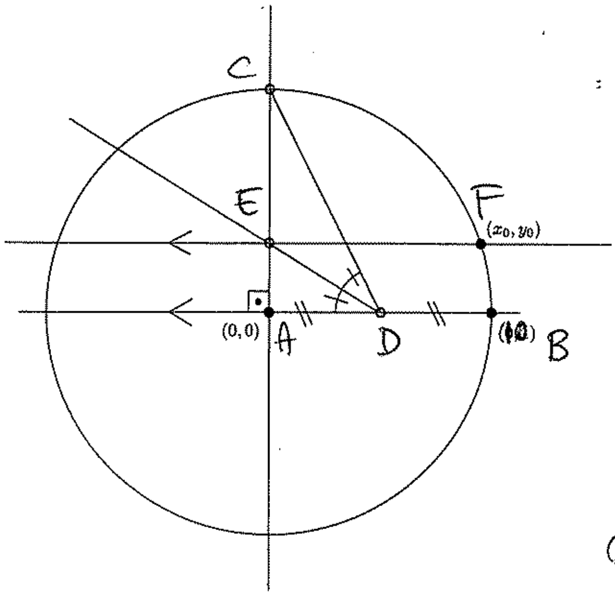
$\boxed{x^4+x^3+1}$

$x^4+x^2+1 \rightsquigarrow (x^2+x+1)^2$ (the other three must be irreducible)

$\boxed{x^4+x+1}$

Note that each irreducible f divides $x^{16}-x$ due to finite fields theory. Moreover their sum of degrees is exactly 16. Thus the product of irreducible polynomials above must be $x^{16}-x$.

6. (12+6=18pts) Starting from $P_0 = \{(0,0),(1,0)\}$, show that (x_0, y_0) can be constructed by a ruler and a compass. Explain each step carefully.



① Line through A & B

② Circle with center A, through B.

③ Line through A, perpendicular to AB. Obtain C.

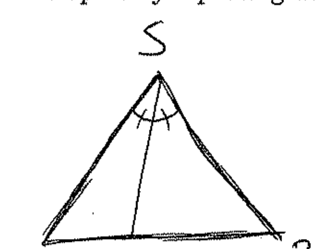
④ Bisect AB. Obtain D

⑤ Line through C & D.

⑥ Bisect angle $\widehat{ADC}$. Obtain E

⑦ Line through E, parallel to AB. Obtain $F = (x_0, y_0)$

- Find x_0 and y_0 in terms of radicals. Show that a regular pentagon can be drawn with a ruler and a compass by repeating the above construction.



Elementary geometry

$$\frac{|PT|}{|TR|} = \frac{|SP|}{|SR|}$$

Using this, one can show that $y_0 = \dfrac{\sqrt{5}-1}{4}$ and $x_0 = \sqrt{1-y_0^2}$

Note that $y_0 = \dfrac{\sqrt{5}-1}{4} = \cos\dfrac{2\pi}{5}$.

Repeating the above construction we obtain a regular pentagon