METU
Department of Mathematics

Field Extensions and Galois Theory FINAL	
Code : *Math 368* Acad. Year : *2017-2018* Semester : *Spring* Instructor : *Karayayla* Date : *28.05.2018* Time : *9.30* Duration : *150 minutes*	Last Name : Name : Student No : Department : Signature : 7 Questions on 5 Pages SHOW DETAILED WORK!

1	2	3	4	5	6				
S	O	L	U	T	I	O	N	S	

1. (8+7+7 pts.) a) Let $F \subset L$ be a finite extension of fields. Write down 4 equivalent conditions for this extension to be a Galois extension.
b) Prove that $F \subset L$ is a Galois extension if and only if for any $\alpha \in L - F$ there exists a $\sigma \in Gal(L/F)$ such that $\sigma(\alpha) \neq \alpha$.
c) Let $F \subset K$ and $K \subset L$ be Galois extensions. Prove that $F \subset L$ is Galois if every $\sigma \in Gal(K/F)$ extends to an automorphism of L.

a) 1) L is a splitting field over F of a separable polynomial $f \in F[x]$.
2) Fixed field of $Gal(L/F)$ is F ($F = L_{Gal(L/F)}$).
3) L is a normal and separable extension over F.
4) $[L:F] = |Gal(L/F)|$.

b) • Assume that for any $\alpha \in L-F$ there exists $\sigma \in Gal(L/F)$ such that $\sigma(\alpha) \neq \alpha$,
then $\alpha \in L-F \Rightarrow \alpha \notin L_{Gal(L/F)}$ = fixed field of $Gal(L/F)$
And since $F \subseteq L_{Gal(L/F)}$ by definition of $Gal(L/F)$, we get $F = L_{Gal(L/F)}$
hence by condition 2 in part "a", $F \subseteq L$ is Galois.
• Assume now, $F \subseteq L$ is Galois. Then $F = L_{Gal(L/F)} = \{\alpha \in L \mid \sigma(\alpha) = \alpha$ for all $\sigma \in Gal(L/F)\}$
Then $\alpha \notin F$ ($\alpha \in L-F$) implies $\alpha \notin L_{Gal(L/F)}$,
hence there is $\sigma \in Gal(L/F)$ such that $\sigma(\alpha) \neq \alpha$.

c) Assume $F \subseteq K$ and $K \subseteq L$ are Galois and every $\sigma \in Gal(K/F)$ extends to an automorphism of L.
Let $\alpha \in L-F$, (we'll use part b to show $F \subseteq L$ is Galois by showing existence of $\sigma \in Gal(L/F)$ such that $\sigma(\alpha) \neq \alpha$).
Case 1, $\alpha \in L-K$, then since $K \subseteq L$ is Galois, there is $\sigma_1 \in Gal(L/K)$ such that $\sigma_1(\alpha) \neq \alpha$ by part (b), but $\sigma_1 \in Gal(L/K)$ and $F \subseteq K \subseteq L \Rightarrow \sigma_1 \in Gal(L/F)$
hence there is $\sigma_1 \in Gal(L/F)$ such that $\sigma_1(\alpha) \neq \alpha$.
Case 2, $\alpha \in K-F$: Then since $F \subseteq K$ is Galois, there is $\sigma \in Gal(K/F)$ such that $\sigma(\alpha) \neq \alpha$ by part b, then σ extends to an automorphism $\sigma_2 : L \to L$
$\sigma_2|_F = \sigma|_F = Id_F \Rightarrow \sigma_2 \in Gal(L/F)$
Thus there exists $\sigma_2 \in Gal(L/F)$ such that $\sigma_2(\alpha) \neq \alpha$.
Thus, by part (b), $F \subseteq L$ is Galois

2. (10+10 pts.) Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
a) Show that $Gal(L/\mathbb{Q})$ is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.
b) Find all fields K such that $\mathbb{Q} \subset K \subset L$.

a) L is splitting field of $(x^2-2)\cdot(x^2-3) = f$ over $\mathbb{Q}$ and f is separable, hence $\mathbb{Q} \subseteq L$ is a Galois extension, thus $|Gal(L/\mathbb{Q})| = [L:\mathbb{Q}]$

$$[L:\mathbb{Q}] = [L:\mathbb{Q}(\sqrt{2})]\cdot[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = [\left(\mathbb{Q}(\sqrt{2})\right)(\sqrt{3}):\mathbb{Q}(\sqrt{2})]\cdot[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]$$
$$= 2\cdot 2 = 4 \Rightarrow |Gal(L/\mathbb{Q})| = 4.$$

$\sigma \in Gal(L/\mathbb{Q}) \Rightarrow \sigma(\sqrt{2}) = \mp\sqrt{2}$ and $\sigma(\sqrt{3}) = \mp\sqrt{3}$, σ is uniquely determined by its images at $\sqrt{2}$ and $\sqrt{3}$. There are 4 possible choices and $|Gal(L/\mathbb{Q})| = 4$, so all those 4 choices correspond to the 4 elements of $Gal(L/\mathbb{Q})$

We have

$\sigma_1 = Id_L$: $\sqrt{2} \mapsto \sqrt{2}$, $\sqrt{3} \mapsto \sqrt{3}$

$\sigma_2 : L \to L$: $\sqrt{2} \mapsto -\sqrt{2}$, $\sqrt{3} \mapsto \sqrt{3}$

$\sigma_3 : L \to L$: $\sqrt{2} \mapsto -\sqrt{2}$, $\sqrt{3} \mapsto \sqrt{3}$

$\sigma_4 : L \to L$: $\sqrt{2} \mapsto -\sqrt{2}$, $\sqrt{3} \mapsto -\sqrt{3}$

For any of σ_i, $i = 1,2,3,4$, $\sigma_i \circ \sigma_i = \sigma_i^2 : L \to L$, $\sqrt{2} \mapsto \sqrt{2}$, $\sqrt{3} \mapsto \sqrt{3}$ $\Rightarrow \sigma_i^2 = Id_L$.

Any group G which satisfies $x \in G \Rightarrow x^2 = e$ (identity) is an abelian group. So, $Gal(L/F)$ is an abelian group of order 4 in which every non-identity element has order 2. Abelian groups of order 4 are $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. In $\mathbb{Z}/4\mathbb{Z}$ there is an element of order 4, Thus $Gal(L/\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

---

b) Intermediate fields k of the extension $\mathbb{Q} \subseteq L$ (which is Galois extension) and subgroups of $Gal(L/\mathbb{Q})$ are in 1 to 1 correspondence.

$H_1 = \{(0,0)\}$, $H_2 = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{(0,0),(0,1),(1,0),(1,1)\}$
$H_3 = \{(0,0),(1,0)\}$, $H_4 = \{(0,0),(0,1)\}$, $H_5 = \{(0,0),(1,1)\}$ → There are 5 subgr. of $Gal(L/\mathbb{Q})$

So there are 5 intermediate fields k, $\mathbb{Q} \subseteq k \subseteq L$.

$L_{H_1} = L$, $L_{H_2} = L_{Gal(L/\mathbb{Q})} = \mathbb{Q}$

$\mathbb{Q}(\sqrt{2})$, $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{6})$ are 3 distinct subfields of $\mathbb{Q} \subseteq L$.
Since there are 5 intermediate fields k (because there are 5 subgr. of $Gal(L/\mathbb{Q})$), these are all possible fields k. $k \in \{\mathbb{Q}, L, \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{6})\}$

3. (4 × 5 pts.) For each of the following field extensions, determine whether it is a Galois extension or not:

a) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$

b) $\mathbb{Q} \subset \mathbb{Q}(\alpha, \beta)$, where α and β are distinct roots of $x^3 + x^2 + 2x + 1$.

c) $F_p(t^p) \subset F_p(t)$ where t is a variable and F_p is finite field with p (prime) elements ($\mathrm{F}_p = \mathbb{Z}/p\mathbb{Z}$).

d) $\mathbb{C}(t^n) \subset \mathbb{C}(t)$ where t is a variable and n is a positive integer.

a) It is not Galois since it is not a normal extension, x^3-2 has a root $\sqrt[3]{2} \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) \subseteq \mathbb{R}$ but the other 2 complex roots of x^3-2 are not in $\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$.

b) $\left.\begin{array}{l} f = x^3+x^2+2x+1 \\ f' = 3x^2+2x+2 \end{array}\right\}$ Check that g.c.d $(f, f') = 1$, so f is separable.

α, β, γ are 3 distinct roots of $f \Rightarrow f = (x-\alpha)(x-\beta)(x-\gamma)$ (f is monic)

so $1 = -\alpha\beta\gamma \Rightarrow \gamma = \frac{-1}{\alpha\beta} \in \mathbb{Q}(\alpha, \beta)$

Thus, f splits completely in $\mathbb{Q}(\alpha, \beta)$

$\mathbb{Q}(\alpha, \beta) = \mathbb{Q}(\alpha, \beta, \gamma)$: splitting field of sep. pol. $f \in \mathbb{Q}[x]$ over $\mathbb{Q}$,

thus $\mathbb{Q} \subseteq \mathbb{Q}(\alpha, \beta)$ is Galois.

c) Let $K = F_p(t^p)$ and $L = F_p(t)$: field of rational functions over F_p in a variable t

$L = K(t)$ and t is a root of $f(x) = x^p - t^p \in K[x]$.

Since char F_p = char K = char $L = p$, $x^p - t^p = (x-t)^p \Rightarrow f$ is not a separable polynomial.

minimal polynomial $g(x) \in K[x]$ of t over K divides f, so

$g \mid x^p - t^p \Rightarrow g \mid (x-t)^p$ in a splitting field $\Rightarrow g$ is not separable.

Hence $t \in L$ is not a separable element over K, thus $K \subseteq L$ is not a separable extension, hence $K \subseteq L$ is <u>not</u> Galois.

d) Let $K = \mathbb{C}(t^4)$, $L = \mathbb{C}(t)$.

Then $L = K(t)$ and t is a root of $f(x) = x^4 - t^4 \in K[x]$

other roots of f are $-t, it$ and $-it$, all lie in L since $t \in L, i \in \mathbb{C} \subseteq L$.

so $f \in K[x]$ splits completely in $L = K(t) = K(t, -t, it, -it)$

L is a splitting field over K of the separable polynomial $f \in K[x]$.

Thus, $K \subseteq L$ is a Galois extension.

4. (5 × 4 pts.) Let F be a field extension of $\mathbb{C}$, and assume that $f = x^n - \beta \in F[x]$ is irreducible. Let α be a root of f in some extension field of F.

a) Show that $F(\alpha)$ is a splitting field of f over F.

b) Show that $F \subset F(\alpha)$ is a Galois extension.

c) Show that there exists a $\sigma \in Gal(F(\alpha)/F)$ such that $\sigma(\alpha) = \zeta_n \alpha$ where $\zeta_n = e^{\frac{2\pi i}{n}} \in \mathbb{C} \subset F$ is the primitive nth root of 1.

d) Show that $Gal(F(\alpha)/F) = \langle \sigma \rangle$ and it is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ (σ as in part (c)).

e) Show that $F \subset K$ is Galois for any intermediate field $F \subset K \subset F(\alpha)$.

a) $f(\alpha) = 0 \Rightarrow \alpha^n - \beta = 0$, other roots of f are $\zeta_n^i \alpha$ for $i = 1, 2, \dots, n-1$

($\zeta_n = e^{\frac{2\pi i}{n}} \in \mathbb{C} \subseteq \mathbb{F} \subsetneq L = K(\alpha) \Rightarrow \zeta_n^i \alpha \in L$ for all $i = 0, 1, \dots, n-1$)

so splitting field of f over $\mathbb{F}$ is $\mathbb{F}(\alpha, \zeta_n \alpha, \zeta_n^2 \alpha, \dots, \zeta_n^{n-1} \alpha) = \mathbb{F}(\alpha)$

($\supseteq$ is clear, for $\subseteq$, each $\zeta_n^i \alpha \in K(\alpha)$ from above.) ∎

b) $f = x^n - \beta$ has n distinct roots $\alpha, \zeta_n \alpha, \zeta_n^2 \alpha, \dots, \zeta_n^{n-1} \alpha$ so f is separable

$\mathbb{F}(\alpha) = L$ is splitting field over $\mathbb{F}$ of the separable $f \in \mathbb{F}[x]$, thus $\mathbb{F} \subseteq L$ is a Galois extension.

c) Since $f = x^n - \beta \in \mathbb{F}[x]$ is assumed to be irreducible and since α and $\zeta_n \alpha$ are roots of the same irreducible polynomial f, by the extension properties of automorphisms to splitting fields, there exists σ which extends $Id : \mathbb{F} \to \mathbb{F}$ to an autom. $\sigma : L \to L$ such that $\sigma(\alpha) = \zeta_n \alpha$.

d) $|Gal(L/\mathbb{F})| = [L : \mathbb{F}] = [\mathbb{F}(\alpha) : \mathbb{F}] = \deg(f) = n$ (since $\mathbb{F} \subseteq L$ is Galois)

σ in part (c) is in $Gal(L/K)$.

$\sigma^i(\alpha) = \sigma^{i-1}(\sigma(\alpha)) = \sigma^{i-1}(\zeta_n \alpha) = \zeta_n \cdot \sigma^{i-1}(\alpha) = \dots = \zeta_n \zeta_n \sigma^{i-2}(\alpha) = \dots = \zeta_n^i \alpha$

since σ fixes $\zeta_n \in \mathbb{F}$ (because $\sigma \in Gal(L/\mathbb{F})$)

$\sigma^i(\alpha) = \zeta_n^i \alpha$ and $\sigma \in Gal(L/\mathbb{F})$ is uniquely determined by $\sigma(\alpha)$,

hence $\sigma^i = Id_L \Leftrightarrow \sigma^i(\alpha) = \alpha \Leftrightarrow \zeta_n^i = 1 \Leftrightarrow n \mid i$.

Then, order of $\sigma \in Gal(L/\mathbb{F})$ is n. $|\langle \sigma \rangle| = n \le |Gal(L/\mathbb{F})| = n$

($\langle \sigma \rangle \le Gal(L/\mathbb{F})$)
subgroup

so $\langle \sigma \rangle = Gal(L/K)$
isom. to $\mathbb{Z}/n\mathbb{Z}$

e) Since $Gal(L/\mathbb{F}) \cong \mathbb{Z}/n\mathbb{Z}$ is abelian, all ~~norma~~ subgroups of $Gal(L/\mathbb{F})$ are normal subgroups. Then, for any K such that $F \subseteq K \subseteq L$, $Gal(L/K) \trianglelefteq Gal(L/F)$

hence, by Fundamental Thm of Galois Theory part 2, $F \subseteq K$ is a Galois extension.

5. (10+10 pts.) a) Let H be a subgroup of $Gal(L/F)$ for a field extension $F \subset L$. Show that the fixed field of H in L defined as $L_H = \{\alpha \in L | \sigma(\alpha) = \alpha \text{ for all } \sigma \in Gal(L/F)\}$ is a subfield of L containing F.
b) Assume that $[L : F] = p^2$ where p is a prime and $L \neq F(\alpha)$ for any $\alpha \in L$. Show that $[F(\beta) : F] = p$ for any $\beta \in L - F$.

$F \subseteq L_H$ since $\alpha \in F \Rightarrow \sigma(\alpha) = \alpha$ for all $\sigma \in Gal(L/F)$ by definition.

so $L_H \neq \emptyset$,

Let $\alpha, \beta \in L_H$, then $\sigma(\alpha) = \alpha$, $\sigma(\beta) = \beta$ for all $\sigma \in Gal(L/F)$

So, for any $\sigma \in Gal(L/F)$,

$\sigma: L \to L$ field autom. of L.

$$\left.\begin{array}{l} \sigma(\alpha \mp \beta) = \sigma(\alpha) \mp \sigma(\beta) = \alpha \mp \beta \\ \sigma(\alpha\beta) = \sigma(\alpha) \cdot \sigma(\beta) = \alpha \cdot \beta \\ \sigma(\alpha^{-1}) = (\sigma(\alpha))^{-1} = \alpha^{-1} \end{array}\right\} \Rightarrow \begin{array}{l} \alpha \mp \beta \in L_H \\ \alpha\beta \in L_H \\ \alpha^{-1} \in L_H \end{array}$$ for any $\alpha, \beta \in L_H$

Hence L_H is a subfield of L, which contains F.

b) Let $\beta \in L - F$, then $[F(\beta) : F] \neq 1$ and $[F(\beta) : F] \neq p^2$ since $F(\beta) \neq L$

$F \subseteq F(\beta) \subseteq L$ field extensions.

Then by Tower Thm

$$[L : F] = [L : F(\beta)] \cdot [F(\beta) : F]$$

Hence $[F(\beta) : F] \mid [L : F] = p^2$

positive divisors of p^2 are $1, p, p^2$, but $[F(\beta) : F] \neq 1$, $\neq p^2$ from above

Hence $[F(\beta) : F] = p$

6. (Bonus: 10 pts.) For each of the following statements, determine whether it is true or false (No explanation is asked, but two wrong answers will cancel one correct answer):

1) There exists finite extensions $F \subset L$ which have infinitely many intermediate fields. (T)

2) $[L : F] = 120$ where $L = \mathbb{Q}(x_1, ..., x_n)$ (field of rational functions in n variables) and $F = \mathbb{Q}(\sigma_1, ..., \sigma_n)$ where σ_i are elementary symmetric polynomials in $x_1, ..., x_n$. (T)

3) For any finite extension $F \subset L$ there exists an intermediate extension $F \subset K \subset L$, $K \neq L$ such that $K \subset L$ is Galois. (F)

4) If $char(F) \neq 0$ and $F \subset L$ is a separable extension which is not Galois, then there is no extension $L \subset M$ such that $F \subset M$ is Galois. (F)

5) If $f \in F[x]$ is irreducible and $F \subset K$ is a finite extension, then f is irreducible in $K[x]$. (F)

6) If L is a splitting field of $f \in F[x]$ over F and if $F \subset K \subset L$ is an intermediate extension, then L is also a splitting field of f over K. (T)

7) Any finite and normal extension $F \subset L$ is a splitting field. (T)

8) An algebraic extension is a finite extension. (F)

9) For finite extensions $F \subset K \subset L$, if $\alpha \in L - K$ is separable over K, then α is separable over F. (F)

10) For polynomials of degree d ($d \geq 5$) over $\mathbb{Q}$, there is no formula (valid for all degree d polynomials) expressing the roots of the polynomial in terms of the coefficients of the polynomial using the operations of taking radicals (nth root), addition, subtraction, multiplication and division. (T)

Some Explanations

1) $F = k(t, u)$, k: field of char. $= p > 0$, t, u variables, $L = F(\alpha, \beta)$ where $\alpha^p = t$, $\beta^p = u$ (Example we had in class).

2) $Gal(L:F) = S_5$ and $|S_5| = 5! = 120 = [L:F]$ since $F \subseteq L$ is Galois.

3) $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2})$

4) Galois Closure Thm.

5) $x^2+1 \in \mathbb{R}[x]$ not irred. in $\mathbb{C}[x]$, $\mathbb{R} \subseteq \mathbb{C}$ finite ext.

6) $\alpha_1, \alpha_2, \dots, \alpha_n$ roots of $f \Rightarrow L = F(\alpha_1, \dots, \alpha_n) = K(\alpha_1, \dots, \alpha_n)$, $f \in F[x] \subseteq K[x] \Rightarrow f \in K[x]$

8) Converse is true. $\mathbb{Q} \subseteq \overline{\mathbb{Q}}$ algebraic closure of $\mathbb{Q} \Rightarrow [\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$, $\overline{\mathbb{Q}}$ is algeb. ov. $\mathbb{Q}$.

9) $char(F_p) = p > 2 \Rightarrow$ Let $F = F_p(t^p)$ and $K = F_p(t)$ (t: a variable)

$[K:F] = p$ (finite)

Let $L = K(\alpha)$ where $\alpha^2 = t$, $\pm\alpha$ are roots of $x^2 - t \in K[x]$

$\alpha \neq -\alpha$ since char $\neq 2$. so α is sep over K, $\alpha \in L \setminus K$.

$\alpha^2 = t \Rightarrow \alpha^{2p} = t^p \Rightarrow \alpha$ is a root of $g(x) = x^{2p} - t^p \in F[x]$

min pol. of α ov. F: $h \Rightarrow h \mid g$

g factorizes as $(x-\alpha)^p \cdot (x+\alpha)^p$

$deg(h) = [F(\alpha) : F] \mid [K(\alpha):F] = 2p \Rightarrow deg(h) \in \{1, 2, p, 2p\}$

$deg\, h \neq 1$ ($\alpha \notin F$)

$deg\, h = 2 \Rightarrow h = (x \mp \alpha)^2$ or $h = (x-\alpha)(x+\alpha)$ but $\alpha^2 \notin F$

$deg\, h = p \Rightarrow$ constant term of $h = \mp\alpha^p \notin F$ contr. $\alpha^p = t^{p/2} \notin F$. so $deg\, h = 2p$, α is not sep. ov. F.