Midterm2 - MATH 742

Boren(Wells) Guan

Date: May 9, 2025

Before Reading:

To make the proof more readable, I will miss or gap some natural or not important facts or notations during my writing. If you feel it hard to see, you can refer the appendix after the proof, where I will try to explain some simple conclusions (will be marked) more clearly. In case that you misunderstand the mark, I will add the mark just after those formulas between $ and before those between $$.

And I have to claim that the appendix is of course a part of my assignment, so the reference of it is required. Enjoy your grading!

Problem.1

Sol.

Only $(\mathbb{Z}/p\mathbb{Z})(z)$ is not.

Problem.2

Set $\alpha = \sqrt{2-\sqrt{2}}$.

(a) Find the minimal polynomial of α over $\mathbb{Q}$.

(b) Show $\mathbb{Q}(\alpha) \supset \mathbb{Q}$ is a Galois extension.

(c) Find the Galois group $\mathrm{Gal}(\mathbb{Q}(\alpha)/\mathbb{Q})$.

Sol.

(a)We know α is a root of $(x^2-2)^2-2 = x^4-4x^2+2$, which is irreducible by choosing $p=2$ and use the Eisenstein's Criterion. So $f(x) = x^4-4x^2+2$ is a minimal polynomial of α over $\mathbb{Q}$.

(b) We know roots of x^4-4x^2+2 are $\pm\sqrt{2+\sqrt{2}}, \pm\sqrt{2-\sqrt{2}}$ and notice $\sqrt{2+\sqrt{2}}\sqrt{2-\sqrt{2}} = \sqrt{2} = 2-\alpha^2$ which means $\sqrt{2+\sqrt{2}} \in \mathbb{Q}[\alpha]$ and hence $\mathbb{Q}[\alpha]$ is generated by $\pm\sqrt{2+\sqrt{2}}, \pm\sqrt{2-\sqrt{2}}$, which means it is a splitting field of a separable polynomial. Therefore, it is a Galois extension.

(c) Since $\mathbb{Q}[\alpha] \cong \mathbb{Q}[x]/(x^4-4x^2+2)$, it has the degree of 4 and hence $\mathrm{Gal}(\mathbb{Q}[\alpha]/\mathbb{Q})$ has the order of 4. Assume $\phi \in \mathrm{Gal}(\mathbb{Q}[\alpha]/\mathbb{Q})$, then $\phi(\alpha) \in \{\pm\sqrt{2+\sqrt{2}}, \pm\sqrt{2-\sqrt{2}}\}$. Notice $\sqrt{2+\sqrt{2}} = (2-\alpha^2)\alpha^{-1}$, so ϕ is uniquely determined by $\phi(\alpha)$ and then there has to be some $\varphi \in \mathrm{Gal}(\mathbb{Q}[\alpha]/\mathbb{Q})$ such that $\varphi(\alpha) = \sqrt{2+\sqrt{2}}$ then it is easy to check $\varphi^k, k = 0, 1, 2, 3$ are distinct with $\varphi^4 = id$ and hence $\text{Gal}(\mathbb{Q}[\alpha]/\mathbb{Q}) = D_2$.

Problem.3

Let $E \supset \mathbb{Q}$ be a degree four extension. Show that it is impossible for it to have exactly two intermediate fields $\mathbb{Q} \subsetneq M \subsetneq E$.

Sol.

Assume $\alpha \in M$ and then there are a basis $\{e_i\}_{i=1}^4$ of E such that $e_1 = a$, then we know $[E : \mathbb{Q}[a]][\mathbb{Q}[a] : \mathbb{Q}] = 4$ and hence the minimal polynomial of a can be only have degree of $1, 2$ or 4. Let M_1, M_2 be two intermediate extensions and they may only have elements with minimal polynomials of degree 2 and 1, and at least one element with minimal polynomial of degree 2, or M_i will have the same degree with E or $\mathbb{Q}$, which hence a contradiction. Assume $\alpha \in M_1, \beta \in M_2$ with α, β have minimal polynomial of degree 2, then we know $\{1, \alpha\}, \{1, \beta\}$ can be relatively bases of M_1, M_2 and hence $\alpha \neq \beta$. Assume $(x + p)^2 - q, x(x + m)^2 - n, p, q, m, n \in \mathbb{Q}$ are relatively the minimal polynomials of α and β, we will know $(\alpha+p)(\beta+m)^2 = qn$. If $qn = r^2$ for some rational number r, then we know $(\alpha+p)^2(\beta+m)^2 = r^2$ and then $(\alpha + p)(\beta + m) = \pm r$ which means $b \in M_1$ and then $M_2 \subset M_1$, similarly $M_1 \subset M_2$ which is a contradiction, so $\gamma := (\alpha + p)(\beta + m)$ is a root of $x^2 - qn$ which is irreducible in $\mathbb{Q}[X]$. If $\mathbb{Q}[\gamma] = M_1$, then we know $s\alpha + t = \alpha\beta + p\beta + m\alpha + pm$ and hence $\beta(\alpha + p) \in M_1$ and hence $\beta \in M_1$ which is a contradiction. Similarly $\mathbb{Q}[\gamma] \neq M_2$ and there is a contradiction and we are done.

Problem.4

Let $n > 1$, and set $E = \mathbb{C}(x)$ and $F = \mathbb{R}(x^n)$. Prove that $E \supset F$ is a finite Galois extension and find its Galois group.

Sol.

Assume $\phi : x \mapsto e^{i2\pi/n}$ and $\varphi(\sum_{i=0}^{n} c_i x^i) = \sum_{i=0}^{n} \overline{c_i} x^i$. ϕ, φ are easy to be checked isomorphisms on $\mathbb{C}[x]$ and hence they induce isomorphisms on $\mathbb{C}(x)$, which can be seen by that ϕ, φ are obviously surjection and if $\phi(a/b) = \phi(a)/\phi(b) = 0$, then $\phi(a) = 0$ which means $a = 0$ and we know ϕ is injection, the same for φ. Let $G = [\phi, \varphi]$ and notice that $\mathbb{R}(x^n)$ is a subfield of E^G. Notice $\mathbb{C}(x) = \mathbb{R}(x)[i]$ and $\mathbb{R}(x) = \mathbb{R}(x^n)[x]$ where $X^2 + 1$ has a root i and $Y^n - x^n$ has a root x. $X^2 + 1$ is irreducible in $\mathbb{R}(x)[X]$ or i will be in $\mathbb{R}(x)$ which is a contradcition. $Y^n - x^n$ should be irreducible in $\mathbb{R}(x^n)[Y]$ or there should be some $g \in \mathbb{R}(x^n)[Y]$ with degree less than n such that $g(x) = 0$, in particular, $f_0 + f_1 x + \cdots + f_k x^k = 0$ for some $f_i \in \mathbb{R}(x^n)$, we may assume $f_i \in \mathbb{R}[x^n]$ by multiplying the product of all the denominators of f_i and then $f_i(0) = 0$, then we know $x^n | (f_0 + f_1 x + \cdots + f_k x^k)$ and we may use the induction to see that $f_i = 0$. Now we have $[E : F] = [E : \mathbb{R}(x)][\mathbb{R}(x^n) : F] = 2n$. However $[E : F] = [E : E^G][E^G : F]$ and hence $F = E^G$, so E is Galois over F. We claim that $G \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ since $\phi\varphi = \varphi\phi$ and the isomorphism is easy to be checked.

Problem.5

Let $E \supset F$ be a Galois extension such that $\mathrm{Gal}(E/F) \cong S_5$. Prove that E is the splitting field of a degree five polynomial over F.

Sol.

Firstly we know $[E : F] = 5!$ and assume $M = E^{S_4}$, then we have $[E^{S_4} : F] = 5$ and then we may consider $\alpha \in E^{S_4} - F$ with a minimal polynomial, whose degree can be only a factor of 5 and hence 5. Let E' the splitting field of the minimal polynomial of α. So we know $1, \alpha, \alpha^2, \alpha^3, \alpha^4$ form a basis of E^{S_4} and hence E'/E^{S_4} Galois, which is from E is Galois, so separable and hence the minimal polynomial of α separable and hence E' is Galois over F. So E' is normal and hence $\mathrm{Gal}(E/E')$ is normal, which means it should be A_5 or $\{id\}$ only, however $[E : E'] \leq 5!/[E' : F] \leq 24$ and hence it will be $\{id\}$ and we know $E = E'$.

Problem.6

Let $E \supset F$ be a finite Galois extension, and suppose $f(x) \in F[x]$ is an irreducible polynomial. Let $f(x) = f_1(x)f_2(x) \cdots f_k(x)$ be the factorization of $f(x)$ in $E[x]$. Prove that all polynomials f_i have the same degree, and that $k|[E : F]$.

Sol.

Assume ϕ is any element in $\mathrm{Gal}(E/F)$ and let ϕg to be the polynomila with ϕ acts on each coeeficient of g. We have $f = \phi f = \prod_{i=1}^{k} \phi f_i$. We know there is always some ϕ_i such that $\phi_i f_i = f_j$ for some $f_j \neq i$ or $f_i \in F[X]$ which is a contradiction since f is irreducible in $F[X]$. We denote $f_i \ f_j$ if there is ϕ such that $\phi f_i = f_j$, then we can show that   is an equivalence relation and WLOG $f_1, \cdots, f_m$ are in a same equivalence class, then $f_1 \cdots f_m$ is invariant under G and hence in $F[X]$, so $m = k$ and notice any equivalent f_i will have equal degree. $\{f_1, \cdots, f_k\} = Gf_1$ and then $k = |Gf_1|||G| = [E : F]$ and we are done.