Homework10 - MATH 742

Boren(Wells) Guan

Date: May 6, 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 A

Let K be the splitting field of the polynomial $x^4 - x^2 - 1$ over $\mathbb{Q}$. Compute the Galois group of the extension $K/\mathbb{Q}$.

Sol.

We assume $\lambda_1 = (1+\sqrt{5})/2, \lambda_2 = (1-\sqrt{5})/2$ are the roots of $x^2 - x - 1$ and hence we know $x^4 - x^2 - 1$ will have roots $\pm\sqrt{(1+\sqrt{5})/2}, \pm i\sqrt{(\sqrt{5}-1)/2}$ in $\mathbb{C}$ which means it is separable. Denote $\alpha = \sqrt{(1+\sqrt{5})/2}, \beta = \sqrt{(\sqrt{5}-1)/2}$. Since $x^4 - x^2 - 1$ is irreducible in $\mathbb{Q}[X]$, which can be seen by that if $g \in \mathbb{Q}[X]$ such that $g | x^4 - x^2 - 1$, then g can only have degree of 2 since it is easy to check $x^4 - x^2 - 1$ does not have rational root. And then we know $g \in \mathbb{Z}[X]$ by Gauss Lemma, which means there are two integers m, h such that $(x^2 + mx - 1)(x^2 + nx + 1) = x^4 - x^2 - 1$ which will induce a contradiction since $m^2 = -1$. So $\mathbb{Q}[\alpha] \cong \mathbb{Q}/(x^4 - x^2 - 1)$ and notice that $K = \mathbb{Q}[\alpha, i]$ and since $x^2 + 1$ is easy to be checked irreducible in $\mathbb{Q}[\alpha]$ and then we may know

$$[K : \mathbb{Q}] = [K : \mathbb{Q}[\alpha]][\mathbb{Q}[\alpha] : \mathbb{Q}] = 8$$

Now notice for any $\phi \in \mathrm{Gal}(K/\mathbb{Q})$, we have $\phi(\alpha)$ is a root of $x^4 - x^2 - 1$. Let $\sigma : \alpha \mapsto \beta, \beta \mapsto -\alpha$ and $\tau : \alpha \mapsto \beta, \beta \mapsto \alpha$ and we have $\tau^2 = id, \sigma^4 = id$ and $\tau\sigma = id, \sigma\tau\sigma\tau = id$ and it is easy to check $\mathrm{Gal}(K/\mathbb{Q}) = D_4$.

Problem B

Consider the field of rational functions $E = \mathbb{C}(x)$ and the subfield $F = \mathbb{C}(x^n) \subset E (n \geq 1)$. Show that $E \supset F$ is a finite Galois extension and find its Galois group.

Sol.

Need to show $[E : F]$ is normal, separable, and finite.

1. Separability: Obvious. Since $\mathrm{Char}(\mathbb{C}) = 0$.
2. Finiteness: Consider the algebraic extension $E[y]/(m_{x,F}(y))$, which gives precisely F. Notice that $y^n - x^n$ annihilates x, so $m_F(x) \mid y^n - x^n$, must be finite degree. So this is a finite extension.
3. Normality: we show F is a splitting field of a polynomial over E. Indeed, since $y^n - x^n$ has n distinct roots: $e^{\frac{2\pi i}{n}} x$.

Therefore, it is a Galois extension. We claim $1, x, x^2, \dots, x^{n-1}$ are linearly independent.

We first need to express the rational functions in terms of a linear combination of these elements.

Indeed, if $a_i \in \mathbb{C}(x^n)$ satisfies

$$a_0 + \cdots + a_{n-1}x^{n-1} = 0,$$

we take the least common multiplier of the denominators of $a_0, \dots, a_n$, say $d \in \mathbb{C}[x^n]$. Then,

$$a_0 d + \cdots + a_{n-1} d x^{n-1} = 0.$$

It is in $\mathbb{C}[x^n]$, hence the degree is a multiple of n. Hence, $a_i d = 0$. d is never 0, hence it has to be $a_i = 0$. Hence they are linearly independent. Consequently, we must have $y^n - x^n$ is irreducible over $\mathbb{C}(x^n)$, otherwise $\deg_F x < n$.

Clearly, $\sigma : x \to xe^{\frac{2\pi i}{n}}$ generates a group of order n. By definition, $\mathrm{Gal}(E/F) = \mathbb{Z}/n\mathbb{Z}$.

Problem C

Sol.

We still need to verify three things:

1. Separability is trivial, since $\mathrm{Char}(\mathbb{C}) = 0$.
2. Finiteness: We find the minimal polynomial of x over F, and show it has finite degree. We see
$$(x^n + x^{-n})^2 - 4 = x^{2n} + x^{-2n} - 2 \in \mathbb{C}(x).$$
Therefore, $E' = F(x^n - x^{-n}) = F[y]/(m_{x^n - x^{-n},F}(y))$ is a finite extension over F, since $m_{x^n - x^{-n},F} \mid (x^n + x^{-n})^2 - 4$. Therefore, we have $x^n \in E'$, and E/E' is finite, hence $[E : F] = [E : E'][E' : E]$ is finite.
3. Normality: Denote $\alpha = x^n + x^{-n}$. We claim that E is the splitting field of $y^{2n} - \alpha y^n + 1$. Indeed, $x^{\frac{\pi i}{n}}$ are $2n$ solutions. So it splits.

So E/F is a Galois extension.

We define the extension:

$$\sigma : x \to xe^{\frac{2\pi i}{n}}, x^n - x^{-n} \to x^n - x^{-n},$$

$$\tau : x \to x, x^n - x^{-n} \to -x^n + x^{-n}.$$

Notice that $\sigma^n = \tau^2 = \sigma\tau\sigma\tau = \mathrm{id}$, we have $\mathrm{Gal}(E/F) = D_{2n}$.

Problem D

Sol.

E/F is a Galois extension of prime degree p, hence the Galois group is $\mathbb{Z}/p\mathbb{Z}$. Let $\sigma \in \mathrm{Gal}(E/F)$. We know $\sigma^p = \mathrm{id}$. So the minimal polynomial of σ acts on E over F divides $x^p - 1$. Choose $\alpha_1, \alpha_2, \dots, \alpha_p$ such that $\sigma(\alpha_i) = \lambda_i \alpha_i$. Clearly, $\det(\sigma) = 1$. So, $\prod_{i=1}^{p} \lambda_i = 1$. We also know $\lambda_i \in F$ since σ is diagonalizable. We also know $\sigma^p(\alpha_i) = \alpha_i$, hence $\lambda_i^p = 1$. Hence, λ_i are roots of 1. Since σ is not trivial, not all λ_i are 1. So, there is a p-th primitive root of 1, say λ, which is an eigenvalue. Hence, the p-th cyclotomic extension of F is contained in F.

Then, let's pick an eigenvector α of σ. We have $\sigma(\alpha^p) = (\sigma(\alpha))^p = (\lambda\alpha)^p = \alpha^p$. So, σ fixes α^p. Since σ generates $\mathrm{Gal}(E/F)$, we have $\alpha^p \in F$. Let $a = \alpha^p$.

So, $F(\alpha)$ is a subextension of E. However, it is of degree p. Hence, we have $E = F(\alpha)$, and α satisfies $x^p - a = 0$.

By our previous calculation, every root of $x^p - a$, lies in $F(\alpha)$. Hence, $E = F(\alpha)$ is the splitting field of $x^p - a$.