Galois Theory HW04

Xianzhi

Due March 11, 2022

Exercise 5.3.9

Question 1. *Is the polynomial $X^4 - 2$ irreducible over the field $\mathbb{Q}(\sqrt{3})$?*

Soln

Assume $X^4 - 2$ is reducible over $\mathbb{Q}(\sqrt{3})$. Then $X^4 - 2$ either factor into 1 degree one factor and 1 degree three factor, or factor into 2 degree two factor (factor means polynomial).

Case 1

$X^4 - 2$ has a degree one factor in $\mathbb{Q}(\sqrt{3})$. so it has a root in $\mathbb{Q}(\sqrt{3})$. The roots of $X^4 - 2$ are

$$\sqrt[4]{2},\ i\sqrt[4]{2},\ -\sqrt[4]{2},\ -i\sqrt[4]{2}. \tag{1}$$

since $\mathbb{Q}(\sqrt{3})$ is a degree 2 extension, (Because $\sqrt{3}$ has minimal polynomial $X^2 - 3$, which is irreducible by Eisenstein,)

$$\mathbb{Q}(\sqrt[2]{3}) = \left\{a + b\sqrt[2]{3} \mid a, b \in \mathbb{Q}\right\} \subseteq \mathbb{R}, \tag{2}$$

since $i\sqrt[4]{2}, -i\sqrt[4]{2} \notin \mathbb{R}$, we conclude that they are not in $\mathbb{Q}(\sqrt[2]{3})$.
Now, observe $\sqrt[4]{2}$ and $-\sqrt[4]{2}$ has $X^4 - 2$ as their minimal polynomial over $\mathbb{Q}$, and $X^4 - 2$ is irreducible over $\mathbb{Q}$ by Eisenstein, so if $\sqrt[4]{2}$ were to be in $\mathbb{Q}(\sqrt[2]{3})$, then necessarily $\mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{Q}(\sqrt[2]{3})$, but $\mathbb{Q}(\sqrt[4]{2})$ is degree 4 extension, and $\mathbb{Q}(\sqrt[2]{3})$ is degree 2 extension, by the tower law, we have a contradiction. The argument for $-\sqrt[4]{2}$ is the same. End of Case 1.

Case 2

$X^4 - 2$ factor into 2 degree two polynomial over $\mathbb{Q}(\sqrt[2]{3})$, thus,

$$(X^2 - \sqrt{2})(X^2 + \sqrt{2}) \tag{3}$$

and $\sqrt[2]{2} \in \mathbb{Q}(\sqrt[2]{3})$.
Comment from instructor: There are other ways to factor $X^4 - 2$ as the product of two quadratic polynomials.
Since $\mathbb{Q}(\sqrt{3})$ is degree 2 extension, we could write $\sqrt{2} = a + b\sqrt{3}$ for $a, b \in \mathbb{Q}$.
So $2 = a^2 + 3b^2 + 2ab\sqrt{3}$. Thus,

$$2ab = 0 \tag{4}$$
$$2 = a^2 + 3b^2 \tag{5}$$

If $a = 0$, then $2/3 = b^2$, which implies $b = \sqrt{\frac{2}{3}}$, which is a contradiction with $b \in \mathbb{Q}$.
If $b = 0$, then $2 = a^2$ which implies $a = \sqrt{2}$, which is a contradiction with $a \in \mathbb{Q}$.
If a, b both zero, then $2 = 0$, which is a contradiction.
Thus $\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$. So $X^4 - 2$ cannot factor into 2 degree two polynomial over $\mathbb{Q}(\sqrt{3})$.
End of Case 2.

Exercise 6.4.6

Question 2. *Let L be the splitting field over $\mathbb{Q}$ of $X^5 - 2$ over $\mathbb{Q}$. Show that the Galois group $G := \Gamma(L : \mathbb{Q})$ has order 20, and G has a normal subgroup N with $|N| = 5$ such that the factor group G/N is cyclic.*

Let L be the splitting field of $X^5 - 2$ over $\mathbb{Q}$.

$$L = \mathbb{Q}(\sqrt[5]{2}, \omega) \text{ where } \omega = e^{\frac{2\pi i}{5}} \tag{6}$$

we have

$$L \subseteq \mathbb{Q}(\sqrt[5]{2}, \sqrt[5]{2}\omega, \sqrt[5]{2}\omega^2, \sqrt[5]{2}\omega^3, \sqrt[5]{2}\omega^4) \tag{7}$$

because $\sqrt[5]{2}$ is in there, and $\omega = \frac{\sqrt[5]{2}\omega}{\sqrt[5]{2}}$ is in there.

$$L \supseteq \mathbb{Q}(\sqrt[5]{2}, \sqrt[5]{2}\omega, \sqrt[5]{2}\omega^2, \sqrt[5]{2}\omega^3, \sqrt[5]{2}\omega^4) \tag{8}$$

because we can multiply $\sqrt[5]{2}$ and ω to generate the roots.
Claim: $[L : \mathbb{Q}] = 20$.
First $[\mathbb{Q}(\sqrt[5]{2} : \mathbb{Q}] = 5$ since $X^5 - 2$ has $\sqrt[5]{2}$ as a root, and $X^5 - 2$ is irreducible by Eisenstein (let $p = 2$), so $X^5 - 2$ is the minimal polynomial of $\sqrt[5]{2}$ over $\mathbb{Q}$, and its degree 5.
$[\mathbb{Q}(\omega) : \mathbb{Q}] = 4$ since ω is a root of $X^4 + X^3 + X^2 + X + 1$, so the degree of $\mathbb{Q}(\omega)$ is at most 4, since $X^5 - 1$ has 4 primitive roots of unity, the degree $[\mathbb{Q}(\omega) : \mathbb{Q}]$ is 4.
Thus, since $\mathbb{Q}(\omega)$ and $\mathbb{Q}(\sqrt[5]{2})$ are intermediate fields in L, their degree devides degree of L over $\mathbb{Q}$. so $[L : \mathbb{Q}]$ is a multiple of 20. but by previous result

$$[K(\alpha_1, \ldots, \alpha_n) : K] \leq deg_K(\alpha_1) \cdots deg_K(\alpha_n) \tag{9}$$
$$[L : \mathbb{Q}] \leq 5 \cdot 4 = 20 \tag{10}$$
$$\implies [L : \mathbb{Q}] = 20 \tag{11}$$

Exercise 6.4.7

Question 3. *Let p be an irreducible polynomial over a subfield K of $\mathbb{C}$, and denote by L the splitting field of p over K. Show that if the Galois group $\Gamma(L : K)$ is abelian (i.e. commutative), then its order equals the degree of p.*

Proof. Let p be irreducible polynomial over $K \subseteq \mathbb{C}$. Let L be the splitting field of p over K. Let α be a root of p. Let $m = m_K^\alpha$ be the minimal polynomial having α as a root over K. Then m divide p. But p is already irreducible, so we conclude that $m = p$. (We can assume p is monic, because if not, we could scale by a constant from

K to make it monic.) Since L is the splitting field of p over K, and $K \subseteq L \subseteq \mathbb{C}$, so p has no multiple roots in L, we apply the equivalence theorem to say L of K is a Galois extension. Since $\Gamma(L : K)$ is abelian, all subgroups are normal. We apply Galois correspondence.

$$\Gamma(K(\alpha) : K) \cong \Gamma(L : K)/\Gamma(L : K(\alpha)) \tag{12}$$

and $K(\alpha) : K$ is Galois extension by Galois correspondence. so $K(\alpha) : K$ is normal and separable. Thus, since we established $m_K^\alpha = p$, $K(\alpha)$ is normal, so $K(\alpha)$ contain all the roots of $m_K^\alpha = p$, so $K(\alpha) \supset L$, and since $K(\alpha) \subseteq L$, we conclude $K(\alpha) = L$. Thus,

$$|\Gamma(L : K)| = [L : K] = [K(\alpha) : K] = deg\ m_K^\alpha = deg\ p \tag{13}$$

and the first equal sign is because extension is Galois.

□

A question from HW02

Question 4. *Show number of automorphisms of a finite degree field extension divides the degree of the field extension.*

Let $K \subset L, L : K$ be a finite degree field extension. Recall

$$\Gamma(L : K) = \{g \in \Gamma(L) : g(x) = x \quad \forall x \in K\}$$
$$\text{WTS:} \quad |\Gamma(L : K)| \mid [L : K].$$

Recall Artin's theorem, let $\Gamma(L : K)$ be the finite subgroup. (Since $|\Gamma(L : K)|$ is bounded by $[L : K] < \infty$.) and

$$M = \{x \in L : \forall g \in \Gamma(L : K) : g(x) = x\}$$

so $K \subset M$, and $[L : M] = |\Gamma(L : K)|$. Thus, consider $K \subset M \subset L$,

$$[L : K] = [L : M][M : K]$$

where $[L : M] = |\Gamma(L : K)|$, so $|\Gamma(L : K)|$ divides $[L : K]$.