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

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.*

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.

$$\Gamma(K(\alpha) : K) \cong \Gamma(L : K)/\Gamma(L : K(\alpha)) \tag{1}$$

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,

$$|\Gamma(L:K)| = [L:K] = [K(\alpha):K] = deg\ m_K^\alpha = deg\ p \tag{2}$$

and the first equal sign is because extension is Galois.

$\square$

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 $[L:K]$.