Math250aHw14

Trustin Nguyen

November 30, 2023

Exercise 1: Let $a_1, \ldots, a_n$ be square-free, relatively prime integers not equal to 1 or -1. Show that $K = \mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_n})/\mathbb{Q}$ is Galois, of Galois group $(\mathbb{Z}/2)^n$. Show that if $0 \leqslant k \leqslant n$ then the number of subfield of K of degree 2^k over $\mathbb{Q}$ is the same as the number of subfields of degree 2^{n-k} and find this number.

Proof. We need to show that each extension is nontrivial in the tower:

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{a_1}) \subseteq \mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}) \subseteq \cdots \subseteq \mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, \ldots, \sqrt{a_n})$$

To show that each extension is nontrivial, we need to show that

$$\sqrt{p_n} \notin \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_{n-1}})$$

We get a basis of $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}})$ over $\mathbb{Q}$ by taking the product of any combination of the $\sqrt{p_i}$. We see that if $\sqrt{p_n} \in \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}})$, then it should be an element of the basis, which is not true, because the p_i are relatively prime.

Now we know that the intersection of each $\mathbb{Q}(\sqrt{a_i})$ pairwise is just $\mathbb{Q}$. Also $\mathbb{Q}(\sqrt{a_i})/\mathbb{Q}$ Galois. Then building $\mathbb{Q}(\sqrt{a_1}, \ldots, \sqrt{a_n})$ by taking the compositum inductively, we get that $\mathbb{Q}(\sqrt{a_1}, \ldots, a_n)$ is Galois over $\mathbb{Q}$ and that the Galois group is just the product of the Galois groups of $\mathbb{Q}(\sqrt{a_i})/\mathbb{Q}$ or $(\mathbb{Z}/2)^2$.

The number of subfields of degree 2^k over $\mathbb{Q}$ is the same as the number of subfields of degree 2^{n-k} because they correspond to the same subgroup of the Galois group. The Galois group is abelian and the number of subfields is $\binom{n}{k}$. □

Exercise 2: Let $E/\mathbb{Q}$ be the splitting field of $x^5 - 2$. Show that :

(a) $[E : \mathbb{Q}] = 20$.

Proof. We have that $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[5]{2})$ is a degree 5 extension since $\sqrt[5]{2}$ is a root of the irreducible polynomial $x^5 - 2$. We also know that $\zeta\sqrt[5]{2}, \zeta^2\sqrt[5]{2}, \zeta^3\sqrt[5]{2}, \zeta^4\sqrt[5]{2}$ are also roots that do not lie in $\mathbb{Q}(\sqrt[5]{2})$ because they are complex. So when we adjoin again $\zeta\sqrt[5]{2}$, we get $\mathbb{Q}(\sqrt[5]{2}, \zeta\sqrt[5]{2}) = \mathbb{Q}(\sqrt[5]{2}, \zeta)$. This gives all the roots and is the splitting field of $x^5 - 2$ over $\mathbb{Q}$. The degree of $[\mathbb{Q}(\sqrt[5]{2}, \zeta), \mathbb{Q}(\sqrt[5]{2})]$ is 4 because we get all the roots of $\frac{x^5-2}{x-\sqrt[5]{2}} \in \mathbb{Q}(\sqrt[5]{2})$ irreducible. So the extension is of degree

$$[E : \mathbb{Q}] = [\mathbb{Q}(\sqrt[5]{2}, \zeta) : \mathbb{Q}(\sqrt[5]{2})][\mathbb{Q}(\sqrt[5]{2}) : \mathbb{Q}] = 5 \cdot 4 = 20$$

□

(b) there is precisely 1 subfield F of E with $[E : F] = 5$, and that F is normal.

Proof. $E/\mathbb{Q}$ is a Galois extension, with $[E : \mathbb{Q}]$ the order of the Galois group. Then we have for $F = E^H$:

$$\mathbb{Q} \subseteq E^H \subseteq E$$
$$G \supseteq H \supseteq \{e\}$$

So we are looking for the subgroups of order 5. We have that the number of sylow-5 subgroups of G is 1 because there are either 1, 2, 4 groups and the number is $\equiv 1 \pmod 5$. So we have one sylow 5 group, that is normal in G. We conclude that H is normal in G. So $F \subseteq \mathbb{Q}$ is normal. There are no other order 5 subgroups of G, so there is only one intermediate field that it corresponds to with degree 5 from E/F. □

(c) the element $2^{1/5} + \zeta$ is a primitive element of $E/\mathbb{Q}$, where ζ is the 5th root of 1.

Proof. Don't know □

(d) $\mathrm{Gal}(E/\mathbb{Q})$ contains elements σ, τ of orders 5 and 4 respectively, with $\tau\sigma\tau^{-1} = \sigma^2$.

Proof. The element σ has order 5, sending $\sqrt[5]{2}$ to one of $\sqrt[5]{2}, \zeta\sqrt[5]{2}, \zeta^2\sqrt[5]{2}, \zeta^3\sqrt[5]{2}, \zeta^4\sqrt[5]{2}$. The element τ has order 4 sending ζ to any root of unity except 1. We know that the sylow 5 group is normal so

$$\tau\sigma\tau^{-1} = \sigma^i$$

Couldn't finish. □

Exercise 3: Let $K = k(x)$ be the field of rational functions in 1 variable over a field k. Show that for any $t = f/g \in K\backslash k$, with f, g relatively prime, the field extension $K/k(t)$ is finite of degree $\max(\deg f, \deg g)$. Show that any automorphism σ of K/k is determined by the image of x, and has the form

$$\sigma(X) = \frac{ax + b}{cx + d}$$

with $ad - bc \neq 0$. Show that the numbers a, b, c, d are well-defined up to a common scalar multiple, and $\mathrm{Gal}(K/k) \cong \mathrm{PGL}(2, k)$ (invertible 2×2 matrices mod scalars).

Proof. We have that

$$tg - f = 0$$

is a polynomial in $k(t)$ that kills x. It is also irreducible because. Since $t \neq 0$, we know that it is invertible, and coefficients in f, g are in k. Then we can reduce this to a monic polynomial:

$$c(g - t^{-1}f)^{-1}(g - t^{-1}f) = 0$$

So this polynomial is of degree $\max(\deg f, \deg g)$ that lies in $k(t)$ which kills x. So we take the quotient from $k(t)$ to get an extension to $k(x)$ with degree $\max(\deg f, \deg g)$.

Any automorphism fixes k, so the action of σ on x determines the action of σ on all of $k(x)$ and therefore the automorphisms of K/k. Don't know why

$$\sigma(X) = \frac{ax + b}{cx + d}$$

But if that is the case, then $\sigma(x) \notin k$. Then since either $c \neq 0$ or $d \neq 0$, we have that

- $c \neq 0$, then $\frac{a}{c}(cx + d) = ax + \frac{da}{c}$. So

$$\frac{ax + b}{ax + \dfrac{da}{c}} \notin k$$

and therefore, $\frac{da}{c} \neq b$ or $ad - bc \neq 0$.

- $d \neq 0$, then $\frac{b}{d}(cx + d) = \frac{bc}{d}x + b$. Then

$$\frac{ax + b}{\dfrac{bc}{d}x + b} \notin k$$

and therefore, $\frac{bc}{d} \neq a$ and $ad - bc \neq 0$.

Now for well-defined, suppose that

$$\frac{ax+b}{cx+d} = \frac{a'x+b'}{c'x+d'}$$

Cross multiply and we get

$$ac'x^2 + (\ldots)x + bd' = a'cx + (\ldots)x + b'd$$

Then

$$ac' = a'c \qquad bd' = b'd$$
$$\frac{a}{a'} = \frac{c}{c'} \qquad \frac{b}{b'} = \frac{d}{d'}$$

If the denominator is 0, we see that the numerator has to be 0 also and continue with that information. Now we have these ratios, and are now considering when

$$\frac{ax+b}{cx+d} = \frac{kax+k'b}{kcx+k'd}$$

Cross multiplying and considering the degree 1 terms:

$$kbcx + k'adx = kadx + k'bcx$$

Then

$$k(bc-ad) = k'(bc-ad)$$

and since $bc - ad \neq 0$, we have

$$\frac{k}{k'} = 1$$

which shows that a, b, c, d are well defined up to scaling. Then the Galois group is in bijection with matrices

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

invertible because $ad - bc \neq 0$ in $PGL(2,k)$ because it is mod scaling. □