MA3D5 Galois Theory
Sheet 8 Solutions

Peize Liu

15 Nov 2024

Exercise 8.1

Let p be a prime and ζ a primitive p-th root of unity. Let $F = \mathbb{Q}(\zeta)$ and $G = \mathrm{Gal}(F/\mathbb{Q})$.

(a) Show that G has a unique subgroup of index 2.

(b) Show that there is a unique intermediate field $\mathbb{Q} \subseteq E \subseteq F$, with $[E : \mathbb{Q}] = 2$.

(c) Show that $E = \mathbb{Q}(\sqrt{\epsilon p})$, with $\epsilon = (-1)^{(p-1)/2}$. [Hint: Show that all powers of ζ are perfect squares in E. Then show that $\left((1-\zeta)\left(1-\zeta^2\right)\cdots\left(1-\zeta^{(p-1)/2}\right)\right)^2 = \epsilon p/\zeta^k$ for some k.]

(a) We must assume that $p > 2$. $\mathbb{Q}(\zeta)/\mathbb{Q}$ is a cyclotomic extension and hence $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/p)^\times$. Since p is prime, $G \cong \mathbb{Z}/(p-1)$. Since p is odd, $m := \frac{p-1}{2}$ is a positive integer and G has a unique subgroup isomorphic to $\mathbb{Z}/m$. This is a subgroup of index 2 in G.

(b) By Galois correspondence, the subgroups of index a are in bijective correspondence with intermediate fields with degree a over $\mathbb{Q}$. It follows from (a) that there is a unique intermediate field E with $[E : \mathbb{Q}] = 2$.

(c) Let $\boldsymbol{\mu}_p = \left\{\alpha \in F \mid \exists\, k \in \mathbb{Z},\ \alpha^k = 1\right\}$ be the group of roots of unity of F. We know that $\boldsymbol{\mu}_p \cong \mathbb{Z}/p$ is a cyclic group generated by $\zeta \in F$. Since p is prime, every non-identity element of $\boldsymbol{\mu}_p$ is a generator of $\boldsymbol{\mu}_p$. In particular ζ^2 also generates $\boldsymbol{\mu}_p$. That is, every $\alpha = \zeta^i \in \boldsymbol{\mu}_p$ is of the form $\zeta^i = (\zeta^2)^j = (\zeta^j)^2$ for some j.

Recall that the minimal polynomial of ζ over $\mathbb{Q}$ is the p-th cyclotomic polynomial:

$$\Phi_p(x) = x^{p-1} + \cdots + x + 1,$$

which splits over F as $\Phi_p(x) = \prod_{i=0}^{p-1}(x - \zeta^i)$. Evaluate the polynomial at $x = 1$:

$$p = \prod_{i=1}^{p-1}(1-\zeta^i) = \prod_{i=1}^{(p-1)/2}(1-\zeta^i)(1-\zeta^{-i}) = \prod_{i=1}^{(p-1)/2}(1-\zeta^i)^2(-\zeta^{-i}).$$

Hence

$$\epsilon p = (-1)^{\frac{p-1}{2}} p = \zeta^k \left(\prod_{i=1}^{(p-1)/2}(1-\zeta^i)\right)^2,$$

where $k = -\sum_{i=1}^{(p-1)/2} i$. Since ζ^k is a perfect square, $\zeta^k = \zeta^{2k'}$ for some $k' \in \mathbb{Z}$. It follows that

$$\sqrt{\epsilon p} = \zeta^{k'} \prod_{i=1}^{(p-1)/2}(1-\zeta^i) \in F.$$

Since $\sqrt{\epsilon p}$ has minimal polynomial $x^2 - \epsilon p$ over $\mathbb{Q}$, we have that $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{\epsilon p}) \subseteq F$ and $[\mathbb{Q}(\sqrt{\epsilon p}) : \mathbb{Q}] = 2$. By uniqueness, $E = \mathbb{Q}(\sqrt{\epsilon p})$.

Exercise 8.2

Let L/K be a Galois extension and $G = \mathrm{Gal}(L/K)$. Define $N : L \longrightarrow L$, by $N(a) = \prod_{\sigma \in G} \sigma(a)$. Prove that $N(a) \in K$ for all $a \in L$. Prove that $N(a) = a^{[L:K]}$ if $a \in K$.

For $\tau \in G$, we have

$$\tau(N(a)) = \prod_{\sigma \in G} \tau\sigma(a) = \prod_{\sigma' \in G} \sigma'(a) = N(a),$$

where we used the fact that left multiplication of τ defines a group automorphism of G. In particular $N(a) \in L^G$ for all $a \in L$. Since L/K is Galois and $G = \mathrm{Gal}(L/K)$, we have $L^G = K$ and hence $a \in K$.

For $a \in K$, we have $\sigma(a) = a$ for all $\sigma \in G$. Hence

$$N(a) = \prod_{\sigma \in G} a = a^{|G|} = a^{[L:K]}.$$

Remark. For $\alpha \in L$, $N(\alpha) \in K$ is called the **norm** of α. Similarly we can define the **trace** of α to be $T(\alpha) = \sum_{\sigma \in G} \sigma(\alpha) \in K$. There is an alternative way to look at the norm and trace. Fix a K-basis $\{u_1, \ldots, u_n\}$ of L. The K-linear map $L \longrightarrow L$ given by multiplication by α has matrix $A = (a_{ij})$ with respect to this basis. That is, $\alpha(u_i) = \sum_{j=1}^n a_{ij} u_j$. Then the norm and trace of α are given by

$$N(\alpha) = \det A; \qquad T(\alpha) = \operatorname{tr} A = \sum_{i=1}^n a_{ii}.$$

Exercise 8.3

Let $L = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ for primes p, q. Find, with justification, $\alpha \in L$, such that $L = \mathbb{Q}(\alpha)$.

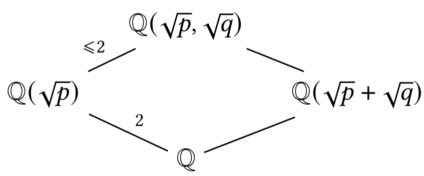
For $p = q$, we can trivially take $\alpha = \sqrt{p}$. So we assume that $p \neq q$. We claim that $L = \mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\sqrt{p} + \sqrt{q})$. It is clear that $\mathbb{Q}(\sqrt{p}, \sqrt{q}) \supseteq \mathbb{Q}(\sqrt{p} + \sqrt{q})$. To show the reverse inclusion,

- you could simply observe that

  $$\sqrt{p} = \frac{(\sqrt{p} + \sqrt{q})^3 - (q + 3p)(\sqrt{p} + \sqrt{q})}{2(q - p)} \in \mathbb{Q}(\sqrt{p}+\sqrt{q}); \qquad \sqrt{q} = \frac{(\sqrt{p} + \sqrt{q})^3 - (p + 3q)(\sqrt{p} + \sqrt{q})}{2(p - q)} \in \mathbb{Q}(\sqrt{p}+\sqrt{q}).$$

  which shows $\mathbb{Q}(\sqrt{p}, \sqrt{q}) \subseteq \mathbb{Q}(\sqrt{p} + \sqrt{q})$ directly.

- If the above method is too tricky, we can work alternatively as follows. Consider the tower of extensions



  To show that $\mathbb{Q}(\sqrt{p}, \sqrt{q}) = \mathbb{Q}(\sqrt{p} + \sqrt{q})$. It suffices to show that $[\mathbb{Q}(\sqrt{p} + \sqrt{q}) : \mathbb{Q}] > 2$. Suppose that there exists $p(x) = x^2 + bx + c \in \mathbb{Q}[x]$ such that $p(\alpha) = 0$. Then

  $$p(\alpha) = p + q + 2\sqrt{pq} + b(\sqrt{p} + \sqrt{q}) + c = 0.$$

  Hence $-b(\sqrt{p} + \sqrt{q}) = p + q + 2\sqrt{pq} + c$. Taking the square, we have

  $$b^2(p + q + 2\sqrt{pq}) = (p + q + c)^2 + 4pq + 4(p + q + c)\sqrt{pq}.$$

Since $\sqrt{pq} \notin \mathbb{Q}$, 1 and $\sqrt{pq}$ are $\mathbb{Q}$-linearly independent, and hence we must have

$$\begin{cases} b^2 = 2(p+q+c) \\ b^2(p+q) = (p+q+c)^2 + 4pq \end{cases}.$$

Combining the two equations, we have $2(p+q+c)(p+q) = (p+q+c)^2 + 4pq$. After simplifying we get $(p-q)^2 = c^2$. Hence $c = p - q$ or $q - p$. Plug this into the first equation, we have either $b = 2\sqrt{p}$ or $2\sqrt{q}$. But both p, q are primes, this is a contradiction to $b \in \mathbb{Q}$.