Topics in Algebra solution

Sung Jong Lee, lovekrand.github.io

December 8, 2020

Problems in Section 5.6.

† **Remark** As Herstein makes use of right-multiplication notation for the automorphism in this section(he usually used left-multiplication notation), we shall follow the same method as of his here.

1. If K is a field and S a set of automorphisms of K, prove that the fixed field of S and that of $\overline{S}$(the subgroup of the group of all automorphisms of K generated by S) are identical.

Proof. Let K_S and $K_{\overline{S}}$ denote the fixed field of S and $\overline{S}$ respectively. Since $S \subset \overline{S}$, it is clear that $K_{\overline{S}} \subset K_S$. We show that the opposite inclusion also holds. Choose $x \in K_S$. For any arbitrary $\sigma \in \overline{S}$, σ is of the form

$$\sigma = \sigma_1^{i_1}\sigma_2^{i_2}\cdots\sigma_k^{i_k}, \quad \sigma_j \in S, \quad i_j \in \mathbb{Z}\,.$$

Since $x \in K_S$, $\sigma_j^{i_j}(x) = x$ for each $j = 1, 2, \cdots k$. Therefore, $\sigma(x) = \sigma_1^{i_1}\sigma_2^{i_2}\cdots\sigma_k^{i_k}(x) = x$. Hence, $x \in K_{\overline{S}}$. Combining the results, we have $K_S = K_{\overline{S}}$. □

2. Prove Lemma 5.6.2.

Proof. Let $\sigma, \tau \in G(K, F)$. Choose $a \in F$. Recall that the composition of automorphism yields again an automorphism. Also, $\sigma\tau(a) = \sigma(a) = a$. Hence, $G(K, F)$ is closed under functional composition(multiplication). No wonder, associativity, existence of identity and inverse elements are naturally induced from $\mathcal{A}(K)$. Therefore, $G(K, F)$ is a subgroup of $\mathcal{A}(K)$. □

3. Using the Eisenstein criterion, prove that $x^4 + x^3 + x^2 + x + 1$ is irreducible over the field of rational numbers.

Proof. Refer the Problem 3, Section 3.10. □

4. In Example 5.6.3, prove that each mapping σ_i defined is an automorphism of $F_0(w)$.

Proof. We can prove this either by direct calculation or using some theorems in Galois theory. We take the later one. Given mapping $\sigma_i : F_0(w) \to F_0(w)$ is defined in a way that it fixes F and sends a root w of $f(x) = x^4 + x^3 + x^2 + x + 1$ into another root w^i of $f(x)$. Note that $f(x)$ is irreuducible in F_0. Hence applying Lemma 5.6.3, there exists an automorphism in $F_0(w)$ which fixes F and sending w into w^i, where w is a root of $f(x)$. But such obtained automorphism is in fact, coincides with σ_i. Thus, each σ_i are automorphisms. □

5. In Example 5.6.3, prove that the fixed field of $F_0(w)$ under $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ is precisely F_0.

Proof. We can prove this either by direct calculation or using some theorems in Galois theory. We take the later one. With the same notations in Problem 4, we conclude that $o(G(F_0(w), F)) \geq 4$. Now by Fundamental theorem of Galois theory, $F_0(W)$ being splitting field of $f(x)$, $o(G(F_0(w), F_0)) = [F_0(w) : F] = \phi(5) = 4$. Since we have already exhibited 4 automorphisms $\sigma_i \in G(F_0(w), F_0)$, fixed field of $F_0(w)$ under σ_i is precisely F_0. □

6. Prove directly that any automorphism of K must leave every rational number fixed.

Proof. We give additional condition that K is a field of characteristic 0. Now refer Problem 12, Section 5.3. Here we can find that from the condition $\sigma(1) = 1$, we can derive that $\sigma\left(\frac{n}{m}\right) = \frac{n}{m}$ for every $n, m \neq 0 \in \mathbb{Q}$. □

7. Prove that a symmetric polynomial in $x_1, \cdots, x_n$ is a polynomial in the elementary symmetric functions in $x_1, \cdots x_n$.

Proof. Proof using lexicographic order can be found here: https://proofwiki.org/wiki/Fundamental_Theorem_of_Symmetric_Polynomials □

8. Express the following as polynomials in the elementary symmetric functions in x_1, x_2, x_3:

a) $x_1^2 + x_2^2 + x_3^2$.

Solution. Note that $x_1^2 + x_2^2 + x_3^2 = (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_2x_3 + x_1x_3)$. Since $a_1 = x_1 + x_2 + x_3$ and $a_2 = x_1x_2 + x_2x_3 + x_1x_3$,

$$x_1^2 + x_2^2 + x_3^2 = a_1^2 - 2a_2.$$

□

b) $x_1^3 + x_2^3 + x_3^3$.

Solution. Recall the identity

$$x_1^3 + x_2^3 + x_3^3 - 3x_1x_2x_3 = (x_1 + x_2 + x_3)(x_1^2 + x_2^2 + x_3^2 - x_1x_2 - x_2x_3 - x_1x_3).$$

Consequently, we have

$$\begin{aligned} x_1^3 + x_2^3 + x_3^3 &= (x_1 + x_2 + x_3)(x_1^2 + x_2^2 + x_3^2 - x_1x_2 - x_2x_3 - x_1x_3) + 3x_1x_2x_3 \\ &= a_1((a_1^2 - 2a_2) - (a_2)) + 3a_3 \\ &= a_1^3 - 3a_1a_2 + 3a_3. \end{aligned}$$

□

c) $(x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2$.

Solution. Let $L_{xy} = x_1^x x_2^y + x_2^x x_3^y + x_3^x x_1^y$. Note that

$$(L_{12} - L_{21})^2 = (L_{12} + L_{21})^2 - 4L_{12}L_{21}.$$

Observe that

$$\begin{aligned} &(x_1x_2)^3 + (x_2x_3)^3 + (x_1x_3)^3 \\ &\quad= (x_1x_2 + x_2x_3 + x_1x_3)((x_1x_2 + x_2x_3 + x_1x_3)^2 - 3x_1x_2x_3(x_1 + x_2 + x_3)) \\ &\qquad+ 3(x_1x_2x_3)^2 \\ &\quad= a_2^3 - 3a_1a_2a_3 + 3a_3^2, \end{aligned}$$

$$\begin{aligned} L_{12}L_{21} &= \left[(x_1x_2)^3 + (x_2x_3)^3 + (x_1x_3)^2\right] + \left[(x_1x_2x_3)(x_1^3 + x_2^3 + x_3^3)\right] + 3(x_1x_2x_3)^2 \\ &= a_2^3 - 3a_1a_2a_3 + 3a_3^2 + a_3(a_1^3 - 3a_1a_2 + 3a_3) + 3a_3^2 \\ &= a_2^3 + a_1^3a_3 + 9a_3^2 - 6a_1a_2a_3, \end{aligned}$$

$$\begin{aligned} L_{12} + L_{21} &= (x_1x_2 + x_2x_3 + x_1x_3)(x_1 + x_2 + x_3) - 3x_1x_2x_3 \\ &= a_1a_2 - 3a_3, \end{aligned}$$

so that

$$\begin{aligned} &(x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2 \\ &\quad= (L_{12} - L_{21})^2 = (L_{12} + L_{21})^2 - 4L_{12}L_{21} \\ &\quad= (a_1a_2 - 3a_3)^2 - 4(a_2^3 + a_1^3a_3 + 9a_3^2 - 6a_1a_2a_3) \\ &\quad= -4a_1^3a_3 + (a_1a_2)^2 + 18a_1a_2a_3 - 4a_2^3 - 27a_3^2. \end{aligned}$$

Therefore, $(x_1 - x_2)^2(x_1 - x_3)^2(x_2 - x_3)^2 = -4a_1^3a_3 + (a_1a_2)^2 + 18a_1a_2a_3 - 4a_2^3 - 27a_3^2$. □

9. If $\alpha_1, \alpha_2, \alpha_3$ are the roots of the cubic polynomial $x^3 + 7x^2 - 8x + 3$, find the cubic polynomial whose roots are
a) $\alpha_1^2, \alpha_2^2, \alpha_3^2$.

Solution. We have

$$\alpha_1 + \alpha_2 + \alpha_3 = -7, \quad \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3 = -8, \quad \alpha_1\alpha_2\alpha_3 = -3.$$

Thus,

$$\begin{aligned}
\alpha_1^2 + \alpha_2^2 + \alpha_3^2 &= (\alpha_1 + \alpha_2 + \alpha_3)^2 - 2(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3) \\
&= 49 + 16 = 65, \\
\alpha_1^2\alpha_2^2 + \alpha_2^2\alpha_3^2 + \alpha_1^2\alpha_3^2 &= (\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3)^2 - \alpha_1\alpha_2\alpha_3(\alpha_1 + \alpha_2 + \alpha_3) \\
&= 64 - 21 = 43, \\
\alpha_1^2\alpha_2^2\alpha_3^2 &= 9
\end{aligned}$$

so that $x^3 - 65x + 43x - 9$ is the required polynomial, whose roots are $\alpha_1^2, \alpha_2^2, \alpha_3^2$. □

b) $\dfrac{1}{\alpha_1}, \dfrac{1}{\alpha_2}, \dfrac{1}{\alpha_3}$.

Solution. By some computations we have

$$\begin{aligned}
\frac{1}{\alpha_1} + \frac{1}{\alpha_2} + \frac{1}{\alpha_3} &= \frac{\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3}{\alpha_1\alpha_2\alpha_3} = \frac{8}{3}, \\
\frac{1}{\alpha_1}\frac{1}{\alpha_2} + \frac{1}{\alpha_2}\frac{1}{\alpha_3} + \frac{1}{\alpha_1}\frac{1}{\alpha_3} &= \frac{\alpha_1 + \alpha_2 + \alpha_3}{\alpha_1\alpha_2\alpha_3} = \frac{7}{3}, \\
\frac{1}{\alpha_1}\frac{1}{\alpha_2}\frac{1}{\alpha_3} &= -\frac{1}{3}
\end{aligned}$$

so that $x^3 - \dfrac{8}{3}x^2 + \dfrac{7}{3}x + \dfrac{1}{3}$ is the required polynomial, whose roots are $\dfrac{1}{\alpha_1}, \dfrac{1}{\alpha_2}, \dfrac{1}{\alpha_3}$. □

c) $\alpha_1^3, \alpha_2^3, \alpha_3^3$.

Solution. By some computations we have

$$\begin{aligned}
\alpha_1^3 + \alpha_2^3 + \alpha_3^3 &= (\alpha_1 + \alpha_2 + \alpha_3)^3 - 3(\alpha_1 + \alpha_2 + \alpha_3)(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3) + 3\alpha_1\alpha_2\alpha_3 \\
&= (-7)^3 - 3(-7)(-8) + 3(-3) = -520, \\
\alpha_1^3\alpha_2^3 + \alpha_2^3\alpha_3^3 + \alpha_1^3\alpha_3^3 &= (\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3)^3 - 3(\alpha_1 + \alpha_2 + \alpha_3)(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_1\alpha_3)(\alpha_1\alpha_2\alpha_3) \\
&\quad + 3(\alpha_1\alpha_2\alpha_3)^2 \\
&= (-8)^3 - 3(-7)(-8)(-3) + (-3)^2 = 1, \\
\alpha_1^3\alpha_2^3\alpha_3^3 &= (-3)^3 = -27
\end{aligned}$$

so that $x^3 + 520x^2 - x + 27$ is the required polynomial, whose roots are $\alpha_1^3, \alpha_2^3, \alpha_3^3$. □

10. Prove Newtons's identities, namely, if $\alpha_1, \alpha_2, \cdots, \alpha_n$ are the roots of $f(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n$ and if $s_k = \alpha_1^k + \alpha_2^k + \cdots \alpha_n^k$ then
a) $s_k + a_1 s_{k-1} + a_2 s_{k-2} + \cdots a_{k-1} s_1 + k a_k = 0$ if $k = 1, 2, \cdots, n$.

Proof. First we prove the case when $k = n$. Using that α_i are the roots of $f(x)$,

$$\begin{gathered}
\alpha_1^n + a_1 \alpha_1^{n-1} + a_2 \alpha_1^{n-2} + \cdots a_{n-1} \alpha_1 + a_n = 0, \\
\alpha_2^n + a_1 \alpha_2^{n-1} + a_2 \alpha_2^{n-2} + \cdots a_{n-1} \alpha_2 + a_n = 0, \\
\vdots \\
\alpha_n^n + a_1 \alpha_n^{n-1} + a_2 \alpha_n^{n-2} + \cdots a_{n-1} \alpha_n + a_n = 0,
\end{gathered}$$

and by combining under a_i, the above equations yields the identity

$$s_n + a_1 s_{n-1} + a_2 s_{n-2} + \cdots a_{n-1} s_1 + n a_n = 0.$$

Now we consider when $k < n$. Let $S_k(\alpha_1, \alpha_2, \cdots, \alpha_n) = s_k + a_1 s_{k-1} + a_2 s_{k-2} + \cdots a_{k-1} s_1 + k a_k$. Since the degree of $S_k(\alpha_1, \alpha_2, \cdots, \alpha_n)$ is at most k, we can delete at least $n - k$ roots α_i from the monomial and not change its value. This is, in fact, equivalent to that of considering $n - k$ roots to be zero, so that the problem is reduced to the case of handling the polynomial f of degree k. But we have already proved that the identity holds for the case with polynomial f with degree k and k roots. Hence, $S_k(\alpha_1, \alpha_2, \cdots, \alpha_n) = 0$ for $k < n$. □

b) $s_k + a_1 s_{k-1} + a_2 s_{k-2} + \cdots a_n s_{k-n} = 0$ for $k > n$.

Proof. At the above problem, we have essentially deleted the roots(set to zero) to obtained the wanted results. In this case, we do in reverse. We shall now add some additional roots. In particular, we add some $k - n$ zeros to the polynomial f. Consequently, our new polynomial would be of the form $f(x) = \prod_{i=1}^{n} (x - \alpha_i) x^{k-n}$. Denote $\alpha_{k+1} = \cdots = \alpha_n = 0$. Then, we have

$$a_i = (-1)^i \sum_{j_1 < \cdots < j_i} \alpha_{j_1} \alpha_{j_2} \cdots \alpha_{j_i}$$

so that any term in which $\alpha_{k+1}, \cdots, \alpha_n = 0$ appears yields 0. Now this gives the required result of

$$s_k + a_1 s_{k-1} + a_2 s_{k-2} + \cdots a_n s_{k-n} = 0.$$

□

c) For $n = 5$, apply part *a*) to determine s_2, s_3, s_4, and s_5.

Solution. From part a) we have

$$\begin{aligned}
&s_1 + a_1 = 0,\\
&s_2 + a_1 s_1 + 2a_2 = 0,\\
&s_3 + a_1 s_2 + a_2 s_1 + 3a_3 = 0,\\
&s_4 + a_1 s_3 + a_2 s_2 + a_3 s_1 + 4a_4 = 0,\\
&s_5 + a_1 s_4 + a_2 s_3 + a_3 s_2 + a_4 s_1 + 5a_5 = 0.
\end{aligned}$$

Solving the above linear system of equations, we obtain

$$\begin{aligned}
s_1 &= -a_1,\\
s_2 &= a_1^2 - 2a_2,\\
s_3 &= -a_1^3 + 3a_1 a_2 - 3a_3,\\
s_4 &= a_1^4 - 4a_1^2 a_2 + 2a_1 a_2 + 4a_1 a_3 - 4a_4,\\
s_5 &= -a_1^5 + 5a_1^3 a_2 - 5a_1^2 a_3 - 2a_1^2 a_2 - 3a_1 a_2^2 + 5a_1 a_4 + 5a_2 a_3 - 5a_5.
\end{aligned}$$

□

11. Prove that the elementary symmetric functions in $x_1, \cdots, x_n$ are indeed symmetric functions in $x_1, \cdots, x_n$.

Proof. Let $f(t) = t^n - a_1 t^{n-1} + a_2 t^{n-2} + \cdots + (-1)^n a_n$ where a_i denote the symmetric functions in $x_1, \cdots, x_n$. Then we have

$$f(t) = \prod_{i=1}^{n} (t - x_i).$$

Consider any permutation $\sigma \in S_n$. We can make S_n act of $F(x_1, \cdots, x_n)$ naturally by sending $r(x_1, x_2, \cdots, x_n)$ to $r(x_{\sigma(1)}, x_{\sigma(2)}, \cdots x_{\sigma(n)})$. Identify such mapping with σ, we have

$$\sigma(f(t)) = \prod_{i=1}^{n} (t - x_{\sigma(i)}) = f(t).$$

This implies that elementary symmetric functions a_i remain unchanged under any permutation $\sigma \in S_n$. Hence, they are indeed symmetric functions in $x_1, \cdots, x_n$. □

12. If $p(x) = x^n - 1$ prove that the Galois group of $p(x)$ over the field of rational numbers is abelian.

Proof. Let w denote the standard primitive nth root of unity. Then the set of all roots of $p(x)$ over some extension where it splits, is exactly (w). Note that this is a cyclic group of order n under multiplication. Thus, we know that the splitting field of $p(x)$ over $\mathbb{Q}$ is $\mathbb{Q}(w)$. Let $\sigma, \tau \in G(\mathbb{Q}(w), \mathbb{Q})$. Recall that such σ and τ must take a root of $p(x)$ into a root of $p(x)$ in $\mathbb{Q}(w)$. So we assume that $\sigma(w) = w^k$, $\tau(w) = w^j$ for some integers k and j. Consequently,

$$\sigma \cdot \tau(w) = \sigma(w^j) = w^{kj} = \tau(w^k) = \tau \cdot \sigma(w).$$

Hence, σ and τ commutes over $\mathbb{Q}(w)$. Therefore, $G(\mathbb{Q}(w), \mathbb{Q})$ is abelian. □

13. a) Prove that there are $\phi(n)$ primitive nth roots of unity where $\phi(n)$ is the Euler ϕ-function.

Proof. Refer the Problem 28, Section 2.4-2.5. □

b) If w is a primitive nth root of unity prove that $F_0(w)$ is the splitting field of $x^n - 1$ over F_0(and so is a normal extension of F_0).

Proof. Refer the argument made in Problem 12. □

c) If $w_1, \cdots, w_{\phi(n)}$ are the $\phi(n)$ primitive nth roots of unity, prove that any automorphism of $F_0(w)$ takes w_1 into some w_i.

Proof. Note that any automorphism of $F_0(w)$, which is a splitting field of $x^n - 1$ over F_0, must permute roots of $x^n - 1$. Since the order of w_1 is n, and any automorphism over a group must preserve the order of the element, w_1 is mapped to another primitive nth root of unity. □

d) Prove that $[F_0(w) : F_0] \leq \phi(n)$.

Proof. We continue using the same notation. Recall that any automorphism in $G(F_0(w), F_0)$ is determined by how w is mapped. Since each w is mapped to one of primitive nth roots of unity, there can be at most $\phi(n)$ distinct automorphisms. Now by the Galois theory, $[F_0(w) : F_0] = o(G(F_0(w), F_0)) \leq \phi(n)$. □

14. The notation is as in Problem 13.
a) Prove that there is an automorphism σ_i of $F_0(w_1)$ which takes w_1 into w_i.

Proof. Let $w_1 = e^{\frac{2\pi i}{n}}$. We can assign each w_k as

$$w_k = e^{\frac{2k\pi i}{n}}, \quad 1 \leq k \leq n, \quad (k, n) = 1.$$

Now define a mapping $\sigma_k : F_0(w_1) \to F_0(w_1)$, which fixes F_0 and $\sigma(w_1) = w_1^k$. Then σ_k is indeed an autormophism, which takes w_1 into $w_1^k = w_k$. □

b) Prove the polynomial $p_n(x) = (x - w_1)(x - w_2)\cdots(x - w_{\phi(n)})$ has rational coefficients. (The polynomial $p_n(x)$ is called the nth cyclotomic polynomial).

Proof. Refer the Problem 8, Section 5.3. □

c) Prove that, in fact, the coefficients of $p_n(x)$ are integers.

Proof. Refer the Problem 8, Section 5.3. Or it is a direct application of Gauss Lemma on the Problem 14 b). □

15. Use the results of Problems 13 and 14 to prove that $p_n(x)$ is irreducible over F_0 for all $n \geq 1$.

Proof. Refer the Problem 8, Section 5.3. □

16. For $n = 3, 4, 6$, and 8, calculate $p_n(x)$ explicitly, show that it has integer coefficients and prove directly that it is irreducible over F_0.

Proof. We have the following cases:

- Let $n = 3$. Then $p_3(x) = x^2 + x + 1$. Since 3 being prime, $p_3(x)$ is irreducible over F_0.
- Let $n = 4$. Then $p_4(x) = x^2 + 1$. Since there is not rational whose square is -1, it is irreducible over F_0.
- Let $n = 6$. Then $p_6(x) = x^2 - x + 1$. By calculating discriminant, $\Delta = (-1)^2 - 4 = -5 < 0$. Hence $p_6(x)$ has no rational roots. So it is irreducible over F_0.
- Let $n = 8$. Then $p_8(x) = x^4 + 1$. Substitute $x + 1$ to x and we have $p_8(x + 1) = x^4 + 4x^3 + 6x^2 + 4x + 2$. Applying Eisenstein's criterion, we conclude that $p_8(x + 1)$ is irreducible in F_0 and so does $p_8(x)$.

□

17. a) Prove that the Galois group of $x^3 - 2$ over F_0 is isomorphic to S_3, the symmetric group of degree 3.

Proof. Note that $x^3 - 2$ is irreducible in F_0 and hence, the Galois group of $x^3 - 2$ over F_0 has at most 6 permutations of its three roots. Let w denote the standard primitive 3rd root of unity. We know that $2^{\frac{1}{3}}, w2^{\frac{1}{3}}, w^2 2^{\frac{1}{3}}$ are the roots of $x^3 - 2$ and hence, $F_0(2^{\frac{1}{3}}, w)$ is the splitting field of $x^3 - 2$ over F_0, of degree 6. Since $o(G(F_0(2^{\frac{1}{3}}, w), F_0)) = [F_0(2^{\frac{1}{3}}, w) : F_0] = 6$, we must have all the 6 permutations of three roots of $x^3 - 2$ as the elements of Galois group. Hence, $G(F_0(2^{\frac{1}{3}}, w), F_0) \simeq S_3$. □

b) Find the splitting field, K, of $x^3 - 2$ over F_0.

Proof. Refer the above Problem 17 a). □

c) For every subgroup H of S_3 find K_H and check the correspondence given in Theorem 5.6.6.

Proof. Let $\sigma_i \in G(K, F_0)$. Then we can identify each σ_i with those in $S_3 = (\sigma, \tau)$, $\sigma^3 = id, \tau^2 = id$ by

$$\begin{aligned}
\sigma_1 &: 2^{\frac{1}{3}} \mapsto 2^{\frac{1}{3}},\ w \mapsto w \iff id, \\
\sigma_2 &: 2^{\frac{1}{3}} \mapsto 2^{\frac{1}{3}},\ w \mapsto w^2 \iff \tau, \\
\sigma_3 &: 2^{\frac{1}{3}} \mapsto w2^{\frac{1}{3}},\ w \mapsto w \iff \sigma, \\
\sigma_4 &: 2^{\frac{1}{3}} \mapsto w2^{\frac{1}{3}},\ w \mapsto w^2 \iff \sigma\tau, \\
\sigma_5 &: 2^{\frac{1}{3}} \mapsto w^2 2^{\frac{1}{3}},\ w \mapsto w \iff \sigma^2, \\
\sigma_6 &: 2^{\frac{1}{3}} \mapsto w^2 2^{\frac{1}{3}},\ w \mapsto w^2 \iff \sigma^2\tau.
\end{aligned}$$

Let $H = A_3 \simeq \{\sigma_1, \sigma_3, \sigma_5\}$. It is clear that $H \simeq G(K, F_0(w))$. By identifying those two, we have

$$K_H = F_0(w)$$

so that $F_0(w) = K_{G(K,F_0(w))}$. Moreover, we know that $[K : F_0(w)] = 3$ and also, $o(G(K, F_0(w))) = 3$. Now consider a polynomial $x^3 - 1$. Then $F_0(w)$ is a normal extension of F_0. But it is also true that $G(K, F_0(w)) \simeq A_3$, is also a normal subgroup of $G(K, F_0) \simeq S_3$. So we have investigated the correspondence of A_3 and $F_0(w)$. Similarly, we can also find the correspondence between $\{id, \tau\}$ and $F_0(w^2 2^{\frac{1}{3}})$, $\{id, \sigma\tau\}$ and $F_0(2^{\frac{1}{3}})$ also $\{id, \sigma^2\tau\}$ and $F_0(w2^{\frac{1}{3}})$. That S_3 and F_0 are corresponding is trivial. Thus, we are done. □

c) Find a normal extension in K of degree 2 over F_0.

Proof. Note that $G(K, F_0(w)) \simeq A_3$ is a normal subgroup of $G(K, F_0) \simeq S_3$. Hence, the corresponding field extension $F_0(w)$ is a normal extension in K, of degree $\dfrac{G(K, F_0)}{G(K, F_0(w))} = 2$ over F_0. □

18. If the field F contains a primitive nth root of unity, prove that the Galois group of $x^n - a$, for $a \in F$, is abelian.

Proof. Let w denote a primitive nth root of unity in F. We know that

$$a^{\frac{1}{n}}, wa^{\frac{1}{n}}, w^2a^{\frac{1}{n}}, \cdots, w^{n-1}a^{\frac{1}{n}}$$

are the roots of $x^n - a$. Since w generates all the other powers of w, that is, it generates all the nth roots of unity in F. Thus, any automorphisms in the Galois group of $x^n - a$ over F, which result in the permutations of roots of $x^n - a$, must be commutative in their operations. Detailed explanation can be found in the text. Refer Lemma 5.7.3 b) . $\square$