Topics in Algebra solution

Sung Jong Lee, lovekrand.github.io

December 8, 2020

Problems in Section 5.8.

1. In S_5 show that $(1, 2)$ and $(1, 2, 3, 4, 5)$ generate S_5.

Proof. Refer the Problem 11, Section 2.10. □

2. In S_5 show that $(1, 2)$ and $(1, 3, 2, 4, 5)$ generate S_5.

Proof. If we could generate $(2, 3)$, then $(2, 3)^{-1}(1, 3, 2, 4, 5)(2, 3) = (1, 2, 3, 4, 5)$. Thus, it is enough to show that $(2, 3)$ can be generated by $(1, 2)$ and $(1, 3, 2, 4, 5)$. Note that

$$\{(1, 3, 2, 4, 5)^{-j}(1, 2)(1, 3, 2, 4, 5)^j : j \in \mathbb{Z}\} = \{(1, 2), (3, 4), (2, 5), (4, 1), (5, 3)\}$$

$(1, 2)(1, 3, 2, 4, 5) = (1, 4, 5)(2, 3)$ and $(1, 2)(2, 5)(4, 1) = (1, 5, 2, 4)$. Moreover,

$$(1, 5, 2, 4) \cdot (1, 4, 5)(2, 3) \cdot (5, 3) = (2, 5, 3) \cdot (5, 3) = (2, 3).$$

Therefore, $(1, 2)$ and $(1, 3, 2, 4, 5)$ generates S_5. □

3. If $p > 2$ is a prime, show that $(1, 2)$ and $(1, 2, \cdots, p-1, p)$ generates S_p.

Proof. Refer the Problem 11, Section 2.10. □

4. Prove that any transposition and p-cycle in S_p, p a prime, generates S_p.

Proof. Let $\sigma = (a, b, \cdots, c, d)$ and $\tau = (e, f)$ be an p-cycle and a transposition in S_p respectively. Note that, as σ is a p-cycle and hence, for some $1 \leq k \leq p-1$, σ^k sends e to 1. Thus, without lossing of generality, we can assume that $\tau = (1, f')$. Now rearranging σ as $\sigma = (1, a', \cdots, c', d')$, there exists $1 \leq t \leq p-1$ such that $\sigma^t = (1, f', \cdots,)$. Note that as p being a prime, $(1, f', \cdots)$ is also a p-cycle. Just as we have done at the beginning, rearranging $\{1, 2, \cdots, p\}$ gives $f' = 2$ and moreover, $(1, 2, \cdots, p-1, p)$. Now applying the Problem 3, we conclude that σ and τ generates S_p. □

5. Show that the following polynomials over $\mathbb{Q}$ are irreducible and have exactly two nonreal roots.
a) $p(x) = x^3 - 3x - 3$.

Proof. Applying Eisenstein's criterion, we conclude that $p(x)$ is irreducible over $\mathbb{Q}$. Now by differentiating $p(x)$, we have $p'(x) = 0 \iff x = \pm 1$. Since $p(-1) = -1 < 0$, $p(1) = -5$ where these points are local maximum and minimum in $\mathbb{R}$ respectively. Thus, there occurs only one real root, and hence two nonreal roots. $\square$

b) $x^5 - 6x + 3$.

Proof. Applying Eisenstein's criterion, we conclude that $p(x)$ is irreducible over $\mathbb{Q}$. Now by differentiating $p(x)$, we have $p'(x) = 0 \iff x^4 = \frac{6}{5} \iff x = \pm\sqrt[4]{\frac{6}{5}}$. Since $p(-\sqrt[4]{\frac{6}{5}}) > 0$, $p(\sqrt[4]{\frac{6}{5}}) < 0$ and $\lim_{x \to \pm\infty} p(x) = \pm\infty$, investigating the structure of the graph we conclude that $p(x)$ has only three real roots. Hence, it admits exactly two nonreal roots. $\square$

c) $x^5 + 5x^4 + 10x^3 + 10x^2 - x - 2$.

Proof. By substituting x by $x - 1$ we obtain $x^5 - 6x + 3$. We know that this is irreducible at $\mathbb{Q}$. Further, parallel transition of the graph of a polynomial does not occur in changes of the nature of its roots. Hence, as similarly as b), given polynomial has exactly two nonreal roots. $\square$

6. What are the Galois groups over $\mathbb{Q}$ of the polynomials in Problem 5?

Proof. For a), it is S_3 and for b) and c), each are S_5 respectively. $\square$

7. Construct a polynomial of degree 7 with rational coefficients whose Galois group over $\mathbb{Q}$ is S_7.

Proof. Let $p(x) = x^7 - 10x^5 - 15x^2 + 5$. Then it clearly irreducible in $\mathbb{Q}$ and has exactly two nonreal roots. Thus, the Galois group of $p(x)$ over $\mathbb{Q}$ is S_7. $\square$