14 Chapter 14 : SOLVABLE PERMUTATION GROUPS

14.1 POLYNOMIAL OF PRIME DEGREE

Ex. 14.1.1 *This exercise is concerned with the proof of part (a) of Lemma 14.1.2. Let* $\theta = (12...p) \in S_p$.

(a) Prove that $\tau \in S_p$ *lies in the normalizer of* $\langle\theta\rangle$ *if and only if* $\tau\theta = \theta^l\tau$ *for some* $1 \le l \le p-1$.

(b) Prove that (14.1) implies that $\tau(i+j) = \tau(i) + jl$ *for all positive integers* j.

Proof. (a) The normalizer of $\langle\theta\rangle$ in S_p consists of all $\tau \in S_p$ such that $\tau\langle\theta\rangle\tau^{-1} = \langle\theta\rangle$. It means that for any $\tau \in S_p$:

$$\begin{aligned}
\tau\langle\theta\rangle\tau^{-1} = \langle\theta\rangle &\iff \exists m, n \nmid p : \tau\theta^m\tau^{-1} = \theta^n \text{ (since } \langle\theta\rangle = \{\theta^{\mathrm{l}} \mid \mathrm{l} \in \mathbb{Z}\}) \\
&\iff \exists k \nmid p, e : mk + pe = 1 \text{ (since m} \nmid \text{p)} \\
&\iff (\tau\theta^m\tau^{-1})^k = \theta^{nk} = \theta^l,\ l = nk\ (mod\ p) \\
&\iff \tau\theta^{1-pe}\tau^{-1} = \tau\theta\tau^{-1} = \theta^l \text{ (since } \theta^p = e) \\
&\iff \tau\theta = \theta^l\tau \text{ for some } 1 \le l \le p-1.
\end{aligned}$$

(b) By induction suppose that $\tau(i+j) = \tau(i) + jl$, then $\tau(i+j+1) = \tau(i+j) + l = \tau(i) + (j+1)l$. Case $j = 1$ is valid by the identity (14.1). Hence, $\tau(i+j) = \tau(i) + jl$ for all positive integers j.

□

Ex. 14.1.2 *Let* H *be a normal subgroup of a finite group* G *and let* $g \in G$. *The goal of this exercise is to prove Lemma 14.1.3.*

(a) Explain why $(gH)^{o(g)} = (gH)^{[G:H]} = H$ *in the quotient group* G/H.

(b) Now assume that $gcd(o(g), [G:H]) = 1$. *Prove that* $g \in H$.

Proof. (a) Since $(gH)^2 = gHgH = g^2H$ and $g^{o(g)} = e$, $(gH)^{o(g)} = g^{o(g)}H = H$.

Since $gH \in G/H$, exists some minimal l such that $(gH)^l = H$ and $l \mid [G:H]$, i.e. $[G:H] = ql$. Then $(gH)^{[G:H]} = (gH)^{ql} = H^q = H$.

(b) The assumption $gcd(o(g), [G:H]) = 1$ means that $o(g)q + [G:H]l) = 1$ for some $q, l \in \mathbb{Z}$. Then $gH = (gH)^{o(g)q+[G:H]l} = ((gH)^{o(g)})^q((gH)^{[G:H]})^l = H^qH^l = H$, i.e. $g \in H$.

□

Ex. 14.1.3 *Let* G *satisfy (14.2). Use (14.2) and the Third Sylow Theorem to prove that* G *has a unique* p*-Sylow subgroup* H *of order* p. *Then conclude that* H *is normal in* G.

Proof. According to (14.2) $|G| = pm$ where $1 <= m <= p-1$, hence p is the highest power of p dividing $|G|$ and, by the First Sylow Theorem, G has a p-Sylow subgroup $H \subset G$ with $|H| = p$.

By the Second Sylow Theorem any two p-Sylow subgroups of G are conjugate in G. Therefore, group G acts on the set of p-Sylow subgroups by conjugation and this action is transitive. Due to transitivity of the action of G on the set of p-Sylow subgroups, the orbit of a fixed p-Sylow subgroup H is the whole set of p-Sylow subgroups, i.e., the order of such orbit is equal to the number of p-Sylow subgroups N and, by the Fundamental Theorem of Group Actions, N divides $|G| = pm$.

By the Third Sylow Theorem the number N of p-Sylow subgroups of G is equal to one by modulo p, $N \equiv 1 \mod p$. We have $N \nmid p$, hence $N \mid m$, which is possible only if $N = 1$.

Suppose that there is exactly one p-Sylow subgroup H of G. For all $g \in G$, gHg^{-1} is another subgroup of G of order equal to $|H|$, hence gHg^{-1} is also a p-Sylow subgroup and so $gHg^{-1} = H$ for all $g \in G$. This says that H is normal in G.

□

Ex. 14.1.4 *The definition of Frobenius group given in the Mathematical Notes involves a group G acting transitively on a set X. Prove that a group G is a Frobenius group if and only if G has a subgroup H such that $1 < |H| < |G|$ and $H \cap gHg^{-1} = \{e\}$ for all $g \notin H$.*

Proof. Suppose that G has a Frobenius action on the set X. Let $x \in X$ be an element with a nontrivial isotropy subgroup $G_x = \{g \in G \mid g \cdot x = x\}$. Since G acts transitively on X and $1 < |X| < |G|$, this element exists. Let fix such element and denote subgroup $H = G_x$ called a Frobenius complement. Due to transitivity, $1 < |H| < |G|$.

For any $g \in G$ an isotropy group of the element $g \cdot x$ is $G_{g \cdot x} = \{\hat{g} \in G \mid \hat{g}g \cdot x = g \cdot x\}$ and, since $gHg^{-1} \cdot g \cdot x = gH \cdot x = g \cdot x$, $gHg^{-1} = G_{g \cdot x}$.

If $g \in H$, then $g \cdot x = x$ and $G_{g \cdot x} = G_x$, hence $gHg^{-1} = H$.

If $g \notin H$, then $g \cdot x \neq x$ and $G_{g \cdot x} \cap G_x = \{e\}$, hence $gHg^{-1} \cap H = \{e\}$.

Now suppose that G has a subgroup H such that $1 < |H| < |G|$ and $H \cap gHg^{-1} = \{e\}$ for all $g \notin H$.

Let define the set X as the full set of left cosets gH, i.e., $X = \{H, g_1H, g_2H, ..., g_nH\}$. Since $1 < |H| < |G|$, then $1 < |X| < |G|$. It is obvious that G acts transitively on X - for any two elements $g_jg_i^{-1}$ moves g_iH to g_jH.

Let $N_G(H) = \{g \in G \mid gHg^{-1} = H\}$ is normalizer of H. Then $H \subset N_G(H)$ and, since $H \cap gHg^{-1} = \{e\}$ for all $g \notin H$, for any $g \in N_G(H)$ we have $g \in H$, hence $N_G(H) = H$, i.e., H is normal subgroup.

An isotropy group of the element g_iH is $G_{g_iH} = \{g \in G \mid g \cdot g_iH = g_iH\}$ and, since $g_iHg_i^{-1} \cdot g_iH = g_iHH = g_iH$, $g_iHg_i^{-1} = G_{g_iH}$.

Let by contradiction exists $g \neq \{e\}$ fixing two different elements from X, i.e., $g \cdot g_iH = g_iH$ and $g \cdot g_jH = g_jH$. Then $g \in G_{g_iH} \cap G_{g_jH}$, $g \in g_iHg_i^{-1} \cap g_jHg_j^{-1}$ and $\{e\} \neq g_j^{-1}gg_j \in g_j^{-1}g_iH(g_j^{-1}g_i)^{-1} \cap H$, where $g_j^{-1}g_i \notin H$. This contradicts with the assumption that $H \cap gHg^{-1} = \{e\}$ for all $g \notin H$ and proves that group G and set X are corresponding to the Frobenius group definition given in the Mathematical Notes.

□

Ex. 14.1.5 *Let F be a subfield of the real numbers, and let $f \in F[x]$ be irreducible of prime degree $p > 2$. Assume that f is solvable by radicals. Prove that f has either a single real root or p real roots.*

Proof. This is the direct corollary from the Theorem 14.1.1. If $\alpha \neq \beta$ are two real roots of solvable by radicals polynomial f of prime degree, then $F(\alpha, \beta)$ extension of subfield F is the splitting field of f over F. Hence all other p roots are in $F(\alpha, \beta)$ extension.

Since any rational extension of a subfield of the real numbers by addition of real numbers is the subfield of real numbers, all p roots are real.

Since the degree of f is odd, at least one real roots always exists. Therefore f has either a single real root or p real roots. $\square$

Ex. 14.1.6 *By Example 8.5.5, $f = x^5 - 6x + 3$ is not solvable by radicals over $\mathbb{Q}$. Give a new proof of this fact using the previous exercise together with the irreducibility of f and part (b) of Exercise 6 from Section 6.4.*

Proof. The given polynomial f has prime degree 5 and only three real roots, according to part (b) of Exercise 6.4.6. Since f has more than one but less than 5 real roots, it is not solvable by radicals by Exercise 14.1.5.

$\square$

Ex. 14.1.7 *Use Lemma 14.1.3 and part (a) of Lemma 14.1.2 to give a proof of part (b) of Lemma 14.1.2 that doesn't use the Sylow Theorems.*

Proof. Assume that $\tau \in S_p$ satisfies $\tau\theta\tau^{-1} \in AGL(1, \mathbb{F}_p)$. Then, since $\langle\theta\rangle$ is a group of order p, $\langle\tau\theta\tau^{-1}\rangle = \tau\langle\theta\rangle\tau^{-1}$ is a subgroup of $AGL(1, \mathbb{F}_p)$ of order p and each element of this subgroup has order p.

By part (a) of Lemma 14.1.2, $AGL(1, \mathbb{F}_p)$ is the normalizer of $\langle\theta\rangle$ in S_p, therefore $\langle\theta\rangle$ is normal in $AGL(1, \mathbb{F}_p)$ with $[AGL(1, \mathbb{F}_p) : \langle\theta\rangle] = (p-1)$. Order of each element from $\tau\langle\theta\rangle\tau^{-1}$ is relatively prime to $(p-1)$, then, by Lemma 14.1.3, $\tau\langle\theta\rangle\tau^{-1} \subset \langle\theta\rangle$, i.e., $\tau\langle\theta\rangle\tau^{-1} = \langle\theta\rangle$, since both groups have the same order p.

Thus τ normalizes $\langle\theta\rangle$ and hence $\tau \in AGL(1, \mathbb{F}_p)$. $\square$