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* $\theta = (1\,2\ldots p) \in S_p$.

(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) If θ lies in the normalizer of $\langle\theta\rangle = \{e, \theta, \theta^2, \ldots, \theta^{p-1}\}$, then

$$\tau\theta\tau^{-1} \in \tau\langle\theta\rangle\tau^{-1} = \langle\theta\rangle,$$

hence

$$\tau\theta\tau^{-1} = \theta^l \text{ for some } l = 0, 1\ldots, p-1.$$

If $l = 0$, then $\tau\theta\tau^{-1} = e$, thus $\tau\theta = \tau$, and $\theta = e$, which is false. Therefore $l \neq 0$.

$$\tau\theta\tau^{-1} = \theta^l,\ 1 \le l \le p-1.$$

(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. By (14.2),

$$|G| = |\mathrm{Gal}(L/F)| = pm, \qquad 1 \le m \le p-1.$$

According the Third Sylow Theorem the number N of p-Sylow subgroups of G satisfies

$$N \equiv 1 \pmod p, \qquad N \mid |G|,$$

so that $N = 1 + kp,\ k \geq 0$, thus $N \wedge p = 1$, and $N \mid pm$, therefore $N \mid m$. If $k \neq 0$, then $N > p$, but $N \mid m > 0$, which implies $N \leq m < p$. This contradiction shows that $k = 0$, and $N = 1$, i.e. there is exactly one p-Sylow subgroup H of G.

For all $g \in G$, gHg^{-1} is also a p-Sylow subgroup of G, hence $gHg^{-1} = H$ for all $g \in G$: 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. ($\Rightarrow$) Assume that G is a Frobenius group. Then G acts transitively on a set X such that $1 < |X| < |G|$, and for every $(x, y) \in X \times X$ such that $x \neq y$, the identity is the only element of G fixing x and y.

First we show that every isotropy group G_x is non trivial, i.e. $G_x \neq \{e\}$ and $G_x \neq G$, for all $x \in G$.

Since G acts transitively on X, $X = G \cdot x$ is the orbit of x, thus

$$|X| = |G \cdot x| = (G : G_x) = |G|/|G_x|,$$

and since $1 < |X| < |G|$, this proves $1 < |G_x| < |G|$, so $G_x \neq \{e\}, G_x \neq G$. Fix $x_0 \in G, x_0 \neq e$, and take $H = G_{x_0}$ the isotropy group of this chosen element x_0. Then $1 < |H| < G$.

Assume that $g \in G, g \notin H$, and $h \in H \cap gHg^{-1}$. Then h and $g^{-1}hg$ are both in $H = G_{x_0}$, so that $h \cdot x_0 = x_0$, and $(g^{-1}hg) \cdot x_0 = x_0$, that is

$$\left\{ \begin{array}{lcl} h \cdot x_0 & = & x_0, \\ h \cdot (g \cdot x_0) & = & (g \cdot x_0). \end{array} \right.$$

Since $g \notin H = G_{x_0}$, $x_0 \neq g \cdot x_0$, thus h fixes two distinct elements of X, and this shows that $h = e$. We have proved $H \cap gHg^{-1} = \{e\}$ for all $g \notin H$.

($\Leftarrow$) Conversely, assume that G has a subgroup H such that $1 < |H| < |G|$ and $H \cap gHg^{-1} = \{e\}$ for all $g \notin H$.

Take X as the set of left cosets $hH,\ h \in G$ relative to H, and consider the action of G on X defined for all $h \in G$ by

$$g \cdot hH = (gh)H.$$

- This action is transitive: if kH and lH are left cosets, then $(lk)^{-1} \cdot kH = lH$.
- Since $1 < |H| < |G|$, then $1 < |G|/|H| < |G|$, thus $1 < |X| < |G|$.
- Assume that g fixes two distinct left cosets $hH \neq kH$:

  $$g \cdot hH = hH,$$
  $$g \cdot kH = kH.$$

  Then $l = h^{-1}gh \in H, m = k^{-1}gk \in H$, therefore $m = k^{-1}gk = k^{-1}hlh^{-1}k \in H$, so that

  $$l \in H, \qquad (h^{-1}k)^{-1}l(h^{-1}k) \in H.$$

This proves $l \in H \cap gHg^{-1}$, where $g = h^{-1}k \notin H$ (since $hH \neq kH$), and the hypothesis $H \cap gHg^{-1} = \{e\}$ gives $l = e$, and $g = hlh^{-1} = e$. The identity is the only element of G fixing hH and kH.

Therefore G is a Frobenius group. □

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. Since $\deg(f) = p$ is odd, f has at least a real root. Suppose that f has two distinct real roots α, β. By Theorem 14.1.1, since f is solvable by radicals, the splitting field of f over F is $F(\alpha, \beta) \subset \mathbb{R}$. In this case all roots of f are real, and these roots are distinct, since the characteristic of F is 0, thus the irreducible polynomial f is separable.

We have proved that f has either a single real root or p real roots.

□

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.

□

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 $\tau\theta\tau^{-1} \in \mathrm{AGL}(1, \mathbb{F}_p)$. 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 $\mathrm{AGL}(1, \mathbb{F}_p)$ of order p and each element of this subgroup has order p (or 1).

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

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

Ex. 14.1.8 *Let $f \in F[x]$ be irreducible of prime degree $p \geq 5$, where F has characteristic 0, and let $\alpha \neq \beta$ be roots of f in some splitting field. If $F(\alpha, \beta)$ contains all other roots of f, then f is solvable by radicals by Theorem 14.1.1. But suppose that there is some third root γ such that $\gamma \in F(\alpha, \beta)$. Is this enough to force f to be solvable by radicals?*

(a) Use the classification of transitive subgroups of S_5 from Section 13.2 to show that the answer is "yes" when p=5.

(b) Use the polynomial $x^7 - 154\,x + 99$ from Example 13.3.10 to show that the answer is "no" when p=7.

Proof. (a) By hypothesis, $\deg(f) = p = 5$, and $\alpha \neq \beta$ are roots of f in some splitting field.

Since α is a root of f, which is irreducible over F,

$$[F(\alpha) : F] = \deg(f) = p = 5.$$

Then β is a root of $\frac{f(x)}{x-\alpha} \in F(\alpha)[x]$, so that the minimal polynomial of β over $F(\alpha)$ has degree $d \leq p - 1$. Thus

$$[F(\alpha, \beta) : F(\alpha] \leq p - 1 = 4.$$

By the Tower Theorem,

$$[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\alpha)]\ [F(\alpha) : F] \leq p(p-1) = 20.$$

Now, suppose that there is some third root γ such that $\gamma \in F(\alpha, \beta)$. Then $F(\alpha, \beta, \gamma) = F(\alpha, \beta)$. Let δ, ε be the remaining roots of f. Since the characteristic is 0, the irreducible polynomial f is separable.Then δ is a root of $\frac{f(x)}{(x-\alpha)(x-\beta)(x-\gamma)} \in F(\alpha, \beta, \gamma)[x]$, so that

$$[F(\alpha, \beta, \gamma, \delta) : F(\alpha, \beta, \gamma)] \leq 2.$$

Since $F(\alpha, \beta, \gamma) = F(\alpha, \beta)$, the tower theorem gives

$$[F(\alpha, \beta, \gamma, \delta) : F] \leq 40.$$

Moreover $\alpha+\beta+\gamma+\delta+\varepsilon = \sigma_1(\alpha, \beta, \gamma, \delta, \varepsilon) \in F$, thus $F(\alpha, \beta, \gamma, \delta, \varepsilon) = F(\alpha, \beta, \gamma, \delta)$. Write $L = F(\alpha, \beta, \gamma, \delta, \varepsilon)$ the splitting field of f over F. We have proved

$$[L : F] \leq 40.$$

The classification of transitive subgroups of S_5 from Section 13.2 shows that any transitive subgroup of S_5 with cardinality ≤ 40 is a subgroup of $\mathrm{AGL}(1, \mathbb{F}_5)$, thus is solvable. So $\mathrm{Gal}(L/F)$ is a solvable group, where F has characteristic 0, therefore f is solvable (Theorem 8.5.3).

To conclude, the answer is "yes" when $p = \deg(f) = 5$.

(b) To prove that the answer is "no" when $p = \deg(f) = 7$, we use the counterexample $f = x^7 - 154\,x + 99$ from Example 13.3.10.

The polynomial f is not solvable, since its Galois group is $\mathrm{GL}(3, \mathbb{F}_2)$, which is simple (Section 14.3) and not commutative, thus non solvable.

We prove that there are roots α, β, γ of f such that $\gamma \in F(\alpha, \beta)$.

As in Example 13.3.10, consider the resolvant

$$\Theta_f(y) = \prod_{1 \leq i < j < k \leq 7} (y - (\alpha_i + \alpha_j + \alpha_k)) \in \mathbb{Q}[y].$$

Then the factorization of $\Theta_f(y)$ over $\mathbb{Q}$ is

$$\Theta_f(y) = g(y)h(y),$$

where the polynomials g, h, given in Example 13.3.10, are irreducible factors of degrees 7 and 28.

Take three roots α, β, γ of f such that $y - (\alpha + \beta + \gamma)$ is any linear factor of g, so that the minimal polynomial of $\alpha + \beta + \gamma$ is g, with $\deg(g) = 7$, thus

$$[\mathbb{Q}(\alpha + \beta + \gamma) : \mathbb{Q}] = 7.$$

Now we prove that $\gamma \in F(\alpha, \beta)$. Consider the chain of extensions

$$\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\alpha, \beta) \subset \mathbb{Q}(\alpha, \beta, \gamma) \subset L,$$

where L is the splitting field of f over $\mathbb{Q}$.

The minimal polynomial of α over $\mathbb{Q}$ is f, thus $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 7$, and

$$[L : \mathbb{Q}] = |\mathrm{Gal}(L/\mathbb{Q})| = |\mathrm{GL}(3, \mathbb{F}_2)| = 168 = 2^3 \times 3 \times 7.$$

By the Tower Theorem,

$$[L : \mathbb{Q}(\alpha)] = \frac{[L : \mathbb{Q}]}{[\mathbb{Q}(\alpha) : \mathbb{Q}]} = 2^3 \times 3$$

is not divisible by 7.

Since γ is a root of f, the minimal polynomial of γ over f divides f. Thus

$$[\mathbb{Q}(\alpha, \beta, \gamma) : \mathbb{Q}(\alpha, \beta)] = 1 \text{ or } 7.$$

If $[\mathbb{Q}(\alpha, \beta, \gamma) : \mathbb{Q}(\alpha, \beta)] = 7$, by the Tower Theorem, 7 divides $[L : \mathbb{Q}(\alpha)] = 2^3 \times 3$. This contradiction proves that

$$[\mathbb{Q}(\alpha, \beta, \gamma) : \mathbb{Q}(\alpha, \beta)] = 1,$$

therefore $\gamma \in \mathbb{Q}(\alpha, \beta)$.

In this example, there exist roots $\alpha \neq \beta$ of f, and some third root γ such that $\gamma \in F(\alpha, \beta)$, but f is not solvable.

This shows that the answer is "no" when $p = \deg(f) = 7$.

$\square$

Note: In the proof of the Proposition 13.3.9, we saw that G_f must be conjugate to $\mathrm{GL}(3, \mathbb{F}_2)$. This means that there is some numbering of the roots

$$\left\{ \begin{array}{ccc} \mathbb{F}_2^3 \setminus \{(0,0,0\} & \to & \{\alpha \in L \mid f(\alpha) = 0\} \\ (\nu_1, \nu_2, \nu_3) & \to & \alpha_{\nu_1, \nu_2, \nu_3} \end{array} \right.$$

which verify that, for all $\sigma \in \mathrm{Gal}(L/F)$, there is some $g \in \mathrm{GL}(3, \mathbb{F}_2)$ such that

$$\sigma(\alpha_{\nu_1, \nu_2, \nu_3}) = \alpha_{g \cdot (\nu_1, \nu_2, \nu_3)}.$$

In this correspondance, the roots of f are seen as nonzero vectors in $\mathbb{F}_2^3$, and the seven roots of g correspond to the seven (unordered) triples of linearly dependent nonzero vectors in $\mathbb{F}_2^3$. So the roots α, β, γ where chosen in the preceding proof such that the corresponding vectors u, v, w verify $w = u + v$ (but not $\gamma = \alpha + \beta$) .

This is what we understand in the hint of D.A. Cox "Regard the roots as the nonzero vectors of $\mathbb{F}_2^3$ and pick roots α, β, γ such that $\gamma = \alpha + \beta$".

This last equality is not true in L, but true for the corresponding vectors in $\mathbb{F}_2^3$.

Moreover, let $\alpha \neq \beta$ be *any* pair of roots. The corresponding vectors u, v are such that $u, v, u + v = -u - v$ is not a base, so that the root γ corresponding to $u + v$ is such that $y - (\alpha + \beta + \gamma)$ is a factor of g, and the preceding proof shows that $\gamma \in \mathbb{Q}(\alpha, \beta)$. For each pair $\alpha \neq \beta$ of roots of $f = x^7 - 154\,x + 99$, there exists a third root $\gamma \notin \{\alpha, \beta\}$ such that $\gamma \in F(\alpha, \beta)$.

14.2 IMPRIMITIVE POLYNOMIALS OF PRIME-SQUARED DEGREE

Ex. 14.2.1 *Prove (14.7).*

Proof. Given $\sigma' = (\tau'; \mu'_1, ..., \mu'_k), \sigma = (\tau; \mu_1, ..., \mu_k) \in A \wr B$. Since σ' maps R_i to $R_{\tau'(i)}$ via μ'_i, if we set $j = \tau'(i)$, then σ maps R_j to $R_{\tau(j)} = R_{\tau(\tau'(i))} = R_{\tau\tau'(i)}$ via $\mu_j = \mu_{\tau'(i)}$.

Hence $\sigma\sigma'$ maps R_i to $R_{\tau\tau'(i)}$ via $\mu_{\tau'(i)}\mu'_i$.

More explicitly, by the definition of $(\tau; \mu_1, \ldots, \mu_k)$, for all $(i,j) \in \{1, \ldots, k\} \times \{1, \ldots, l\}$,

$$(\tau; \mu_1, \ldots, \mu_k)(i,j) = (\tau(i), \mu_i(j)).$$

Applying three times this definition, we obtain

$$\begin{aligned}
(\tau; \mu_1, \ldots, \mu_k)(\tau'; \mu'_1, \ldots, \mu'_k) &= (\tau; \mu_1, \ldots, \mu_k)(\tau'(i), \mu'_i(j)) \\
&= ((\tau\tau')(i), \mu_{\tau'(i)}(\mu'_i(j)) \\
&= ((\tau\tau')(i), (\mu_{\tau'(i)}\mu'_i)(j) \\
&= (\tau\tau'; \mu_{\tau'(1)}\mu'_1, ..., \mu_{\tau'(k)}\mu'_k)(i,j)
\end{aligned}$$

Since this equality is true for all $(i,j) \in \{1, \ldots, k\} \times \{1, \ldots, l\}$,

$$(\tau; \mu_1, ..., \mu_k)(\tau'; \mu'_1, ..., \mu'_k) = (\tau\tau'; \mu_{\tau'(1)}\mu'_1, ..., \mu_{\tau'(k)}\mu'_k).$$

$\square$