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

(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 $\langle\theta\rangle = \{e, \theta, \theta^2, \dots, \theta^{p-1}\}$, then

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

hence

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

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

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

(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, $\tau\langle\theta\rangle\tau^{-1} \subset \langle\theta\rangle$, 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

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

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 $(i, j) \in \{1, \ldots, k\} \times \{1, \ldots, l\}$,

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

□

Ex. 14.2.2 *The wreath product $S_3 \wr S_2 \subset S_6$ can be thought of as the subgroup of all permutations that preserve the blocs $R_1 = \{1, 2\}, R_2 = \{3, 4\}, R_3 = \{5, 6\}$. As noted in Example 14.2.11, $S_3 \wr S_2$ has order $6 \cdot 3^3 = 48$.*

(a) Show that $(S_3 \wr S_2) \cap A_6$ has order 24.

(b) Show that $S_3 \wr S_2$ is the centralizer of $(1\,2)(3\,4)(5\,6)$ in S_6 (meaning that $S_3 \wr S_2$ consists of all permutations in S_6 that commute with $(1\,2)(3\,4)(5\,6)$).

(c) Use part (b) to show that $S_3 \wr S_2$ is isomorphic to $((S_3 \wr S_2) \cap A_6) \times S_2$.

See the next exercise for more on $S_3 \wr S_2$ and $(S_3 \wr S_2) \cap A_6$.

Proof.

(a) Let φ the restriction of the sign sgn to $(S_3 \wr S_2) \cap A_6$:

$$\varphi \left\{ \begin{array}{ccc} S_3 \wr S_2 & \to & \{-1, 1\} \\ \sigma & \mapsto & \mathrm{sgn}(\sigma) \end{array} \right.$$

Since sgn is a morphism, its restriction φ is also a morphism, and φ is surjective (onto), because $\varphi(e) = 1$, and $\varphi((1\,2)) = -1$, where $(1\,2) \in S_3 \wr S_2$. Moreover the kernel of φ is $\ker(\varphi) = (S_3 \wr S_2) \cap A_6$.

Therefore $\mathrm{im}(\varphi)\{-1, 1\} \simeq (S_3 \wr S_2)/((S_3 \wr S_2) \cap A_6)$. This shows that

$$|(S_3 \wr S_2) \cap A_6| = \frac{1}{2}|S_3 \wr S_2| = 24.$$

(b) Let $\tau \in S_n$. Then τ is in the centralizer of $\sigma = (1\,2)(3\,4)(5\,6)$ if and only if

$$\tau(1\,2)(3\,4)(5\,6)\tau^{-1} = (1\,2)(3\,4)(5\,6),$$

which is equivalent to

$$(\tau(1)\,\tau(2))(\tau(3)\,\tau(4))(\tau(5)\,\tau(6)) = (1\,2)(3\,4)(5\,6).$$

Write $R_1 = \{1,2\}, R_2 = \{3,4\}, R_3 = \{4,5\}$. Then R_1, R_2, R_3 are the three orbits of σ acting on $\{1,\ldots,6\}$, the supports of the decomposition of σ in disjoint cycles.

Since τ is a bijection, the 6 values $\tau(1), \tau(2), \tau(3), \tau(4), \tau(5), \tau(6)$ are distinct, so $(\tau(1)\,\tau(2)), (\tau(3)\,\tau(4)), (\tau(5)\,\tau(6))$ are disjoint 2-cycles.

If τ is the centralizer of σ, the equality $(\tau(1)\,\tau(2))(\tau(3)\,\tau(4))(\tau(5)\,\tau(6)) = (1\,2)(3\,4)(5\,6)$ shows that $\tau(R_1), \tau(R_2), \tau(R_3)$ are also the three orbits of σ, so that

$$\{\{1,2\},\{3,4\},\{5,6\}\} = \{\{\tau(1),\tau(2)\},\{\tau(3),\tau(4)\},\{\tau(5),\tau(6)\}\},$$

that is

$$\{R_1, R_2, R_3\} = \{\tau(R_1), \tau(R_2), \tau(R_3)\},$$

which means that there is some permutation τ' of $\{1,2,3\}$ such that $\tau(R_i) = R_{\tau'(i)},\ i = 1,2,3$. In other words, σ preserves the blocks R_1, R_2, R_3, so that $\sigma \in S_3 \wr S_2$.

To prove the converse, it is more convenient to use the other usual representation of $S_3 \wr S_2$. Then $\sigma = (e; \mu, \mu, \mu)$, where $\mu = (1\,2) \in S_2$. Let $\tau = (\lambda; \mu_1, \mu_2, \mu_3)$ be any element of $S_3 \wr S_2$ (then $\mu_i = ()$ or $\mu_i = \mu$). Then (14.7) gives

$$\begin{aligned}
\tau\sigma &= (\lambda; \mu_1, \mu_2, \mu_3)(e; \mu, \mu, \mu)\\
&= (\lambda; \mu_1\mu, \mu_2\mu, \mu_3\mu)\\
\sigma\tau &= (e; \mu, \mu; \mu)(\lambda, \mu_2, \mu_2, \mu_3)\\
&= (\lambda; \mu\mu_1, \mu\mu_2, \mu\mu_3)
\end{aligned}$$

Since $S_2 = \{e, \mu\}$ is commutative, $\mu\mu_i = \mu_i\mu,\ i = 1,2,3$, thus $\tau\sigma = \sigma\tau$.

The centralizer of $(1\,2)(3\,4)(5\,6)$ in S_n is $S_3 \wr S_2$.

(c) Since the order of $\sigma = (1\,2)(3\,4)(5\,6)$ is 2, $\langle\sigma\rangle = \{e, \sigma\} \simeq S_2$ and we can write σ^ε , $\varepsilon \in \{0,1\}$ the two elements of $\langle\sigma\rangle$. Let

$$\varphi \left\{ \begin{array}{ccc} (S_3 \wr S_2) \cap A_6 \times \langle\sigma\rangle & \to & S_3 \wr S_2 \\ (\tau, \sigma^\varepsilon) & \mapsto & \tau\sigma^\varepsilon. \end{array} \right.$$

• φ is a morphism: For all $\tau, \tau' \in (S_3 \wr S_2) \cap A_6$ and $\sigma^\varepsilon, \sigma^{\varepsilon'} \in \langle\sigma\rangle$, $\sigma\tau' = \tau'\sigma$ by part (b), thus

$$\begin{aligned}
\varphi(\tau\sigma^\varepsilon)\varphi(\tau'\sigma^{\varepsilon'}) &= \tau\sigma^\varepsilon\tau'\sigma^{\varepsilon'}\\
&= \tau\tau'\sigma^\varepsilon\sigma^{\varepsilon'}\\
&= \varphi((\tau, \sigma^\varepsilon)(\tau', \sigma^{\varepsilon'}))
\end{aligned}$$

• $\ker\varphi$ is trivial: if $\varphi(\tau, \sigma^\varepsilon) = e$, then $\tau\sigma^\varepsilon = e$, so that $\tau = \sigma^{-\varepsilon} \in \{e, \sigma\}$. $\tau = \sigma$ is impossible, since τ is an even permutation, and σ is odd. Therefore $\tau = e$, and $\sigma^\varepsilon = e$. Thus φ is injective (one to one).

• Since $|((S_3 \wr S_2) \cap A_6) \times \langle\sigma\rangle| = |S_3 \wr S_2|$, φ is a bijection, thus φ is a group isomorphism.

$$S_3 \wr S_2 \simeq ((S_3 \wr S_2) \cap A_6) \times \langle\sigma\rangle \simeq ((S_3 \wr S_2) \cap A_6) \times S_2.$$

$\square$

Ex. 14.2.3 *One of the challenges of group theory is that the same group can have radically differnet descriptions. For instance, S_4 and the group $G = (S_3 \wr S_2) \cap A_6$ appearing in Example 14.2.11 both have order 24. In this exercise, you will prove that they are isomorphic. We will use the notation of Exercise 2.*

(a) There is a natural homomorphism $G \to S_3$ given by how elements of G permute the blocks R_1, R_2, R_3. Show that this map is onto, and express the elements of the kernel as products of disjoints cycles.

(b) Use the Sylow Theorems to show that G has one or four 3-Sylow subgroups.

(c) Show that A_6 has no element of order 6.

(d) Use part (c) and the kernel of the map $G \to S_3$ from part (a) to show that G has four 3-Sylow subgroups.

(e) G acts by conjugation on its four 3-Sylow subgroups. Use this to prove that $G \simeq S_4$.

(f) Using Exercise 2, conclude that $S_3 \wr S_2 \simeq S_4 \times S_2$.

We note without proof that $S_3 \wr S_2 \simeq S_4 \times S_2$ is also isomorphic to the full symmetry group (rotations and reflexions) of the octahedron.

Proof.

(a) Let $\varphi : G \to S_3$ defined by $\tau = \varphi(\sigma)$ iff $\sigma(R_i) = R_{\tau(i)}$. In other notations, this is the restriction to G of the homomorphism of part (b) of Lemma 14.2.8, thus φ is an homomorphism.

• φ is surjective: Let τ be any permutation in S_3.
If τ is even, $\tau = (1\,2\,3)^k,\ k = 0,1,2$. Let

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix} = (1\,3\,5)(2\,4\,6).$$

σ preserves the block structure defined by R_1, R_2, R_3, and $\sigma \in A_6$, so that $\sigma \in G = (S_3 \wr S_2) \cap A_6$. Moreover $\sigma(R_1) = R_2, \sigma(R_2) = R_3, \sigma(R_3) = R_1$, thus $\varphi(\sigma) = (1\,2\,3)$, and $\varphi(\sigma^k) = (1\,2\,3)^k = \tau$.

If τ is odd, then $\tau \in \{(1\,2), (2\,3), (1\,3)\}$, and

$$(1\,2) = \varphi(\sigma_1), \qquad \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 2 & 5 & 6 \end{pmatrix} = (1\,3)(2\,4) \in G,$$

$$(2\,3) = \varphi(\sigma_2), \qquad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 5 & 6 & 3 & 4 \end{pmatrix} = (3\,5)(4\,6) \in G,$$

$$(1\,3) = \varphi(\sigma_3), \qquad \sigma_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 3 & 4 & 1 & 2 \end{pmatrix} = (1\,5)(2\,6) \in G.$$

Therefore φ is surjective.

• Let $\sigma \in S_6$. Then $\sigma \in \ker \varphi$ iff $\sigma \in A_6$ and $\sigma(R_1) = R_1, \sigma(R_2) = R_2, \sigma(R_3) = R_3$.
Morerover, for all $\sigma \in A_6$,

$$\begin{aligned} &\sigma(R_1) = R_1, \sigma(R_2) = R_2, \sigma(R_3) = R_3 \\ \iff &\{\sigma(1), \sigma(2)\} = \{1,2\}, \{\sigma(3), \sigma(4)\} = \{3,4\}, \{\sigma(5), \sigma(6)\} = \{5,6\} \\ \iff &\sigma \in \{e, (1\,2)(3\,4), (1\,2)(5\,6), (3\,4)(5\,6)\}. \end{aligned}$$

$$\ker\varphi = \{e, (1\,2)(3\,4), (1\,2)(5\,6), (3\,4)(5\,6)\}.$$

Verification: $6 = |S_3| = |G/\ker(\varphi)| = 24/4$.

(b) Let N be the number of 3-Sylow subgroups of G. By the third Slow Theorem,

$$N \mid 24 = |G|, \qquad N \equiv 1 \pmod 3.$$

Therefore $N = 1$ or $N = 4$.

(c) Let $\tau \in S_6$ be a permutation of order 6. If $\tau = \tau_1 \cdots \tau_k$ is the decomposition of τ in disjoint cycles, then the order of τ is the lcm of the order of$\tau_1, \ldots, \tau_k$. Therefore τ is a 6-cycle or a product of a 2-cycle by a 3-cycle. In both cases τ is odd. Therefore A_6 has no element of order 6.

(d) Reasoning by contradiction, suppose that G has only one 3-Sylow subgroup H. Then, for all $g \in G$, gHg^{-1} is a 3-Sylow, thus $gHg^{-1} = H$, and H is a normal subgroup of G.

Moreover $K = \ker\varphi = \{e, (1\,2)(3\,4), (1\,2)(5\,6), (3\,4)(5\,6)\}$ is normal in G, and has order 4. Therefore $H \cap K = \{e\}$.

The usual characterization of direct products (see Ex. 14.3.7) shows that, for all $h \in H$, all $k \in K$, $hk = kh$, and HK is a normal subgroup of G isomorphic to $H \times K$.

Take h an element of order 3 in H, and k and element of order 2 in K. Since $kh = hk$, the order of $hk \in A_6$ is 6, which is impossible by part (c).

Therefore G has exactly four 3-Sylow subgroups.

(e) Write $X = \{H_1, H_2, H_3, H_4\}$ the set of 3-Sylow subgroups of G, and $S(X)$ the set of permutations of X. Then $S(X) \simeq S_4$, and $g \cdot H = gHg^{-1}$ defines a left action of G on X, so that

$$\psi \left\{ \begin{array}{ccc} G & \to & S(X) \\ g & \mapsto & \sigma = \begin{pmatrix} H_1 & H_2 & H_3 & H_4 \\ gH_1g^{-1} & gH_2g^{-1} & gH_3g^{-1} & gH_4g^{-1} \end{pmatrix} \end{array} \right.$$

is a group homomorphism.

It is not obvious that ψ is bijective. We prove first that ψ is surjective (onto). We give explicitly the 3-Sylow subgroups. Let

$$\lambda_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix} = (1\,3\,5)(2\,4\,6),$$

$$\lambda_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 6 & 5 & 2 & 1 \end{pmatrix} = (1\,3\,6)(4\,5\,2),$$

$$\lambda_3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 1 & 3 & 4 \end{pmatrix} = (1\,6\,4)(5\,3\,2),$$

$$\lambda_4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 6 & 5 & 1 & 2 \end{pmatrix} = (1\,4\,5)(3\,6\,2).$$

Then $\lambda_1, \ldots, \lambda_4 \in G$ have order 3, and $H_1 = \langle \lambda_1 \rangle = \{e, \lambda_1, \lambda_1^2\}, \ldots, H_4 = \langle \lambda_1 \rangle = \{e, \lambda_4, \lambda_4^2\}$ are distinct, thus they are the four 3-Sylow of G.

Now take

$$g = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 1 & 5 & 6 \end{pmatrix} = (1\,4)(2\,3)$$

$$h = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 5 & 6 & 4 & 3 \end{pmatrix} = (1\,2)(3\,5\,4\,6)$$

(We give a geometrical explanation of this choice in the final note.)

Then

$$\begin{aligned} g\lambda_1 g^{-1} &= (1\,4)(2\,3)(1\,3\,5)(2\,4\,6)(1\,4)(2\,3) \\ &= \begin{pmatrix} 1 & 2 & & 3 & 4 & & 5 & 6 \\ 6 & 5 & & 1 & 2 & & 4 & 3 \end{pmatrix} = (1\,6\,3)(2\,5\,4) = \lambda_2^2, \end{aligned}$$

thus $gH_1g^{-1} = H_2$, and since $g = g^{-1}$, $gH_2g^{-1} = H_1$. Moreover

$$\begin{aligned} g\lambda_3 g^{-1} &= (1\,4)(2\,3)(1\,6\,4)(5\,3\,2)(1\,4)(2\,3) \\ &= \begin{pmatrix} 1 & 2 & & 3 & 4 & & 5 & 6 \\ 4 & 3 & & 5 & 6 & & 2 & 1 \end{pmatrix} = (1\,4\,6)(2\,3\,5) = \lambda_3^2, \end{aligned}$$

thus $gH_3g^{-1} = H_3$, and since $\psi(g)$ is a permutation, $gH_4g^{-1} = H_4$.

Therefore $\psi(g) \in S(X)$ is the permutation $\begin{pmatrix} H_1 & H_2 & H_3 & H_4 \\ H_2 & H_1 & H_3 & H_4 \end{pmatrix}$, which corresponds to the transposition $(1\,2) \in S_4$. Similarly

$$\begin{aligned} h\lambda_1 h^{-1} &= (1\,2)(3\,4\,5\,6)(1\,3\,5)(2\,4\,6)(3\,6\,4\,5)(1\,2) \\ &= \begin{pmatrix} 1 & 2 & & 3 & 4 & & 5 & 6 \\ 6 & 5 & & 1 & 2 & & 4 & 3 \end{pmatrix} = (1\,6\,3)(2\,5\,4) = \lambda_2^2, \\ h\lambda_2 h^{-1} &= (1\,2)(3\,4\,5\,6)(1\,3\,6)(4\,5\,2)(3\,6\,4\,5)(1\,2) \\ &= \begin{pmatrix} 1 & 2 & & 3 & 4 & & 5 & 6 \\ 6 & 5 & & 2 & 1 & & 3 & 4 \end{pmatrix} = (1\,6\,4)(2\,5\,3) = \lambda_3, \\ h\lambda_3 h^{-1} &= (1\,2)(3\,4\,5\,6)(1\,6\,4)(5\,3\,2)(3\,6\,4\,5)(1\,2) \\ &= \begin{pmatrix} 1 & 2 & & 3 & 4 & & 5 & 6 \\ 4 & 3 & & 6 & 5 & & 1 & 2 \end{pmatrix} = (1\,4\,5)(2\,6\,4) = \lambda_4, \end{aligned}$$

thus $hH_1h^{-1} = H_2, hH_2h^{-1} = H_3, hH_1h^{-1} = H_4$, and since $\psi(g)$ is a permutation, $hH_4h^{-1} = H_1$. Therefore $\psi(g) = \begin{pmatrix} H_1 & H_2 & H_3 & H_4 \\ H_2 & H_3 & H_4 & H_1 \end{pmatrix}$ corresponds to the 4-cycle $(1\,2\,3\,4)$.

Since $\{(1\,2), (1\,2\,3\,4)\}$ is a set of generators of S_4, $S(X)$ is generated by $\psi(g), \psi(h)$, so that $S(X) = \psi(G)$, and ψ is surjective. Moreover, $|G| = |S(X)| = 24$, thus ψ is a bijection, and a group isomorphism:

$$G \simeq S(X) \simeq S_4.$$

(f) To conclude, using Exercise 2, we obtain

$$S_3 \wr S_2 \simeq ((S_3 \wr S_2) \cap A_6) \times S_2 = G \times S_2 \simeq S_4 \times S_2.$$

Note: We have proved in Exercise 7.5.10 that the symmetry group G_0 of the cube (or octahedron), is isomorphic to S_4. By composition with the indirect isometry $\sigma : v \mapsto -v$, which commutes with all elements in the group, we obtain the full symmetry group, isomorphic to $S_4 \times S_2$.

We have a geometrical description of $G = (S_3 \wr S_2) \cap A_6$ by regrouping the opposite faces of a cube in blocs: stick 1 on a face of a dice, 2 on the opposite face, and so on

(I stuck labels on my Rubik's cube). Then the 24 rotations of the cube send opposite faces on opposite faces, so that the bloc structure $\{\{1,2\},\{3,4\},\{5,6\}\}$ is preserved by rotations.

We have proved in Exercise 7.5.10 that G_0 acts on the 4 long diagonals D_1, D_2, D_3, D_4 of the cube, so that $G_0 \simeq S_4$. Each of the four 3-Sylow of G_0 is generated by the rotation with angle $\frac{2\pi}{3}$ around such a long diagonal. They correspond to the 3-Sylow $H_1, \dots, H_4$ of G: this was useful for the above description of the H_i. Each 3-Sylow corresponds to a long diagonal, so that $gH_ig^{-1} = H_j$ is equivalent to $\sigma(D_i) = D_j$, where σ corresponds to g. It remains to find a rotation which acts on these diagonals as some given permutation in S_4, such that $(1\,2)$ or $(1\,2\,3\,4)$. The corresponding permutations $g, h \in G$ are given in the text.

$\square$

Ex. 14.2.4 *Let A and B be solvable permutation groups. Prove that their wreath product $A \wr B$ is also solvable.*

We first proof a lemma, which is not given in Chapter 8.

Lemma. *If G, H are solvable groups, then $G \times H$ is solvable.*

Proof of Lemma. We have subgroups

$$\begin{aligned}\{e\} \subset G_n \subset \cdots \subset G_1 \subset G_0 = G\\ \{e'\} \subset H_m \subset \cdots \subset H_1 \subset H_0 = H\end{aligned}$$

such that G_i is normal in G_{i-1} and G_{i-1}/G_i is Abelian for $i = 1, \dots, n$, and H_i is normal in H_{i-1} and H_{i-1}/H_i is Abelian for $i = 1, \dots, m$.

If $n > m$, we can define $H_{m+1} = H_{m+2} = \cdots = H_n = \{e'\}$, and proceed similarly if $n < m$, so we can assume that $n = m$:

$$\begin{aligned}\{e\} \subset G_n \subset \cdots \subset G_1 \subset G_0 = G\\ \{e'\} \subset H_n \subset \cdots \subset H_1 \subset H_0 = H\end{aligned}$$

Then

$$\{(e, e')\} = G_n \times H_n \subset \cdots \subset G_1 \times H_1 \subset G_0 \times H_0 = G \times H.$$

We prove

$$(G_{i-1} \times H_{i-1})/(G_i \times H_i) \simeq G_{i-1}/G_i \times H_{i-1}/H_i.$$

Indeed,

$$\psi \left\{ \begin{array}{ccc} G_{i-1} \times H_{i-1} & \to & G_{i-1}/G_i \times H_{i-1}/H_i \\ (g,h) & \mapsto & (gG_i, hH_i) \end{array} \right.$$

is surjective, and its kernel is $G_i \times H_i$. This proves our assertion.

Therefore $(G_{i-1} \times H_{i-1})/(G_i \times H_i)$ is Abelian. Then Exercise 8.1.8 shows that $G \times H$ is solvable. $\square$

Proof. (of Ex.14.2.4.) Let

$$\varphi \left\{ \begin{array}{ccc} A \wr B & \to & A \\ (\tau; \mu_1, \dots, \mu_k) & \mapsto & \tau. \end{array} \right.$$

By Lemma 14.2.8, φ is onto, and its kernel $H = \ker(\varphi)$ is isomorphic to B^k. Then B^k is solvable by induction with the above Lemma, so that H is solvable, and $(A \wr B)/H = (A \wr B)/\ker(\varphi) \simeq A$ is solvable. By Theorem 8.1.4, $A \wr B$ is solvable. $\square$

Ex. 14.2.5 *This exercise will complete the proof of Theorem 14.2.15.*

(a) Let $G_i \to S_p$ be the map defined in (14.9). Prove that it is a group homomorphism and that its image $G_i' \subset S_p$ is transitive and solvable.

(b) Let $\sigma = (\tau; \mu_1, \ldots, \mu_p)$ and $(\rho; \nu_1, \ldots, \nu_p)$ be as in the proof of Theorem 14.2.15. Thus we have a fixed j such that $i = \tau(j), \nu_i = \theta$, and $\rho(i) = i$. Now let $\gamma = (\tau^{-1}\rho\tau; \lambda_1, \ldots, \lambda_p)$ be as in (14.11). Prove carefully that $\lambda_j = \mu_j^{-1}\theta\mu_j$.

Proof.

(a) The map φ_i defined in (14.9) is

$$\varphi_i \left\{ \begin{array}{ccc} G_i & \to & S_p \\ (\tau; \mu_1, \ldots, \mu_p) & \mapsto & \mu_i. \end{array} \right.$$

Let $\lambda = (\tau; \mu_1, \ldots, \mu_p), \lambda' = (\tau'; \mu_1, \ldots, \mu_p)$ be elements of G_i. The definition of G_i shows that $\lambda(R_i) = \lambda'(R_i) = R_i$, so that $\tau(i) = \tau'(i) = i$.

By (14.7) (see Exercise 1),

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

therefore, using $\tau'(i) = i$,

$$\begin{aligned} \varphi_i(\lambda\lambda') &= \mu_{\tau'(i)}\mu_i' \\ &= \mu_i\mu_i' \\ &= \varphi_i(\lambda)\varphi_i(\lambda'), \end{aligned}$$

thus φ_i is a group homomorphism.

Write $G_i' = \varphi_i(G_i) \subset S_p$. We prove first that G_i' is transitive.

Take any k and l in $\{1, \ldots, p\}$. Since G is transitive, there exists some $\lambda = (\tau; \mu_1, ..., \mu_k) \in G$ which sends (i, j) on (i, k):

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

Then $\tau(i) = i$, so that $\lambda \in G_i$ and $\mu_i = \varphi_i(\lambda) \in G_i'$. Moreover $\mu_i(j) = k$. This proves that G_i' is a transitive subgroup of S_p.

Moreover, G_i is a subgroup of the solvable group G, thus G_i is solvable. Then $G_i' = \varphi_i(G_i)$ is isomorphic to $G_i/\ker(\varphi_i)$, which is a quotient of a solvable group, thus G_i' is solvable.

(b) As in the proof of Theorem 14.2.15, let $\sigma = (\tau; \mu_1, \ldots, \mu_p) \in G$ be arbitrary, and fix j between 1 and p. By (14.10) with $i = \tau(j)$, $\theta \in G_i' = \varphi_i(G_i)$, thus there exists $\lambda = (\rho; \nu_1, \ldots, \nu_p) \in G_i$ such that $\theta = \varphi_i(\lambda)$, thus $\theta = \nu_i$ and $\rho(i) = i$.

Now consider the element $\gamma = \sigma^{-1}\lambda\sigma \in G$. Using (14.6) and (14.7), we obtain

$$\begin{aligned} \gamma &= (\tau; \mu_1, \ldots, \mu_p)^{-1}(\rho; \nu_1, \ldots, \nu_p)(\tau; \mu_1, \ldots, \mu_p) \\ &= (\tau^{-1}; \mu_{\tau^{-1}(1)}^{-1}, \ldots, \mu_{\tau^{-1}(p)}^{-1})(\rho\tau; \nu_{\tau(1)}\mu_1, \ldots, \nu_{\tau(p)}\mu_p) \\ &= (\tau^{-1}; \xi_1, \ldots, \xi_p)(\rho\tau; \nu_{\tau(1)}\mu_1, \ldots, \nu_{\tau(p)}\mu_p) \qquad (\text{where } \xi_1 = \mu_{\tau^{-1}(1)}^{-1}, \ldots, \xi_p = \mu_{\tau^{-1}(p)}^{-1}) \\ &= (\tau^{-1}\rho\tau; \xi_{(\rho\tau)(1)}\nu_{\tau(1)}\mu_1, \ldots, \xi_{(\rho\tau)(p)}\nu_{\tau(p)}\mu_p) \\ &= (\tau^{-1}\rho\tau; \mu_{\tau^{-1}((\rho\tau)(1))}^{-1}\nu_{\tau(1)}\mu_1, \ldots, \mu_{\tau^{-1}((\rho\tau)(p))}^{-1}\nu_{\tau(p)}\mu_p) \\ &= (\tau^{-1}\rho\tau; \mu_{(\tau^{-1}\rho\tau)(1)}^{-1}\nu_{\tau(1)}\mu_1, \ldots, \mu_{(\tau^{-1}\rho\tau)(p)}^{-1}\nu_{\tau(p)}\mu_p) \end{aligned}$$

If we write $\gamma = (\tau^{-1}\rho\tau; \lambda_1, \ldots, \lambda_p)$, we obtain

$$\lambda_k = \mu^{-1}_{(\tau^{-1}\rho\tau)(k)} \nu_{\tau(k)} \mu_k, \qquad k = 1, \ldots, p,$$

and at the index j, using $\theta = \nu_i = \nu_{\tau(j)}$,

$$\begin{aligned} \lambda_j &= \mu^{-1}_{(\tau^{-1}\rho\tau)(j)} \nu_{\tau(j)} \mu_j \\ &= \mu^{-1}_{(\tau^{-1}\rho\tau)(j)} \theta \mu_j \end{aligned}$$

Since $i = \tau(j)$ and $\rho(i) = i$,

$$(\tau^{-1}\rho\tau)(j) = (\tau^{-1}\rho)(i) = \tau^{-1}(i) = j,$$

thus

$$\lambda_j = \mu_j^{-1} \theta \mu_j.$$

$\square$