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

$$\begin{cases} h \cdot x_0 & = & x_0, \\ h \cdot (g \cdot x_0) & = & (g \cdot x_0). \end{cases}$$

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 $p = \deg(f) = 7$.

□

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

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

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 $\{1,\dots,6\}$, 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.

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

□

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,

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

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.

□

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

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

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 $n = m$:

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

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. □

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. □

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

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

□

Ex. 14.2.6 *Let A be a subgroup of S_n, and let G be any group. Then define $A \wr G$ as in the Mathematical Notes.*

(a) Prove that $A \wr G$ is a group under the multiplication defined in the Mathematical Notes.

(b) State and prove a version of part (b) of Lemma 14.2.8 for $A \wr G$.

(c) Prove that $|A \wr G| = |A||G|^n$ when G is finite.

Proof. (a) Let G be any group and let $A \subset S_n$ be a permutation group. Then set

$$A \wr G = \{(\tau; g_1, \ldots, g_n) \,|\, \tau \in A,\ g_1, \ldots, g_n \in G\},$$

with an operation on this set defined by

$$(\tau; g_1, \ldots, g_n)(\tau'; g'_1, \ldots, g'_n) = (\tau\tau'; g_{\tau'(1)}g'_1, \ldots, g_{\tau'(n)}g'_n) \in A \wr G.$$

We write e the identity of G, and $()$ the identity of S_n.

- Let $\lambda = (\tau; g_1, \ldots, g_n), \lambda' = (\tau'; g'_1, \ldots, g'_n), \lambda'' = (\tau''; g''_1, \ldots, g''_n)$ be elements of $A \wr G$. Then

$$\begin{aligned}\lambda(\lambda'\lambda'') &= (\tau; g_1, \ldots, g_n)(\tau'\tau''; g_{\tau''(1)}g''_1, \ldots, g_{\tau''(n)}g''_n) \\ &= (\tau\tau'\tau''; g_{(\tau'\tau'')(1)}g'_{\tau''(1)}g''_1, \ldots, g_{(\tau'\tau'')(n)}g'_{\tau''(n)}g''_n) \\ (\lambda\lambda')\lambda'' &= (\tau\tau'; g_{\tau'(1)}g'_1, \ldots, g_{\tau'(n)}g'_n)(\tau''; g''_1, \ldots, g''_n) \\ &= (\tau\tau'; h_1, \ldots, h_n)(\tau''; g''_1, \ldots, g''_n) \qquad (\text{where } h_k = g_{\tau'(k)}g'_k) \\ &= (\tau\tau'\tau''; h_{\tau''(1)}g''_1, \ldots, h_{\tau''(n)}g''_n) \\ &= (\tau\tau'\tau''; g_{\tau'(\tau''(1))}g'_{\tau''(1)}g''_1, \cdots, g_{\tau'(\tau''(n))}g'_{\tau''(n)}g''_n) \\ &= (\tau\tau'\tau''; g_{(\tau'\tau'')(1)}g'_{\tau''(1)}g''_1, \ldots, g_{(\tau'\tau'')(n)}g'_{\tau''(n)}g''_n)\end{aligned}$$

thus $\lambda(\lambda'\lambda'') = (\lambda\lambda')\lambda''$, and the law is associative.

- Write $\varepsilon = ((); e, \ldots, e) = (\iota; e_1, \ldots, e_n)$, where $\iota = ()$, and $e_k = e, k = 1, \ldots, n$. Then

$$\begin{aligned}
\varepsilon\lambda &= (\iota; e_1, \ldots, e_n)(\tau; g_1, \ldots, g_n) \\
&= (\tau; e_{\tau'(1)} g_1, \ldots, e_{\tau'(n)} g_n) \\
&= (\tau; g_1, \ldots, g_n) = \lambda \qquad (\text{since } e_{\tau'(k)} = e) \\
\lambda\varepsilon &= (\tau; g_{\iota(1)} e_1, \ldots, g_{\iota(n)} e_n) \\
&= (\tau; g_1, \ldots, g_n) = \lambda \qquad (\text{since } \iota(k) = k, e_k = e).
\end{aligned}$$

  Therefore $\varepsilon = ((); e, \ldots, e)$ is the identity of $A \wr G$.

- Set $\mu = (\tau^{-1}; h_1, \ldots, h_n) = (\tau^{-1}; g^{-1}_{\tau^{-1}(1)}, \ldots, g^{-1}_{\tau^{-1}(n)})$, with $h_k = g^{-1}_{\tau^{-1}(k)}$, $k = 1, \ldots, n$. Then

$$\begin{aligned}
\lambda\mu &= (\tau; g_1, \ldots, g_n)(\tau^{-1}; h_1, \ldots, h_n) \\
&= ((); g_{\tau^{-1}(1)} h_1, \ldots, g_{\tau^{-1}(n)} h_n) \\
&= ((); g_{\tau^{-1}(1)} g^{-1}_{\tau^{-1}(1)}, \ldots, g_{\tau^{-1}(n)} g^{-1}_{\tau^{-1}(n)}) \\
&= ((); e, \ldots, e) = \varepsilon \\
\mu\lambda &= (\tau^{-1}; h_1, \ldots, h_n)(\tau; g_1, \ldots, g_n) \\
&= ((); h_{\tau(1)} g_1, \ldots, h_{\tau(n)} g_n \\
&= ((); g^{-1}_{\tau^{-1}(\tau(1))} g_1, \ldots, g^{-1}_{\tau^{-1}(\tau(n))} g_n) \\
&= ((); g_1^{-1} g_1, \ldots, g_n^{-1} g_n) = ((); e, \ldots, e) = \varepsilon.
\end{aligned}$$

  Therefore every element in $A \wr G$ is invertible.

  $A \wr G$ is a group under the multiplication defined in the Mathematical Notes.

(b) For the group $A \wr G$ of part (a), where $A \subset S_n$ and G is a group, we show the following lemma:

Lemma. *The map*

$$\varphi \left\{ \begin{array}{ll} A \wr G & \to A \\ (\tau; g_1, \ldots, g_n) & \mapsto \tau \end{array} \right.$$

is a group homomorphism that is surjective and whose kernel is isomorphic to G^n.

Let $\lambda = (\tau; g_1, \ldots, g_n), \lambda' = (\tau'; g'_1, \ldots, g'_n)$ be any elements of $A \wr G$. By definition, $\lambda\lambda' = (\tau\tau'; g_{\tau'(1)} g'_1, \ldots, g_{\tau'(n)} g'_n)$, so that

$$\varphi(\lambda\lambda') = \tau\tau' = \varphi(\lambda)\varphi(\lambda').$$

φ is a group homormphism.

If τ is any element of A, then $\varphi(\tau; e, \ldots, e) = \tau$, where $(\tau; e, \ldots, e) \in A \wr G$. Therefore φ is surjective.

Moreover $(\tau; g_1, \ldots, g_n) \in \ker\varphi$ if and only if $\tau = ()$, therefore

$$\ker\varphi = \{\iota; g_1, \ldots, g_n) \,|\, (g_1, \ldots, g_n) \in G^n\}, \qquad \text{where } \iota = ().$$

Consider

$$\psi \left\{ \begin{array}{ccc} \ker\varphi & \to & G^n \\ (\iota; g_1, \ldots, g_n) & \mapsto & (g_1, \ldots, g_n) \end{array} \right.$$

Then ψ is bijective (with inverse map $(g_1, \ldots, g_n) \mapsto (\iota, g_1, \ldots, g_n)$). We verify that ψ is a group homomorphism: if $\lambda = (\iota; g_1, \ldots, g_n), \lambda' = (\iota; g'_1, \ldots, g'_n)$ are elements of $\ker \varphi$, then

$$\begin{aligned}
\psi(\lambda\lambda') &= \psi((\iota; g_1, \ldots, g_n)(\iota; g'_1, \ldots, g'_n)) \\
&= \psi(\iota; g_{\iota(1)}g'_1, \ldots, g_{\iota(n)}g'_n) \\
&= \psi(\iota; g_1 g'_1, \ldots, g_n g'_n) \qquad (\text{since } \iota(k) = k) \\
&= (g_1 g'_1, \ldots, g_n g'_n) \\
&= (g_1 \ldots, g_n)(g'_1, \ldots, g'_n) \\
&= \psi(\lambda)\psi(\lambda').
\end{aligned}$$

So ψ is an group isomorphism, and $\ker \varphi \simeq G^n$.

(c) By part (b), since φ is a surjective homomorphism,

$$(A \wr G)/\ker \varphi \simeq A,$$

and $\ker \varphi \simeq G^n$. Therefore

$$|A| = |A \wr G|/|\ker \varphi| = |A \wr G|/|G|^n,$$

which proves

$$|A \wr G| = |A||G|^n.$$

□

Ex. 14.2.7 *Let $A \wr G$ be as in Exercise 6, and let H be the set of all functions*

$$\phi : \{1, \ldots, n\} \to G.$$

(a) Given $\phi, \chi \in H$, define $\phi\chi \in H$ by $(\phi\chi)(i) = \phi(i)\chi(i)$. Prove that this makes H into a group isomorphic to the product group G^n.

(b) Elements of $A \wr G$ can be written (τ, ϕ), where $\phi \in H$. Prove that in this notation, (14.7) becomes

$$(\tau, \phi)(\tau', \phi') = (\tau\tau', ((\tau')^{-1} \cdot \varphi)\phi').$$

(c) $A \subset S_n$ acts on $\{1, \ldots, n\}$. Show that this induces an action of A on H via $(\tau \cdot \phi)(i) = \phi(\tau^{-1}(i))$. Be sure you understand why the inverse is necessary.

(d) The action of part (c) enable us to define the semidirect product $H \rtimes A$. Using the description of $A \wr G$ given in part (b), prove that the map

$$(\tau, \phi) \mapsto (\tau \cdot \phi, \tau)$$

defines a group isomorphism $A \wr G \simeq H \rtimes A$. This shows that wreath products can be represented as semidirect products.

Proof. (a) Consider the two maps

$$\varphi \left\{ \begin{array}{ccc} H & \to & G^n \\ \phi & \mapsto & (\phi(1), \ldots, \phi(n)), \end{array} \right. \qquad \psi \left\{ \begin{array}{ccc} G^n & \to & H \\ (x_1, \ldots, x_n) & \mapsto & \xi \left\{ \begin{array}{ccc} \{1, \ldots, n\} & \to & G \\ i & \mapsto & x_i. \end{array} \right. \end{array} \right.$$

Then $\psi \circ \varphi = 1_H$ and $\varphi \circ \psi = 1_{G^n}$, therefore φ is bijective.

Moreover, for all $(\phi, \chi) \in H$,

$$\begin{aligned}\varphi(\phi\chi) &= ((\phi\chi)(1), \ldots, (\phi\chi)(n)) \\ &= (\phi(1)\chi(1), \ldots, \phi(n)\chi(n)) \\ &= (\phi(1), \ldots, \phi(n))(\chi(1), \ldots, \chi(n)) \\ &= \varphi(\phi)\varphi(\chi)).\end{aligned}$$

Therefore $H \simeq G^n$ via φ.

(b,c) If we define ϕ^τ, for $\tau \in S_n$ and $\phi \in H$, by $(\phi^\tau)(i) = \phi(\tau(i)),\ i = 1, \ldots, n$, we obtain a right action: if $\tau, \tau' \in S_n$, for all $i \in \{1, \ldots, n\}$,

$$((\phi^\tau)^{\tau'})(i) = (\phi^\tau)(\tau'(i)) = \phi(\tau(\tau'(i))) = \phi((\tau\tau')(i)) = \phi^{\tau\tau'}(i)),$$

thus $(\phi^\tau)^{\tau'} = \phi^{\tau\tau'}$. To obtain a left action, we must define, as in part (c),

$$(\tau \cdot \phi)(i) = \phi(\tau^{-1}(i)),\ i = 1, \ldots, n.$$

Then

$$(\tau' \cdot (\tau \cdot \phi))(i) = (\tau \cdot \phi)(\tau'^{-1}(i)) = \phi(\tau^{-1}(\tau'^{-1}(i))) = \phi(\tau'\tau)^{-1}(i) = ((\tau'\tau) \cdot \phi)(i),$$

so that $\tau' \cdot (\tau \cdot \phi) = (\tau'\tau) \cdot \phi)$ (and $e \cdot \tau = \tau$).

This is a proof of part (c), and this explains the recurrent and stressful injonction from D.A.Cox "**Be sure you understand** why the inverse is necessary".

Using this action for part (b), we define (τ, ϕ) for $\tau \in S_n, \phi \in H = G^{\{1, \cdots, n\}}$,by

$$(\tau, \phi) = (\tau; \phi(1), \ldots, \phi(n)),$$

so that

$$(\tau, \phi) = (\tau; g_1, \ldots, g_n) \iff \phi(1) = g_1, \ldots, \phi(n) = g_n.$$

If $(\tau, \phi) = (\tau; g_1, \ldots, g_n), (\tau', \phi') = (\tau; g'_1, \ldots, g'_n)$, then

$$\begin{aligned}(\tau, \phi)(\tau', \phi') &= (\tau; g_1, \ldots, g_n)(\tau; g'_1, \ldots, g'_n) \\ &= (\tau\tau'; g_{\tau'(1)}g'_1, \ldots, g_{\tau'(n)}g'_n) \\ &= (\tau\tau'; \phi(\tau'(1))\phi'(1), \ldots, \phi(\tau'(n))\phi'(n) \\ &= (\tau\tau'; ((\tau')^{-1} \cdot \phi)(1)\phi'(1), \ldots, ((\tau')^{-1} \cdot \phi)(n))\phi'(n) \\ &= (\tau\tau', ((\tau')^{-1} \cdot \phi)\phi').\end{aligned}$$

(d) Consider the map

$$\varphi \begin{cases} A \wr G & \to & H \rtimes A \\ (\tau, \phi) & \mapsto & (\tau \cdot \phi, \tau). \end{cases}$$

If $\psi : H \rtimes A \to A \wr G$ is defined by $\psi(\chi, \tau) = (\tau, \tau^{-1} \cdot \chi)$, then, for all $\tau \in S_n, \phi, \chi \in H$,

$$\begin{aligned}(\psi \circ \varphi)(\tau, \phi) &= \psi(\tau \cdot \phi, \tau) = (\tau, \tau^{-1} \cdot (\tau \cdot \phi) = (\tau, \phi), \\ (\varphi \circ \psi)(\chi, \tau) &= \varphi(\tau, \tau^{-1} \cdot \chi) = (\tau \cdot (\tau^{-1} \cdot \chi), \tau) = (\chi, \tau).\end{aligned}$$

Thus $\psi \circ \varphi = 1_{A \wr G},\ \varphi \circ \psi = 1_{H \rtimes A}$. This proves that φ is bijective.

Recall that the binary operation in $H \rtimes A$ is defined by (6.9):

$$(\phi, \tau)(\phi', \tau') = (\phi(\tau \cdot \phi'), \tau\tau').$$

We verify that φ is a group homomorphism. Note first that, for $\tau \in S_n, \phi\chi \in H$,

$$\tau \cdot (\phi\chi) = (\tau \cdot \phi)(\tau \cdot \chi).$$

Indeed, for all $i \in \{1, \ldots, n\}$,

$$\begin{aligned}(\tau \cdot (\phi\chi))(i) &= (\phi\chi)(\tau^{-1}(i)) \\ &= \phi(\tau^{-1}(i))\chi(\tau^{-1}(i)) \\ &= (\tau \cdot \phi)(i)(\tau \cdot \chi)(i) \\ &= ((\tau \cdot \phi)(\tau \cdot \chi))(i).\end{aligned}$$

Using this rule, we obtain

$$\begin{aligned}\varphi((\tau, \phi)(\tau', \phi')) &= \varphi(\tau\tau'; ((\tau')^{-1} \cdot \phi)\phi') \\ &= ((\tau\tau') \cdot ((\tau')^{-1} \cdot \phi)\phi'), \tau\tau') \\ &= ((\tau\tau') \cdot ((\tau')^{-1} \cdot \phi)((\tau\tau') \cdot \phi'), \tau\tau') \\ &= ((\tau \cdot \phi)((\tau\tau') \cdot \phi'), \tau\tau'),\end{aligned}$$

and using the binary operation in $H \rtimes A$,

$$\begin{aligned}\varphi(\tau, \phi)\varphi(\tau', \phi') &= (\tau \cdot \phi, \tau)((\tau' \cdot \phi', \tau') \\ &= ((\tau \cdot \phi)(\tau \cdot (\tau' \cdot \phi')), \tau\tau') \\ &= ((\tau \cdot \phi)((\tau\tau') \cdot \phi'), \tau\tau'),\end{aligned}$$

thus $\varphi((\tau, \phi)(\tau', \phi')) = \varphi(\tau, \phi)\varphi(\tau', \phi')$. We have proved that φ is a group isomorphism, so

$$A \wr G \simeq H \rtimes A = G^{\{1,\ldots,n\}} \rtimes A.$$

Wreath products can be represented by semidirect products.

□

Ex. 14.2.8 *The goal of this exercise is to relate Definition 14.2.2 to Galois's definition of not primitive. Let $f \in F[x]$ be monic, separable, and irreducible with splitting field $F \subset L$. Also assume that f is imprimitive with blocks of roots given by $R_1, \ldots, R_m$, where each block has n elements (thus $\deg(f) = mn$). Let f_i be the monic polynomial whose roots are the elements of R_i, and let $K \subset L$ be the fixed field of*

$$\{\sigma \in \mathrm{Gal}(L/F) \,|\, \sigma(R_i) = R_i \text{ for all } i\}.$$

(a) Show that $f = \prod_{i=1}^m f_i$ and that $f_i \in K[x]$ for all i.

(b) In Galois' definition, K is obtained by adjoining the roots of a separable polynomial of degree m. In modern terms, Galois wants $F \subset K$ to be Galois extension such that $\mathrm{Gal}(K/F)$ (*) is isomorphic to a subgroup of S_m. Prove that the field K defined in part (a) has these properties. See Exercise 14 for some examples.

[(*) misprint in Cox.]

Proof. (a) By Definition 14.2.2, $R = R_1 \cup \cdots \cup R_m$ (disjoint union) is the set of roots of f. Since f is separable, by definition of f_i,

$$f = \prod_{\alpha \in R} (x - \alpha) = \prod_{i=1}^{m} \prod_{\alpha \in R_i} (x - \alpha) = \prod_{i=1}^{m} f_i.$$

Let

$$G = \{\sigma \in \mathrm{Gal}(L/F) \,|\, \forall i \in [\![1, m]\!],\ \sigma(R_i) = R_i\}.$$

If $G_i = \{\sigma \in \mathrm{Gal}(L/F) \,|\, \sigma(R_i) = R_i\}$ for $i = 1, \ldots, n$, then $G = \bigcap_{i=1}^{m} G_i$.

Each G_i is a subgroup of $\mathrm{Gal}(L/F)$: $e(R_i) = R_i$, and if $\sigma, \tau \in R_i$, then $(\sigma\tau)(R_i) = \sigma(R_i) = R_i$ and $R_i = \sigma^{-1}(R_i)$. Therefore $G = \bigcap_{i=1}^{m} G_i$ is a subgroup of $\mathrm{Gal}(L/F)$.

Let $K = L_G$ be the fixed field of G. By the Galois correspondence, $G = \mathrm{Gal}(L/K)$.

If $\sigma \in G_i$, since $\sigma(R_i) = R_i$, where le restriction of σ to R_i is bijective, then

$$\sigma \cdot f_i = \prod_{\alpha \in R_i} (x - \sigma(\alpha)) = \prod_{\beta \in R_i} (x - \beta) = f_i, \qquad (\beta = \sigma(\alpha)).$$

Therefore, if $\sigma \in G = \bigcap_{i=1}^{m} G_i$, then for all $i \in \{1, \ldots, m\}$, $\sigma \cdot f_i = f_i$. The coefficients of f_i are in the fixed field K of G, so that

$$f_i \in K[x],\ i = 1, \ldots, m.$$

To give a first example, $f = x^4 - 2$ is imprimitive with blocks

$$R_1 = \{\sqrt[4]{2}, -\sqrt[4]{2}\}, R_2 = \{i\sqrt[4]{2}, -i\sqrt[4]{2}\}.$$

If τ, σ are defined by $\tau(\sqrt[4]{2}) = \sqrt[4]{2}, \tau(i) = -i$, and $\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}, \sigma(i) = i$, then

$$\mathrm{Gal}(L/F) = \{e, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\} \simeq D_8.$$

Here $G = G_1 = G_2 = \{e, \sigma^2, \tau, \sigma^2\tau\}$, and $K = L_G = \mathbb{Q}(\sqrt{2})$ (see Ex. 6.3.2 and Ex. 7.3.3).

We verify $f_1(x) = x^2 - \sqrt{2}, f_2(x) = x^2 + \sqrt{2} \in K[x]$.

(b) We prove that G is a normal subgroup of $\mathrm{Gal}(L/F)$.

Let $\lambda \in \mathrm{Gal}(L/F)$, and $\sigma \in G$. Since f is imprimitive, $\lambda \in \mathrm{Gal}(L/F)$ permutes the blocks R_i: there exists $\tau \in S_m$ such that

$$\lambda(R_i) = R_{\tau(i)},\ i = 1, \ldots, m.$$

Let j be any fixed index in $\{1, \ldots, m\}$, and i such that $\tau(i) = j$. Since $\sigma \in G \supset G_i$, $\sigma(R_i) = R_i$, thus

$$(\lambda\sigma\lambda^{-1})(R_j) = (\lambda\sigma)(R_i) = \lambda(R_i) = R_j.$$

Since this is true for all $j \in \{1, \ldots, m\}$, $\lambda\sigma\lambda^{-1} \in G$. This proves that G is a normal subgroup of $\mathrm{Gal}(L/F)$. Therefore $F \subset K$ is a Galois extension (Theorem 7.2.5).

Now we prove that $\mathrm{Gal}(K/F)$ is isomorphic to a subgroup of S_m.

Since f is imprimitive with blocks of roots given by $R_1, \ldots, R_m$, for each $\sigma \in \mathrm{Gal}(L/F)$, there exists $\tau \in S_m$ such that $\sigma(R_i) = R_{\tau(i)},\ i = 1, \ldots, m$. Consider the map φ sending σ to τ:

$$\varphi \left\{ \begin{array}{ccc} \mathrm{Gal}(L/F) & \to & S_m \\ \sigma & \mapsto & \tau : \forall i \in [\![1, m]\!],\ \sigma(R_i) = R_{\tau(i)}. \end{array} \right.$$

Then , for all $\sigma \in \mathrm{Gal}(L/F)$,

$$\varphi(\sigma) = () \iff \forall i \in [\![1, m]\!],\ \sigma(R_i) = R_i \iff \sigma \in G.$$

Therefore, $\ker(\varphi) = G$, and by the Galois correspondence (see part (a)) $G = \mathrm{Gal}(L/K)$, so that

$$\ker(\varphi) = G = \mathrm{Gal}(L/K).$$

Then, by Theorem 7.3.2, since K is Galois over F,

$$S_m \supset \mathrm{im}(\varphi) \simeq \mathrm{Gal}(L/F)/\ker(\varphi) = \mathrm{Gal}(L/F)/\mathrm{Gal}(L/K) \simeq \mathrm{Gal}(K/F).$$

Therefore $\mathrm{Gal}(K/F)$ is isomorphic to the subgroup $\mathrm{im}(\varphi)$ of S_m.

□

Ex.14.2.9 Assume that $G \subset S_n$ is transitive and Abelian.

(a) Prove that $|G| = n$ by considering the isotropy subgroups of G.

(b) Prove that G is primitive if and only if $|G|$ is prime.

Thus a transitive Abelian permutation group is imprimitive unless it is cyclic of prime order.

Proof.

(a) $G \subset S_n$ acts on $\{1, \ldots, n\}$ by the action defined by $\sigma \cdot k = \sigma(k),\ \sigma \in G, k \in \{1, \ldots, n\}$.

Consider the isotropy group G_1 of 1: $G_1 = \{\sigma \in G \,|\, \sigma(1) = 1\}$. Let σ be any permutation in G_1, and let i be any element in $\{1, \ldots, n\}$. Since G is transitive, there exists $\tau \in G$ such that $\tau(1) = i$. By hypothesis, G is Abelian, therefore

$$\sigma(i) = (\sigma\tau)(1) = (\tau\sigma)(1) = \tau(1) = i.$$

Since this is true for all $i \in \{1, \ldots, n\}$, $\sigma = e$. This proves $G_1 = \{e\}$.

Moreover, since G is transitive, the orbit of 1 is $G \cdot 1 = \{1, \ldots, n\}$, thus $|G \cdot 1| = n$.

By the Fundamental Theorem of Group Actions,

$$|G \cdot 1| = (G : G_1) = |G|,$$

thus $|G| = n$.

(b) By Lemma 14.2.7, if $G \subset S_n$ is transitive and imprimitive, then $n = kl,\ k > 1, l > 1$, is composite. Thus, if n is prime, a transitive subgroup of S_n is primitive.

Conversely, let G be a transitive Abelian subgroup of S_n, where $n > 1$ is composite. By part (a), $|G| = n$. We must prove that G is imprimitive.

By the Kronecker's Theorem on the structure of Abelian groups,

$$G \simeq C_{n_1} \times \cdots \times C_{n_r}$$

is a product of cyclic groups.

Therefore, either G is cyclic of order n, or $G = HK \simeq H \times K, H \neq \{e\}, K \neq \{e\}$ is a direct product of two non trivial subgroups (take for instance $H \simeq C_{n_1}, K \simeq C_{n_2} \times \cdots \times C_{n_r}$). We will deal with these two cases.

• Case 1. We assume that $G \simeq C_n$ is cyclic, where $n = ml,\ m > 1, l > 1$. Then $G = \langle \sigma \rangle$, where the permutation σ has order n. Take

$$\begin{aligned} R_1 &= \{1, \sigma^m(1), \ldots, \sigma^{(l-1)m}(1)\}, \\ R_2 &= \{\sigma(1), \sigma^{m+1}(1), \ldots, \sigma^{(l-1)m+1}(1)\} = \sigma(R_1), \\ &\cdots \\ R_m &= \{\sigma^{m-1}(1), \sigma^{m+m-1}(1), \ldots, \sigma^{lm-1}(1)\} = \sigma^{m-1}(R_1). \end{aligned}$$

Since G is transitive,

$$R_1 \cup \cdots \cup R_m = \{1, \sigma(1), \ldots, \sigma^{n-1}(1)\} = G \cdot 1 = \{1, \ldots, n\}.$$

Moreover, if $\tau \in G$, then $\tau = \sigma^j,\ j = 0, \ldots, n-1$, thus, using $\sigma^n = e$, if k is the remainder of $i + j - 1$ modulo n,

$$\tau(R_i) = (\sigma^j \sigma^{i-1})(R_1) = \sigma^{i+j-1}(R_1) = \sigma^k(R_1) = R_{k+1}.$$

This proves that G is imprimitive, with blocks $R_1, \ldots, R_m$.

• Case 2. Now, assume that $G = HK \simeq H \times K, |H| = l > 1, |K| = m > 1$. Then $n = ml$. Write

$$\begin{aligned} H &= \{\sigma_1 = e, \ldots, \sigma_l\}, \\ K &= \{\tau_1 = e, \ldots, \tau_m\}, \end{aligned}$$

and take

$$\begin{aligned} R_1 &= \{(\sigma_1\tau_1)(1), \ldots, (\sigma_l\tau_1)(1)\}, \\ R_2 &= \{(\sigma_1\tau_2)(1), \ldots, (\sigma_l\tau_2)(1)\}, \\ &\cdots \\ R_m &= \{(\sigma_1\tau_m)(1), \ldots, (\sigma_l\tau_m)(1)\}. \end{aligned}$$

Since $G = HK$, every permutation $\lambda \in G$ is a product $\lambda = \sigma_i\tau_j,\ 1 \leq i \leq l, 1 \leq j \leq m$, and since G is transitive,

$$R_1 \cup \cdots \cup R_m = G \cdot 1 = \{1, \ldots, n\}.$$

Take $\lambda = \sigma_i\tau_j \in G$, and $R_k = \{\sigma_u\tau_k, 1 \leq u \leq n\}$. Then $\tau_j\tau_k = \tau_r$ for some fixed $r \in \{1, \ldots, m\}$. Since G is Abelian,

$$\lambda(R_k) = \{(\sigma_i\sigma_u\tau_j\tau_k)(1), 1 \leq u \leq n\} = \{(\sigma_i\sigma_u\tau_r)(1), 1 \leq u \leq n\} = \{(\sigma_v\tau_r)(1), 1 \leq v \leq n\} = R_r,$$

because the map $H \to H$, $\sigma_u \mapsto \sigma_i\sigma_u$ is bijective.

This proves that G is imprimitive, with blocks $R_1, \ldots, R_m$.

To conclude, G is primitive if and only if $|G|$ is prime (or $|G| = 1$). Thus a non trivial transitive Abelian permutation group is imprimitive unless it is cyclic of prime order.

Examples: $G = \{(), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$ is a transitive Abelian subgroup of S_4, and an example of Case 2. If H, K are two distinct subgroups of G with order 2, then $G = HK \simeq C_2 \times C_2$. We can take $R_1 = \{1, 2\}, R_2 = \{3, 4\}$, but we can also take $R_1' = \{1, 3\}, R_2' = \{2, 4\}$. G is imprimitive with blocks R_1, R_2, or with blocks R_1', R_2'.

$G' = \langle(1\,2\,3\,4)\rangle$ is a another transitive Abelian subgroup of S_4, and an example of Case 1. This times, we can take only $R_1 = \{1, 3\}, R_2 = \{2, 4\}$. □

Ex.14.2.10 *Let $\Phi_p(x)$ be the cyclotomic polynomial whose roots are the primitive pth roots of unity, where p is prime. We know that $\Phi_p(x)$ is irreducible of degree $p - 1$. In the quotation given in the Historical Notes, Galois asserts that $\Phi_p(x)$ is imprimitive.*

(a) Prove Galois's claim for $p > 3$ using Exercise 9.

(b) Explain why we need to assume that $p > 3$ in part (a).

Proof.

(a) We know that the splitting field of $\Phi_p(x)$ over $\mathbb{Q}$ is $L = \mathbb{Q}(\zeta_p)$ (where $\zeta_p = e^{\frac{2i\pi}{p}}$), and that $\mathrm{Gal}(L/\mathbb{Q}) \simeq (\mathbb{Z}/p\mathbb{Z})^*$, via the isomorphism

$$\begin{cases} \mathrm{Gal}(L/\mathbb{Q}) & \to & (\mathbb{Z}/p\mathbb{Z})^* \\ \sigma & \mapsto & a : \sigma(\zeta_p) = \zeta_p^a. \end{cases}$$

Therefore, $\mathrm{Gal}(L/\mathbb{Q})$ is Abelian, and even cyclic with order $p - 1$. Let $\mathrm{Gal}(L/\mathbb{Q}) \simeq G \subset S_{p-1}$. If $p > 3$, then $p - 1$ is not prime, and Exercise 9 prove that G_n is imprimitive, so that $\Phi_p(x)$ is imprimitive.

(b) If $p = 3$, $p - 1 = 2$ is prime, and $(\mathbb{Z}/3\mathbb{Z})^* = \{1, -1\}$ is cyclic of prime order. Moreover $\Phi_3(x) = x^2 + x + 1$ is not imprimitive, as every polynomial of degree 2: by Definition 14.2.2, if f is imprimitive, since $k > 1, l > 1$, $\deg(f) \geq |R_1| + |R_2| > 2$.

If $p = 2$, $(\mathbb{Z}/2\mathbb{Z})^* = \{1\}$, and $\Phi_2(x) = x + 1$. Since $\deg(\Phi_2) = 1$, $\Phi_2(x)$ is not imprimitive.

□

Ex. 14.2.11 *Given a prime p, let $C_p \subset S_p$ be the cyclic subgroup generated by the p-cycle $(1\,2 \cdots p)$. As explained in the text, this gives the wreath product $C_p \wr C_p \subset S_{p^2}$. Prove that $C_p \wr C_p$ is a p-Sylow subgroup of S_{p^2}.*

Proof. By Lemma 14.2.8, we know that $C_p \wr C_p$ is a subgroup of $S_p \wr S_p$, which may be viewed as S_{p^2}.

Exercise 6 shows that $|C_p \wr C_p| = |C_p||C_p|^p = p^{p+1}$.

Moreover $|S_{p^2}| = (p^2)!$, and, if $\nu_p(n)$ is the exponent of p in the prime factorization of $n!$, then

$$\nu_p(n!) = \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^k} \right\rfloor + \cdots .$$

(see for instance Ex. 2.6 in Ireland and Rosen)

Therefore

$$\begin{aligned}\nu_p((p^2)!) &= \left\lfloor \frac{p^2}{p} \right\rfloor + \left\lfloor \frac{p^2}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{p^2}{p^k} \right\rfloor + \cdots \\ &= \left\lfloor \frac{p^2}{p} \right\rfloor + \left\lfloor \frac{p^2}{p^2} \right\rfloor \\ &= p + 1.\end{aligned}$$

Therefore p^{p+1} is the maximal power of p which divides $(p^2)! = S_{p^2}$, so that $C_p \wr C_p$ is a p-Sylow subgroup of S_{p^2}. □

Ex. 14.2.12 *Let f be an irreducible imprimitive polynomial of degree 6,8 or 9 over a field F of characteristic 0. Prove that f is solvable by radicals over F.*

Proof. Write L the splitting field of f. Since the characteristic of F is 0, the irreducible polynomial f is separable, so f is separable, irreducible and imprimitive. By Corollary 14.2.10, $G = \mathrm{Gal}(L/F)$ is isomorphic to a subgroup of $S_k \wr S_l$, where $n = kl$ is a nontrivial factorization. The only nontrivial factorizations of 6,8 or 9 are

$$6 = 2 \times 3 = 3 \times 2, \qquad 8 = 2 \times 4 = 4 \times 2, \qquad 9 = 3 \times 3.$$

Thus G is isomorphic to a subgroup of the list

$$S_2 \wr S_3, S_3 \wr S_2, S_4 \wr S_2, S_2 \wr S_4, S_3 \wr S_3,$$

whose cardinalities are

$$\begin{aligned}|S_2 \wr S_3| &= 2!3^2 = 2 \times 3^2, \\ |S_3 \wr S_2| &= 3!2^3 = 2^4 \times 3, \\ |S_4 \wr S_2| &= 4!2^4 = 2^7 \times 3, \\ |S_2 \wr S_4| &= 2!4^2 = 2^5, \\ |S_3 \wr S_3| &= 3!3^3 = 2 \times 3^4.\end{aligned}$$

So $S_k \wr S_l$ has only two prime factors 2 and 3. By Burnside's Theorem (Theorem 8.1.8), $S_k \wr S_l$ solvable for these values of k, l, thus the subgroup G is solvable. Since the characteristic of F is 0, this proves that f is solvable by radicals over f. □

Ex. 14.2.13 *Let $f = x^6 + bx^3 + c \in F[x]$ be irreducible, where F has characteristic different from 2 or 3. We will study the size of the Galois group of f over F.*

(a) Show that f is separable. So we can think of the Galois group as a subgroup of S_6.

(b) Show that $x^6 + bx^3 + c$ is imprimitive and that its Galois group lies in $S_2 \wr S_3$. Also show that $|S_2 \wr S_3| = 72$. Thus the Galois group has order ≤ 72.

(c) Let $F \subset L$ be the splitting field of f over F. Use the Tower Theorem to show that $[L : F] \leq 36$. Hence the Galois group has order at most 36.

Using Maple or Sage, one can show that the Galois group of $x^6 + 2x^3 - 2$ over $\mathbb{Q}$ has order 36 and hence is as large as possible.

Proof.

(a) Since F has characteristic different from 2 or 3, $f' = 6x^5 + 3bx^2 \neq 0$. By hypothesis, f is irreducible, thus any factor of f is associate to f or 1. Since $f' \neq 0$, $\gcd(f, f')$ divides f', thus $\deg(\gcd(f, f')) \leq \deg(f') = 5$, and $\gcd(f, f')$ is a factor of f, which cannot be associate to f, therefore $\gcd(f, f') = 1$. This proves that f is separable.

(b) If α is a root of f in L, then $\lambda = \alpha^3 \in L$ is a root of $g = x^2 + bx + c$. Let $\mu = -b - \lambda \in L$. Then μ is a root of g:

$$\mu^2 + b\mu + c = (-b - \lambda)^2 + b(-b - \lambda) + c = \lambda^2 + b\lambda + c = 0.$$

Moreover $\lambda \neq \mu$, otherwise $b = -2\lambda, c = -\lambda^2 - b\lambda = \lambda^2$, and $g = (x - \lambda)^2$, where $\lambda = -b/2 \in F$, so that $f = g(x^3) = (x^3 - \lambda)^2$ would not be irreducible over f. Therefore

$$g = (x - \lambda)(x - \mu), \qquad \lambda \neq \mu.$$

Write $K = F(\lambda, \mu)$. Then $F \subset K \subset L$ is an intermediate field which is a splitting field of g over F. If $\lambda \in F$, then $\mu \in F$ and $f = g(x^3) = (x^3 - \lambda)(x^3 - \mu)$ would not be irreducible over F. Therefore $\lambda \notin F, \mu \notin F$, g is irreducible over F. K is the splitting field of the separable polynomial g, thus $F \subset K$ is a Galois extension, where $F \subsetneq K \subset L$.

Moreover,

$$f = g(x^2) = (x^3 - \lambda)(x^3 - \mu) = f_1 f_2,$$

where $f_1 = x^3 - \lambda, f_2 = x^3 - \mu \in K[x]$. Therefore three roots $\alpha, \alpha', \alpha''$ of f are the roots of $x^3 - \lambda$, and three other roots β, β', β'' of f are the roots of $x^3 - \mu$:

$$\alpha^3 = \alpha'^3 = \alpha''^3 = \lambda, \qquad \beta^3 = \beta'^3 = \beta''^3 = \mu.$$

This gives the blocks

$$R_1 = \{\alpha, \alpha', \alpha''\}, \qquad R_2 = \{\beta, \beta', \beta''\}.$$

If $\sigma \in \mathrm{Gal}(L/F)$, then $g = \sigma \cdot g = (x - \sigma(\lambda))(x - \sigma(\mu))$, thus $\{\lambda, \mu\} = \{\sigma(\lambda), \sigma(\mu)\}$: σ fixes λ, μ, or exchanges λ, μ. Since α, β, γ are the roots of $x^3 - \lambda$, $\sigma(\alpha), \sigma(\beta), \sigma(\gamma)$ are the roots of $x^3 - \sigma(\lambda)$, thus $\sigma(R_1) = R_1$ or $\sigma(R_1) = R_2$, and similarly $\sigma(R_2) = R_1$ or R_2. This proves that f is imprimitive, with blocks R_1, R_2, and $\mathrm{Gal}(L/F)$ is isomorphic to a subgroup of $S_2 \wr S_3$(Corollary 14.2.10), whose order is $2(3!)^2 = 72$ (see Ex. 6 (c)).

(c) We don't know if F or K contains the cubic roots of unity, but L does: since α, α' are two distinct roots of $x^3 - \lambda$ (where $\alpha \neq 0$, otherwise $\lambda = 0 \in F$), then $(\frac{\alpha'}{\alpha})^3 = 1$. If we write $\omega = \frac{\alpha'}{\alpha}$, then $\omega \in L$ and $\omega^3 = 1, \omega \neq 1$, thus $1, \omega, \omega^2$ are three distinct roots of $x^3 - 1$, and $1 + \omega + \omega^2 = 0$, so that $[K(\omega) : K] = 1$ or 2.

Then the six roots of f are

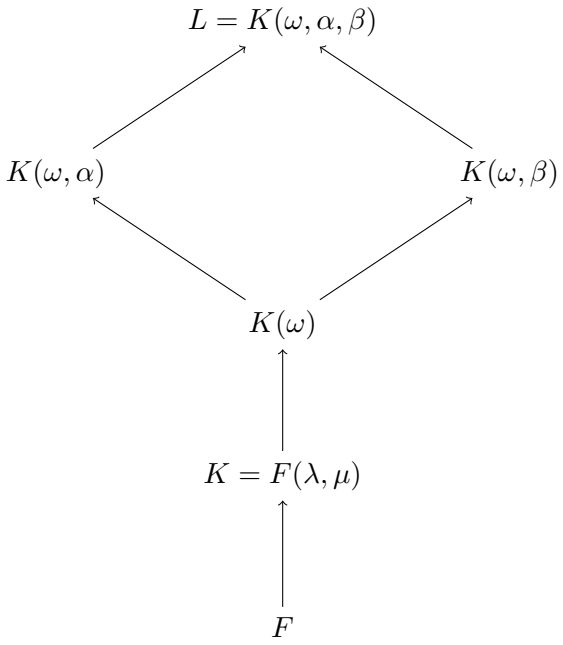
$$\alpha_1 = \alpha, \alpha_2 = \omega\alpha, \alpha_3 = \omega^2\alpha, \alpha_4 = \alpha', \alpha_5 = \omega\alpha', \alpha_6 = \omega^2\alpha'.$$

Therefore

$$L = F(\alpha, \omega\alpha, \omega^2\alpha, \beta, \omega\beta, \beta^2) = F(\omega, \alpha, \beta) = K(\omega, \alpha, \beta).$$

Consider the chain of fields

$$F \subset K = F(\lambda, \mu) \subset K(\omega) \subset K(\omega, \alpha) \subset L = K(\omega, \alpha, \beta).$$



• Since λ, μ are the roots of the irreducible polynomial f, $K = F(\lambda, \mu)$ is a quadratic extension of F, so $[K : F] = 2$.

• Since $\omega^2 + \omega + 1 = 0$, $[K(\omega) : K] \leq 2$.

• Since $\alpha^3 - \lambda = 0$, where $\lambda \in K \subset K(\omega)$, $[K(\omega, \alpha) : K(\omega)] \leq 3$.

• Since $\beta^3 - \mu = 0$, where $\mu \in K \subset K(\omega, \alpha)$, $[K(\omega, \alpha, \beta) : K(\omega, \alpha)] \leq 3$.

By the Tower Theorem,

$$[L : K] = [K(\omega, \alpha, \beta) : K] = [K(\omega, \alpha, \beta) : K(\omega, \alpha)][K(\omega, \alpha) : K(\omega)][K(\omega) : K] \leq 3{\times}3{\times}2{\times}2 = 36.$$

Therefore,

$$|\mathrm{Gal}(L/K)| = [L : K] \leq 36.$$

□

Note : Some permutations of $S_2 \wr S_3$ can't lie in the Galois group $G \subset S_6$ of f, for instance if the transposition $(4\,5)$ corresponds to $\sigma \in \mathrm{Gal}(L/F)$, given by

$$\begin{pmatrix} \alpha & \omega\alpha & \omega^2\alpha & \beta & \omega\beta & \omega^2\beta \\ \alpha & \omega\alpha & \omega^2\alpha & \omega\beta & \beta & \omega^2\beta \end{pmatrix},$$

then $\sigma(\alpha) = \alpha$ and $\sigma(\omega\alpha) = \omega\alpha$ show that $\sigma(\omega) = \omega$, and $\sigma(\beta) = \omega\beta$ implies $\sigma(\omega\beta) = \omega^2\beta \neq \beta$. This contradiction proves that $(4\,5) \notin G$ (but $(4\,5) \in S_3 \wr S_2 \subset S_6$). More generally, all odd permutations are impossible, so that G is a subgroup of $(S_2 \wr S_3) \cap A_6$.

Ex. 14.2.14 *Here are some examples to illustrate Galois's definition of imprimitive. We will use the notation of Exercise 8. Let F be a field of characteristic different from 2 or 3.*

(a) Let $f = x^6 + bx^4 + cx^2 + d \in F[x]$ be irreducible with splitting field $F \subset L$. Show that the splitting field of $x^3 + bx^2 + cx + d$ gives an intermediate field $F \subset K \subset L$ such that $F \subset K$ is Galois and $f = f_1 f_2 f_3$, where $f_i \in K[x]$ has degree 2 for $i = 1, 2, 3$. Also explain how K relates to the field K constructed in Exercise 8.

(b) Work out the analogous theory when $f = x^6 + bx^3 + c \in F[x]$ is irreducible.

Proof.

(a) By hypothesis, $f = x^6 + bx^4 + cx^2 + d$ is irreducible. Since the characteristic of F is different from 2 or 3, $f' = 6x^5 + \cdots \neq 0$, thus $\gcd(f, f') = 1$, and f is separable.

If α is a root of f, then $-\alpha$ is a root of f. Moreover $\alpha \neq 0$, otherwise $d = 0$ and f would not be irreducible, therefore $\alpha \neq -\alpha$. Since f is separable, the roots of f can be partitioned into three blocks

$$R_1 = \{\alpha, -\alpha\}, \qquad R_2 = \{\beta, -\beta\}, \qquad R_3 = \{\gamma, -\gamma\}.$$

If $\sigma \in \mathrm{Gal}(L/F)$ and if $\lambda \in R_i$ is a root of f, then $\sigma(\lambda) \in R_j$ for some index λ, and $\sigma(-\lambda) = -\sigma(\lambda) \in R_j$, thus $\sigma(R_i) = R_j$. Therefore f is imprimitive, with blocks R_1, R_2, R_3. By Corollary 14.2.10, $\mathrm{Gal}(L/F)$ is isomorphic to a subgroup of $S_3 \wr S_2$.

Since $\alpha, -\alpha, \beta, -\beta, \gamma, -\gamma$ are the distinct roots of f, then $\alpha^2, \beta^2, \gamma^2$ are distinct and they are the roots of $g = x^3 + bx^2 + cx + d$. Therefore

$$g = x^3 + bx^2 + cx + d = (x - \alpha^2)(x - \beta^2)(x - \gamma^2),$$

so that a splitting field K of g over F is

$$K = F(\alpha^2, \beta^2, \gamma^2), \qquad F \subset K \subset L.$$

Since K is the splitting field of the separable polynomial g, $F \subset K$ is a Galois extension. Note that g is irreducible over F, otherwise any non trivial factorization of g over F gives a factorisation of f over F. Therefore $K \neq F$.

Moreover,

$$f = g(x^2) = (x^2 - \alpha^2)(x^2 - \beta^2)(x^2 - \gamma^2) = f_1 f_2 f_3,$$

where $f_1 = x^2 - \alpha^2, f_2 = x^2 - \beta^2, f_3 = x^2 - \gamma^2 \in K[x]$. This proves the first assertion of part (a).

It remains to prove that K is the fixed field of the subgroup G of $\mathrm{Gal}(L/F)$ defined in Exercise 8:

$$G = \{\sigma \in \mathrm{Gal}(L/F) \,|\, \forall i \in [\![1, 3]\!],\ \sigma(R_i) = R_i\}.$$

To give an explicit description of G, note that

$$\begin{aligned} \sigma \in G &\iff \sigma(\alpha) = \pm\alpha,\ \sigma(\beta) = \pm\beta,\ \sigma(\gamma) = \pm\gamma \\ &\iff \sigma(\alpha^2) = \alpha^2,\ \sigma(\beta^2) = \beta^2, \sigma(\gamma^2) = \gamma^2 \\ &\iff \forall \lambda \in K,\ \sigma(\lambda) = \lambda, \end{aligned}$$

where the last equivalence is explained by the fact that every $\lambda \in K = F(\alpha^2, \beta^2, \gamma^2)$ is a polynomial in $\alpha^2, \beta^2, \gamma^2$.

This proves that every element of K is fixed by every $\sigma \in G$, thus $K \subset L_G$, where L_G is the fixed field of G.

Since the Galois correspondence is order reversing, $K \subset L_G$ implies $\mathrm{Gal}(L/K) \supset G$. To prove the inverse inclusion, take $\sigma \in \mathrm{Gal}(L/K)$. Then $\sigma(\lambda) = \lambda$ for all $\lambda \in K$, and the preceding equivalence shows that $\sigma \in G$. Thus $\mathrm{Gal}(L/K) = G$. Applying the Galois correspondence once more, the fixed fields of $\mathrm{Gal}(L/K)$ and G are equal, that is

$$K = L_G.$$

K is the fixed field of $G = \{\sigma \in \mathrm{Gal}(L/F) \,|\, \sigma(R_1) = R_1, \sigma(R_2) = R_2, \sigma(R_3) = R_3\}$.

(b) We have proved in Exercise 13 that f is imprimitive, with blocks

$$R_1 = \{\alpha, \beta, \gamma\}, \qquad R_2 = \{\alpha', \beta', \gamma'\}.$$

With the same notations as in Exercise 13 and 8, we have

$$G = \{\sigma \in \mathrm{Gal}(L/F) \,|\, \sigma(R_1) = R_1,\ \sigma(R_2) = R_2\}.$$

Since α, β, γ are the roots of $x^3 - \lambda$, and α', β', γ' the roots of $x^3 - \mu$, where $\{\lambda, \mu\} = \{\sigma(\lambda), \sigma(\mu)\}$, then, for all $\sigma \in \mathrm{Gal}(L/F)$,

$$\begin{aligned} \sigma \in G &\iff \sigma(\{\alpha, \beta, \gamma\} = \{\alpha, \beta, \gamma\},\ \sigma(\{\alpha', \beta', \gamma'\}) = \{\alpha', \beta', \gamma'\} \\ &\iff \sigma(\lambda) = \lambda,\ \sigma(\mu) = \mu \\ &\iff \forall \xi \in K,\ \sigma(\xi) \in K. \end{aligned}$$

This proves as in part (a) that $K = L_G$. □

Ex. 14.2.15 *Let $G \subset S_n$ be transitive. Prove that G is primitive if and only if the isotropy subgroups of G are maximal with respect to inclusion.*

Proof. Let i be a fixed integer in $\{1, \ldots, n\}$. Since G is transitive, $G \cdot i = \{1, \ldots, n\}$. The Fundamental Theorem of group actions gives $n = |G \cdot i| = (G : G_i)$, thus $|G_i| n = |G|$.

Given a subgroup $G_i \subset H \subset G$, let $\{\tau_1 = e, \ldots, \tau_m\}$ be a complete system of representatives of the left cosets $\tau H, \tau \in G$, where $m = (G : H)$, so that $\tau_1 H, \ldots, \tau_m H$ partition G.

Consider

$$R_1 = (\tau_1 H) \cdot i, \ldots, R_m = (\tau_m H) \cdot i.$$

As $G = \tau_1 H \cup \cdots \cup \tau_m H$, then

$$R_1 \cup \cdots \cup R_m = (\tau_1 H) \cdot i \cup \cdots \cup (\tau_m H) \cdot I = G \cdot i = \{1, \ldots, n\}.$$

Now we show that this union is disjoint.

If $u \in R_j \cap R_k = (\tau_j H) \cdot i \cap (\tau_k H) \cdot i$, then

$$u = (\tau_j h)(i) = (\tau_k h')(i), \quad h, h' \in H.$$

Then $h'^{-1} \tau_k^{-1} \tau_j h)(i) = i$, thus

$$h'' = h'^{-1} \tau_k^{-1} \tau_j h \in G_i \subset H,$$

hence $\tau_j h = \tau_k h' h''$, $h, h', h'' \in H$. This shows that $\tau_j H = \tau_k H$, thus $j = k$. This proves

$$j \neq k \Rightarrow R_j \cap R_k = (\tau_j H) \cdot i \cap (\tau_k H) \cdot i = \varnothing.$$

Now we prove that every $\sigma \in G$ preserves the block structure:

If $\sigma \in G$ and $R_j = (\tau_j H) \cdot i$, then $\sigma \tau_j H$ is a left coset, thus $\sigma \tau_j H = \tau_k H$ for some index k, and

$$\sigma(R_j) = (\sigma(\tau_j H \cdot i)) = (\sigma \tau_j H) \cdot i = (\tau_k H) \cdot i = R_k.$$

Since G is transitive, all R_j have same cardinality l, and $n = lm$.

To conclude, $R_1, \ldots, R_m$ have same cardinality, partition $\{1, \ldots, n\}$, and every $\sigma \in G$ preserves the block structure. If $l > 1$ and $m > 1$, then G is imprimitive.

Hence, if we assume that G is primitive, either $l = 1$ or $m = 1$.

• If $l = 1$, then for all indices k, $(\tau_k H) \cdot i = \{\tau_k(i)\}$. With $k = 1$ and $\tau_k = e$, we obtain $H \cdot i = \{i\}$, which shows that $H \subset G_i$, thus $H = G_i$.

• If $m = 1$, then $(G : H) = m = 1$, thus $H = G$.

This proves that there is no subgroup H such that $G_i \subsetneq H \subsetneq G$: G_i is maximal with respect to inclusion.

Conversely, suppose that G is imprimitive, with respect to the blocks $R_1, \ldots, R_m$, where $m > 1$. Since G is transitive, all R_j have the same cardinality $|R_j| = l > 1$.

If $i \in \{1, \ldots, n\}$ is some fixed integer, there is some index $j, 1 \leq j \leq m$ such that $i \in R_j$. Now, consider the subgroup

$$H = \{\sigma \in G \,|\, \sigma(R_j) = R_j\}.$$

Then $G_i \subset H$: if $\sigma \in G_i$, then $\sigma(i) = i \in R_j$, thus $\sigma(R_j) = R_j$. Moreover

• $H \neq G$: Since $m > 1$, there is some $R_k \neq R_j$, and some $w \in R_k$. Since G is transitive, there is some $\sigma \in G$ such that $\sigma(i) = w$, so that $\sigma(R_j) = R_k$. Then $\sigma \notin H$, and $H \neq G$.

• $G_i \neq H$: Since $|R_j| > 1$, there is some $i' \neq i$ in the same block R_j. Since G is transitive, there is some $\sigma' \in G$ such that $\sigma'(i) = i'$, so that $\sigma(R_j) = R_j$. Then $\sigma \in H$, but $\sigma \notin G_i$, so $G_i \neq H$.

To conclude, the subgroup H satisfies

$$G_i \subsetneq H \subsetneq G.$$

This proves that G_i is not maximal with respect to inclusion.

We have proved that G is primitive if and only if the isotropy subgroups of G are maximal with respect to inclusion.

□

Ex. 14.2.16 *Let p be prime. The ring $\mathbb{Z}/p^2\mathbb{Z}$ is not a field, but one can still define the group $\mathrm{AGL}(1, \mathbb{Z}/p^2\mathbb{Z})$. Its action on $\mathbb{Z}/p^2\mathbb{Z}$ allows us to write $\mathrm{AGL}(1, \mathbb{Z}/p^2\mathbb{Z}) \subset S_{p^2}$.*

(a) Prove that $\mathrm{AGL}(1, \mathbb{Z}/p^2\mathbb{Z})$ is solvable and transitive of order $p^3(p-1)$.

(b) Prove that $\mathrm{AGL}(1, \mathbb{Z}/p^2\mathbb{Z}) \subset S_{p^2}$ is imprimitive.

Proof.

(a) Recall that the group of invertible elements of $\mathbb{Z}/p^2\mathbb{Z}$ is $(\mathbb{Z}/p^2\mathbb{Z})^*$, where

$$|(\mathbb{Z}/p^2\mathbb{Z})^*| = \phi(p^2) = p^2 - p.$$

As in section 6.4, if $a, b \in \mathbb{Z}/p^2\mathbb{Z}$, we define $\gamma_{a,b} : \mathbb{Z}/p^2\mathbb{Z} \to \mathbb{Z}/p^2\mathbb{Z}$ by $\gamma_{a,b}(x) = ax + b$. Note that $\gamma_{a,b}$ is bijective if and only if $a \in (\mathbb{Z}/p^2\mathbb{Z})^*$. We define

$$G = \mathrm{AGL}(1, \mathbb{Z}/p^2\mathbb{Z}) = \{\gamma_{a,b} \,|\, a \in (\mathbb{Z}/p^2\mathbb{Z})^*, b \in \mathbb{Z}/p^2\mathbb{Z}\}.$$

We note that $\gamma_{a,b} = \gamma_{c,d}$ implies $\gamma_{a,b}(0) = \gamma_{c,d}(0)$, thus $b = d$, and then $\gamma_{a,b}(1) = \gamma_{c,d}(1)$ gives $a = c$:

$$\gamma_{a,b} = \gamma_{c,d} \Rightarrow (a, b) = (c, d).$$

Therefore the map

$$\left\{ \begin{array}{ccc} (\mathbb{Z}/p^2\mathbb{Z})^* \times \mathbb{Z}/p^2\mathbb{Z} & \to & G \\ (a, b) & \mapsto & \gamma_{a,b} \end{array} \right.$$

is bijective, which proves $|G| = \phi(p^2)p^2 = (p^2-p)p^2 = p^3(p-1)$.

As in section 6.4 (and Exercise 6.4.1), we obtain, if $a, c \in (\mathbb{Z}/p^2\mathbb{Z})^*$,

$$\gamma_{a,b} \circ \gamma_{c,d} = \gamma_{ac,ad+c} \in G,$$

since $ac \in (\mathbb{Z}/p^2\mathbb{Z})^*$. Moreover, $\gamma_{a,b}^{-1} = \gamma_{a^{-1},-a^{-1}b} \in G$, so that G is a subgroup of $S(\mathbb{Z}/p^2\mathbb{Z}) \simeq S_{p^2}$.

The map

$$\varphi \left\{ \begin{array}{ccc} G & \to & (\mathbb{Z}/p^2\mathbb{Z})^* \\ \gamma_{a,b} & \mapsto & a \end{array} \right.$$

is well-defined, and is a surjective homomorphism by definition of G. Moreover, the kernel of φ is the subgroup

$$T = \{\gamma_{1,b} \,|\, b \in \mathbb{Z}/p^2\mathbb{Z}\}.$$

Therefore $\mathrm{AGL}(1, \mathbb{Z}/p^2\mathbb{Z})/T \simeq (\mathbb{Z}/p^2\mathbb{Z})^*$. Since T and $(\mathbb{Z}/p^2\mathbb{Z})^*$ are Abelian, this proves that $G = \mathrm{AGL}(1, \mathbb{Z}/p^2\mathbb{Z})$ is solvable.

To prove that G acts transitively on $\mathbb{Z}/p^2\mathbb{Z}$, for all $\alpha, \beta \in \mathbb{Z}/p^2\mathbb{Z}$, we must find $\gamma_{a,b} \in G$ such that $\gamma_{a,b}(\alpha) = \beta$.

Write $\alpha = [u]_{p^2}, \beta = [v]_{p^2}, a = [A]_{p^2}, b = [B]_{p^2}$, where $u, v, A, B \in \mathbb{Z}$, and $\gcd(p, A) = 1$. Then

$$\gamma_{a,b}(\alpha) = \beta \iff a\alpha + b = \beta \iff Au + B \equiv v \pmod{p^2}.$$

If $\alpha \in (\mathbb{Z}/p^2\mathbb{Z})^*$, $b = 0$ and $a = \alpha^{-1}\beta$ give a solution $\gamma_{a,b} = \gamma_{\alpha^{-1}\beta,0}$.

Otherwise, $p \mid u$. If $p^2 \nmid u$, then $u = kp, k \in \mathbb{Z}, p \nmid k$. We can take $B = v - p$, so that

$$\begin{aligned} Au + B \equiv v \pmod{p^2} &\iff Akp + v - p \equiv v \pmod{p^2} \\ &\iff Ak \equiv 1 \pmod{p}, \end{aligned}$$

which has a solution $A \in \mathbb{Z}$ since $p \nmid A$.

Finally, if $p^2 \mid u$, then $\alpha = 0$, and $a = 1, b = \beta$ gives a solution $\gamma_{1,\beta}$.

Thus G, viewed as a subgroup of S_{p^2}, is transitive.

(b) Consider the subgroup H of G defined by

$$H = p\mathbb{Z}/p^2Z = \{\overline{0}, \overline{p}, \overline{2p}, \ldots, \overline{(p-1)p}\},$$

where we write, for every integer a, $\overline{a} = [a]_{p^2}$ the class of a modulo p^2.

Then the cosets $R_i = \overline{i} + H, 0 \leq i \leq p-1$, partition G:

$$\begin{aligned} &R_0 = H = \{\overline{0}, \overline{p}, \overline{2p}, \ldots, \overline{(p-1)p}\}, \\ &R_1 = \overline{1} + H = \{\overline{1}, \overline{1+p}, \overline{1+2p}, \ldots, \overline{1+(p-1)p}\}, \\ &\ldots \\ &R_{p-1} = \overline{p-1} + H = \{\overline{p-1}, \overline{p-1+p}, \overline{p-1+2p}, \ldots, \overline{p^2-1}\}. \end{aligned}$$

Note that $R_i = \gamma_{1,i}(R_0)$ for all i (here $\gamma_{1,i}$ refers to $\gamma_{\overline{1},\overline{i}}$, and $i + H$ to $\overline{i} + H = R_i$).

We prove

$$\gamma_{a,b}(R_0) = R_b.$$

Indeed, if $\alpha = \overline{kp} \in R_0$, then $\gamma_{a,b}(\overline{kp}) = a\overline{kp} + b \in b + H = R_b$, thus $\gamma_{a,b}(R_0) \subset R_b$. Moreover the cosets R_0, R_b have same cardinality, so that $\gamma_{a,b}(R_0) = R_b$.

Using this result, for all index i, since $R_i = i + R_0 = \gamma_{1,i}(R_0)$,

$$\begin{aligned}\gamma_{a,b}(R_i) &= (\gamma_{a,b}\,\gamma_{1,i})(R_0)\\ &= \gamma_{a,a+ib}(R_0)\\ &= R_{ai+b}.\end{aligned}$$

Therefore G permutes the blocks $R_0, \ldots, R_{p-1}$.

This proves that $G = \mathrm{AGL}(1, \mathbb{Z}/p^2\mathbb{Z})$ is imprimitive. □

14.3 PRIMITIVE PERMUTATION GROUPS

Ex. 14.3.1 *The goal of this exercise is to prove that primitive permutation groups are transitive. Assume that $G \subset S_n$ is primitive but not transitive, and derive a contradiction as follows.*

(a) Explain why $n > 1$.

(b) Let the orbits of G acting on $\{1, \ldots, n\}$ be $R_1, \ldots, R_k$ (see Section A.4 if you have forgotten about orbits). Explain why $k > 1$ and why elements of G map every orbit to itself.

(c) Conclude that G is imprimitive. Be sure to take into account the case when every orbit consists of a single element.

Proof.

(a) If $n = 1$, then $S_n = \{e\}$ and $G = \{e\}$. Then G is primitive (we can't partition $\{1, \ldots, n\} = \{1\}$ with classes R_i such that $|R_i| > 1$ for some i), but G is transitive, since $e(1) = 1$. So the assumption $G \subset S_n$ is primitive but not transitive implies $n > 1$.

(b) If $k = 1$, there is only one orbit $R_1 = G \cdot 1$. Then G is transitive: if $i, j \in \{1, n\}$, $i = \sigma(1), j = \tau(1)$, $\sigma, \tau \in G$, thus $(\tau\sigma^{-1})(i) = j$, where $\tau\sigma^{-1} \in G$. This shows that G is transitive. Since G is not transitive, then $k > 1$.

Now we prove that, if $\sigma \in G$ and R_i is an orbit, then $\sigma(R_i)$ is an orbit R_j.

We know that the orbits partition $\{1, \ldots, n\}$. Let u a fixed element in R_i, and $v = \sigma(u)$. Then $v \in R_j$ for some index j. We prove $\sigma(R_i) = R_j$.

If $s \in R_i$, since u, r are in the same orbit, there is some $\tau \in G$ such that $\tau(i) = s$. Then $\sigma(s) = (\sigma\tau\sigma^{-1})(v)$, where $\sigma\tau\sigma^{-1} \in G$, so that $\sigma(s) \in R_j$ and $v \in R_j$. This proves $\sigma(R_i) \subset R_j$.

Conversely, since $\sigma^{-1}(v) = u \in R_i$, the same reasoning shows that $\sigma^{-1}(R_j) \subset R_i$: if $t \in R_j$: there is some $\lambda \in G$ such that $\lambda(v) = t$, thus $\sigma^{-1}(t) = (\sigma^{-1}\lambda\sigma)(u)$, where $\sigma^{-1}\lambda\sigma \in G$ and $u \in R_i$, so that $t \in R_i$. The two inclusions $\sigma(R_i) \subset R_j$ and $\sigma^{-1}(R_j) \subset R_i$ show that $\sigma(R_i) = R_j$.

(c) If $|R_i| > 1$ for some i, then G is imprimitive by Definition 14.2.5. By assumption, G is primitive, thus $|R_i| = 1$ for all i, so that every orbit consists of a single element. This means that for all $\sigma \in G$, and for all $i \in \{1, \ldots, n\}$, $\sigma(i) = i$. Therefore $\sigma = e$ for all $\sigma \in G$, $G = \{e\}$. Since $n > 1$ by part (a), G is imprimitive, because there are partitions with at least two classes, and several elements in a class, for instance $R_1 = \{1, 2\}, R_2 = \{1, \ldots, n\} \setminus R_1$, is preserved by $G = \{e\}$. This proves that $G = \{e\}$ is imprimitive when $n > 1$, in contradiction with the assumption.

This contradiction proves $|R_i| > i$ for some index i, thus G is imprimitive.

To conclude, all primitive permutation groups are transitive. □

Ex. 14.3.2 *Let $\gamma_{I_n,v} \in \mathrm{AGL}(n,\mathbb{F}_q)$ be translation by $v \in \mathbb{F}_q^n$, and let $\gamma_{A,w} \in \mathrm{AGL}(n,\mathbb{F}_q)$ be arbitrary.*

(a) Prove that $\gamma_{A,w}^{-1} = \gamma_{A^{-1},-A^{-1}w}$.

(b) Prove that $\gamma_{A,w} \circ \gamma_{I_n,v} \circ \gamma_{A,w}^{-1} = \gamma_{I_n,Av}$.

(c) Part (b) shows that the translation subgroup $\mathbb{F}_q^n \subset \mathrm{AGL}(n,\mathbb{F}_q)$ is normal. Prove that the quotient group $\mathrm{AGL}(n,\mathbb{F}_q)/\mathbb{F}_q^n$ is isomorphic to $\mathrm{GL}(n,\mathbb{F}_q)$.

(d) Prove that $\mathrm{AGL}(n,\mathbb{F}_q)$ is isomorphic to the semidirect product $\mathbb{F}_q^n \rtimes \mathrm{GL}(n,\mathbb{F}_q)$, where $\mathrm{GL}(n,\mathbb{F}_q)$ acts on $\mathbb{F}_q^n$ by matrix multiplication.

Proof. We give first the product of two elements in $\mathrm{AGL}(n,\mathbb{F}_q)$, to generalize the results of Section 6.4A. Using the definition $\gamma_{A,v}(u) = Au + v$, we obtain, for all $u \in \mathbb{F}_q^n$,

$$\begin{aligned}(\gamma_{A,v} \circ \gamma_{B,w})(u) &= \gamma_{A,v}(Bu + w) \\ &= A(Bu + w) + v \\ &= ABu + Aw + v \\ &= \gamma_{AB,Aw+v}(u),\end{aligned}$$

thus

$$\gamma_{A,v} \circ \gamma_{B,w} = \gamma_{AB,Aw+v} \tag{1}$$

(a) For all $u, v \in \mathbb{F}_q^n$,

$$\begin{aligned}v = \gamma_{A,w}(u) &\iff v = Au + w \\ &\iff u = A^{-1}(v - w) = A^{-1}v - A^{-1}w,\end{aligned}$$

thus

$$\gamma_{A,w}^{-1} = \gamma_{A^{-1},-A^{-1}w}. \tag{2}$$

(b) Using the formulas (1) and (2), we obtain

$$\begin{aligned}\gamma_{A,w} \circ \gamma_{I_n,v} \circ \gamma_{A,w}^{-1} &= \gamma_{A,w} \circ \gamma_{I_n,v} \circ \gamma_{A^{-1},-A^{-1}w} \\ &= \gamma_{A,w} \circ \gamma_{A^{-1},-A^{-1}w+v} \\ &= \gamma_{I_n,A(-A^{-1}w+v)+w} \\ &= \gamma_{I_n,Av}.\end{aligned}$$

We have proved

$$\gamma_{A,w} \circ \gamma_{I_n,v} \circ \gamma_{A,w}^{-1} = \gamma_{I_n,Av}. \tag{3}$$

(c) Consider the map

$$\varphi \left\{ \begin{array}{ccc} \mathrm{AGL}(n,\mathbb{F}_q) & \to & \mathrm{GL}(n,\mathbb{F}_q) \\ \gamma_{A,v} & \mapsto & A. \end{array} \right.$$

The map φ is well defined, since for all $A, B \in \mathrm{GL}(n,\mathbb{F}_q)$ and for all $v, w \in \mathbb{F}_q^n$,

$$\gamma_{A,v} = \gamma_{B,w} \iff (A, v) = (B, w). \tag{4}$$

Then

$$\varphi(\gamma_{A,v} \circ \gamma_{B,w}) = \varphi(\gamma_{AB,Aw+v}) = AB = \varphi(\gamma_{A,v}\varphi(\gamma_{B,w})),$$

thus φ is a group homomorphism.

Since every $A \in \mathrm{GL}(n, \mathbb{F}_q)$ is the image of $\gamma_{A,0}$, φ is surjective, and

$$\ker \varphi = \{\gamma_{I,w} \,|\, w \in \mathbb{F}_q^*\} \simeq \mathbb{F}_q^n.$$

Therefore, the first Isomorphism Theorem gives

$$\mathrm{AGL}(n, \mathbb{F}_q)/\mathbb{F}_q^n \simeq \mathrm{GL}(n, \mathbb{F}_q),$$

with the identification of vectors w with the translations $\gamma_{I,w}$.

(d) Consider

$$\psi \left\{ \begin{array}{ccc} \mathrm{AGL}(n, \mathbb{F}_q) & \to & \mathbb{F}_q^n \rtimes \mathrm{GL}(n, \mathbb{F}_q) \\ \gamma_{A,v} & \mapsto & (v, A). \end{array} \right.$$

By formula (4), the map ψ is well defined. It is a bijection, with inverse $(v, A) \mapsto \gamma_{A,v}$.

Following the formula (6.9), $(h, g)\,(h', g') = (h(g \cdot h'), gg')$, which defines the product in $H \rtimes G$, the product in $\mathbb{F}_q^n \rtimes \mathrm{GL}(n, \mathbb{F}_q)$ is given by

$$(v, A)\,(w, B) = (v + Aw, AB), \qquad v, w \in \mathbb{F}_q^n, \quad A, B \in \mathrm{GL}(n, \mathbb{F}_q). \tag{5}$$

Therefore, using (5) and (1),

$$\begin{aligned} \psi(\gamma_{A,v})\psi(\gamma_{B,w}) &= (v, A)(w, B) \\ &= (v + Aw, AB) \\ &= \psi(\gamma_{AB,Aw+v}) \\ &= \psi(\gamma_{A,v}) \circ \psi(\gamma_{B,w}), \end{aligned}$$

thus ψ is a group isomorphism, and

$$\mathrm{AGL}(n, \mathbb{F}_q) \simeq \mathbb{F}_q^n \rtimes \mathrm{GL}(n, \mathbb{F}_q).$$

□

Ex. 14.3.3 *Consider the affine semilinear group* $\mathrm{A\Gamma L}(n, \mathbb{F}_q)$ *for* $q = p^m$.

(a) Prove that $\mathrm{AGL}(n, \mathbb{F}_q)$ *is a normal subgroup of* $\mathrm{A\Gamma L}(n, \mathbb{F}_q)$ *of index* m.

(b) Prove that $\mathbb{F}_q^n$ *is a normal subgroup of* $\mathrm{A\Gamma L}(n, \mathbb{F}_q)$.

(c) Prove that elements of $\mathrm{A\Gamma L}(n, \mathbb{F}_q)$ *give maps* $\mathbb{F}_q^n \to \mathbb{F}_q^n$ *that are affine linear over* $\mathbb{F}_p$.

We give some preliminary formulas.

Note that $\gamma_{A,v} = \gamma_{A,e,v}$, $A \in \mathrm{GL}(n, \mathbb{F}_q), v \in \mathbb{F}_q$, where e is the identity element of $\mathrm{Gal}(F_{q^m}/\mathbb{F}_p)$, thus $\mathrm{AGL}(n, \mathbb{F}_q) \subset \mathrm{A\Gamma L}(n, \mathbb{F}_q)$.

For all $u = (\alpha_1, \ldots, \alpha_n) \in \mathbb{F}_q^n$, we write $\sigma(u) = (\sigma(\alpha_1), \ldots, \sigma(\alpha_n))$.

If $A = (a_{ij})_{1\leq i,j\leq n} \in \mathrm{GL}(n, \mathbb{F}_q)$, then

$$\begin{aligned}\sigma(A \cdot u) &= \sigma\left(\sum_{j=1}^{n} a_{1j}\alpha_j, \ldots, \sum_{j=i}^{n} a_{ij}\alpha_j, \ldots, \sum_{j=1}^{n} a_{nj}\alpha_k\right) \\ &= \left(\sum_{j=1}^{n} \sigma(a_{1j})\sigma(\alpha_j), \ldots, \sum_{j=i}^{n} \sigma(a_{ij})\sigma(\alpha_j), \ldots, \sum_{j=1}^{n} \sigma(a_{nj})\sigma(\alpha_j)\right) \\ &= \sigma(A) \cdot \sigma(u),\end{aligned}$$

where $\sigma(A) = (\sigma(a_{ij}))_{1\leq i,j\leq n}$, and similarly

$$\sigma(A \cdot u + v) = \sigma(A) \cdot \sigma(u) + \sigma(v).$$

Then, for all $u \in \mathbb{F}_q^n$,

$$\begin{aligned}(\gamma_{A,\sigma,v} \circ \gamma_{B,\tau,w})(u) &= A\sigma(B\tau(u) + w) + v \\ &= A\sigma(B)(\sigma\tau)(u) + A\sigma(w) + v \\ &= \gamma_{A\sigma(B),\sigma\tau,A\sigma(w)+v}(u),\end{aligned}$$

thus

$$\gamma_{A,\sigma,v} \circ \gamma_{B,\tau,w} = \gamma_{A\sigma(B),\sigma\tau,A\sigma(w)+v}. \tag{6}$$

For all $u, s \in \mathbb{F}_q^n$,

$$\begin{aligned}s = \gamma_{A,\sigma,v}(u) &\iff s = A\sigma(u) + v \\ &\iff \sigma(u) = A^{-1}(s - v) \\ &\iff u = \sigma^{-1}(A^{-1}s - A^{-1}v) \\ &\iff u = \sigma^{-1}(A^{-1})\sigma^{-1}(s) - \sigma^{-1}(A^{-1})\sigma^{-1}(v) \\ &\iff u = \gamma_{\sigma^{-1}(A^{-1}),\sigma^{-1},-\sigma^{-1}(A^{-1})\sigma^{-1}(v)},\end{aligned}$$

thus

$$\gamma_{A,\sigma,v}^{-1} = \gamma_{\sigma^{-1}(A^{-1}),\sigma^{-1},-\sigma^{-1}(A^{-1})\sigma^{-1}(v)}. \tag{7}$$

By (6) and (7), $\mathrm{A\Gamma L}(n, \mathbb{F}_q)$ is a subgroup of $S(\mathbb{F}_q^n)$. Moreover, if $\gamma_{A,\sigma,v}, \gamma_{B,\tau,w} \in \mathrm{A\Gamma L}(n, \mathbb{F}_q)$, then

$$\gamma_{A,\sigma,v} = \gamma_{B,\tau,w} \Rightarrow (A, \sigma, v) = (B, \tau, w). \tag{8}$$

Indeed, if $\gamma_{A,\sigma,v} = \gamma_{B,\tau,w}$, then for all $u \in \mathbb{F}_q^n$, $A\sigma(u) + v = B\tau(u) + w$. With $u = 0$, we obtain $v = w$. If we take $u = e_i = (0, \ldots, 0, 1, 0, \ldots, 0)$, where $(e_1, \ldots, e_n)$ is the standard base of $\mathbb{F}_q^n$, then $\sigma(e_i) = e_i = \tau(e_i)$, so that $Ae_i = Be_i$, $i = 1, \ldots, n$. This implies $A = B$, and $\sigma(u) = \tau(u)$ for all $u \in \mathbb{F}_q^n$. Therefore, with $u = (\alpha, 0, \ldots, 0)$, $\alpha \in \mathbb{F}_q$, we obtain $\sigma(\alpha) = \tau(\alpha)$, thus $\sigma = \tau$.

Proof.

(a) By (8),

$$\varphi \left\{ \begin{array}{ccc} \mathrm{A\Gamma L}(n,\mathbb{F}_q) & \to & \mathrm{Gal}(\mathbb{F}_{p^m},\mathbb{F}_p) \\ \gamma_{A,\sigma,v} & \mapsto & \sigma \end{array} \right.$$

is well defined. Moreover, by (6), if $\gamma_{A,\sigma,v}, \gamma_{B,\tau,w} \in \mathrm{AGL}(n,\mathbb{F}_q)$,

$$\varphi(\gamma_{A,\sigma,v} \circ \gamma_{B,\tau,w}) = \varphi(\gamma_{A\sigma(B),\sigma\tau,A\sigma(w)+v}) = \sigma\tau = \varphi(\gamma_{A,\sigma,v})\varphi(\gamma_{B,\tau,w}),$$

thus φ is a group homomorphism. If σ is any element of $\mathrm{Gal}(\mathbb{F}_{p^n},\mathbb{F}_p)$, then $\sigma = \varphi(\gamma_{I_n,\sigma,0}$, thus φ is surjective. The kernel of φ is

$$\ker\varphi = \{\gamma_{A,e,v} \,|\, A \in \mathrm{GL}(n,\mathbb{F}_q), v \in \mathbb{F}_q^n\} = \{\gamma_{A,v} \,|\, A \in \mathrm{GL}(n,\mathbb{F}_q), v \in \mathbb{F}_q^n\} \subset \mathrm{AGL}(n,\mathbb{F}_q).$$

This shows that $\mathrm{AGL}(n,\mathbb{F}_q)$ is a normal subgroup of $\mathrm{A\Gamma L}(n,\mathbb{F}_q)$, and the first Isomorphism Theorem gives

$$\mathrm{A\Gamma L}(n,\mathbb{F}_q)/\mathrm{AGL}(n,\mathbb{F}_q) \simeq \mathrm{Gal}(\mathbb{F}_{p^m},\mathbb{F}_p).$$

Since $\mathrm{Gal}(\mathbb{F}_{p^m},\mathbb{F}_p)$ is a cyclic group of order m, $\mathrm{AGL}(n,\mathbb{F}_q)$ is a normal subgroup of $\mathrm{A\Gamma L}(n,\mathbb{F}_q)$ of index m.

(b) Here, $\mathbb{F}_q^n$ is identified with the group of translations $\{\gamma_{I_n,e,w} \,|\, w \in \mathbb{F}_q^n\}$, and, using (6) and (7),

$$\begin{aligned} \gamma_{A,\sigma,v} \circ \gamma_{I_n,e,w} \circ \gamma_{A,\sigma,v}^{-1} &= \gamma_{A,\sigma,v} \circ \gamma_{I_n,e,w} \circ \gamma_{\sigma^{-1}(A^{-1}),\sigma^{-1},-\sigma^{-1}(A^{-1})\sigma^{-1}(v)} \\ &= \gamma_{A,\sigma,v} \circ \gamma_{\sigma^{-1}(A^{-1}),\sigma^{-1},-\sigma^{-1}(A^{-1})\sigma^{-1}(v)+w} \\ &= \gamma_{A\sigma\sigma^{-1}(A^{-1}),\sigma\sigma^{-1},A\sigma(-\sigma^{-1}(A^{-1})\sigma^{-1}(v)+w)+v} \\ &= \gamma_{I_n,e,A\sigma(w)}. \end{aligned}$$

We have proved

$$\gamma_{A,\sigma,v} \circ \gamma_{I_n,e,w} \circ \gamma_{A,\sigma,v}^{-1} = \gamma_{I_n,e,A\sigma(w)} \in \mathbb{F}_q^n, \tag{9}$$

therefore $\mathbb{F}_q^n$ is a normal subgroup of $\mathrm{A\Gamma L}(n,\mathbb{F}_q)$.

(c) $\mathbb{F}_q^n$, which is a vector space over $\mathbb{F}_q$, is also a vector space over $\mathbb{F}_p$, by restriction of the extern operation $\left\{ \begin{array}{ccc} \mathbb{F}_q \times \mathbb{F}_q^n & \to & \mathbb{F}_q^n \\ u & \mapsto & \lambda u \end{array} \right.$ to $\mathbb{F}_p \times \mathbb{F}_q^n$.

Let $\mathcal{B} = (e_1,\ldots,e_m)$ be a base of $\mathbb{F}_q$ over $\mathbb{F}_p$. As $\mathbb{F}_p$-vector spaces, $\mathbb{F}_q^n$ and $\mathbb{F}_p^{nm}$ are isomorphic, where an isomorphism φ is given by

$$\varphi \left\{ \begin{array}{ccc} \mathbb{F}_q^n & \to & \mathbb{F}_p^{nm} \\ (\alpha_1,\ldots,\alpha_n) & \mapsto & (x_1^1,\ldots,x_m^1;\ldots;x_1^n,\ldots,x_m^n), \end{array} \right.$$

where $\alpha_i = \sum_{j=1}^m x_j^i e_j,\ i = 1,\ldots,n.$ (this isomorphism depends of the choice of the base $\mathcal{B}$). This proves $\dim_{\mathbb{F}_p} \mathbb{F}_q^n = nm$. Consider the two maps

$$\psi \left\{ \begin{array}{ccc} \mathbb{F}_q^n & \to & \mathbb{F}_q^n \\ u = (\alpha_1,\ldots,\alpha_n) & \mapsto & \sigma(u) = (\sigma(\alpha_1),\ldots,\sigma(\alpha_n)), \end{array} \right. \qquad \chi \left\{ \begin{array}{ccc} \mathbb{F}_q^n & \to & \mathbb{F}_q^n \\ v & \mapsto & A \cdot v. \end{array} \right.$$

The automorphism $\sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ is $\mathbb{F}_q$-linear: if $\lambda \in \mathbb{F}_p, \alpha \in \mathbb{F}_q$, $\sigma(\lambda\alpha) = \sigma(\lambda)\sigma(\alpha) = \lambda\sigma(\alpha)$. Thus ψ is $\mathbb{F}_p$-linear. Moreover, χ is $\mathbb{F}_q$-linear, a fortiori $\mathbb{F}_p$-linear. Therefore, $\chi \circ \psi = u \mapsto A \cdot \sigma(u)$ is $\mathbb{F}_p$-linear, so that

$$\gamma_{A,\sigma,v} \left\{ \begin{array}{ccc} \mathbb{F}_q^n & \to & \mathbb{F}_q^n \\ u & \mapsto & A \cdot \sigma(u) + v \end{array} \right.$$

is affine linear over $\mathbb{F}_p$. □