14 Chapter 14 : SOLVABLE PERMUTATION GROUPS

14.1 POLYNOMIAL OF PRIME DEGREE

Ex. 14.1.1 *This exercise is concerned with the proof of part (a) of Lemma 14.1.2. Let* $\theta = (1\,2\dots p) \in S_p$.

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

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

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

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

hence

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

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

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

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

$\square$

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

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

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

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

$\square$

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

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

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

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

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

Proof.

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

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

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

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

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

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

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

which is equivalent to

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

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

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

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

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

that is

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

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

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

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

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

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

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

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

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

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

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

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

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

□

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 Sylow 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

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

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 $H_1, \ldots, H_4$ 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

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

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

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

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

Then

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

We prove

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

Indeed,

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

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

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

Proof. (of Ex.14.2.4.) Let

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

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 $\sigma = (\tau; \mu_1, \dots, \mu_p)$ and $(\rho; \nu_1, \dots, \nu_p)$ 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 $\gamma = (\tau^{-1}\rho\tau; \lambda_1, \dots, \lambda_p)$ 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

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

Let $\lambda = (\tau; \mu_1, \dots, \mu_p), \lambda' = (\tau'; \mu_1, \dots, \mu_p)$ 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 $\{1, \dots, p\}$. Since G is transitive, there exists some $\lambda = (\tau; \mu_1, ..., \mu_k) \in G$ which sends (i, j) on (i, k):

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

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 $\sigma = (\tau; \mu_1, \dots, \mu_p) \in G$ 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 $\lambda = (\rho; \nu_1, \dots, \nu_p) \in G_i$ 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

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

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

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

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

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

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

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

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

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*

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

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

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

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

φ is a group homormphism.

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

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

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

Consider

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

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

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

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*

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

(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 $\{1, \dots, n\}$. 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

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

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

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

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 $i \in \{1, \dots, n\}$,

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

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

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

Wreath products can be represented by semidirect products.

$\square$

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 $R_1, \dots, R_m$, 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

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

If $G_i = \{\sigma \in \mathrm{Gal}(L/F) \mid \sigma(R_i) = R_i\}$ 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 $R_1, \dots, R_m$, for each $\sigma \in \mathrm{Gal}(L/F)$, there exists $\tau \in S_m$ such that $\sigma(R_i) = R_{\tau(i)},\ i = 1, \dots, m$. Consider the map φ sending σ to τ:

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

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 $\{1, \dots, n\}$ by the action defined by $\sigma \cdot k = \sigma(k),\ \sigma \in G, k \in \{1, \dots, n\}$.
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 $\{1, \dots, n\}$. 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 $i \in \{1, \dots, n\}$, $\sigma = e$. This proves $G_1 = \{e\}$.
Moreover, since G is transitive, the orbit of 1 is $G \cdot 1 = \{1, \dots, n\}$, 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

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

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

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

$$
\begin{tikzcd}
& L = K(\omega, \alpha, \beta) & \\
K(\omega, \alpha) \arrow[ur] & & K(\omega, \beta) \arrow[ul] \\
& K(\omega) \arrow[ul] \arrow[ur] & \\
& K = F(\lambda, \mu) \arrow[u] & \\
& F \arrow[u] &
\end{tikzcd}
$$

• 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,

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

$\square$

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:

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

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 $G = \{\sigma \in \mathrm{Gal}(L/F) \mid \sigma(R_1) = R_1, \sigma(R_2) = R_2, \sigma(R_3) = R_3\}$.

(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

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

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 $K = L_G$. $\square$

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.

$\square$

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

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

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

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

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

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 $k > 1$.

We know that the orbits partition $\{1, \ldots, n\}$.

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

Fix $x \in R_i$, so that $R_i = \mathcal{O}_x = G \cdot x$ is the orbit of x.

Let $u \in R_i$. Then $u = \tau(x)$ for some $\tau \in G$. Then $\sigma(u) = (\sigma\tau)(x) \in R_i$. This proves $\sigma(R_i) \subset R_i$.

Conversely, for every $u = \tau(x) \in R_i$, $u = \sigma((\sigma^{-1}\tau)(x))$,where $(\sigma^{-1}\tau)(x) \in R_i$, thus $u \in \sigma(R_i)$. Therefore $R_i \subset \sigma(R_i)$. For all $\sigma \in G$,

$$\sigma(R_i) = R_i.$$

(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
$$\ker \varphi = \{\gamma_{I,w} \mid w \in \mathbb{F}_q^*\} \simeq \mathbb{F}_q^n.$$
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
$$\psi \begin{cases} \mathrm{AGL}(n, \mathbb{F}_q) & \to & \mathbb{F}_q^n \rtimes \mathrm{GL}(n, \mathbb{F}_q) \\ \gamma_{A,v} & \mapsto & (v, A). \end{cases}$$
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

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

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 $u = e_i = (0, \dots, 0, 1, 0, \dots, 0)$, where $(e_1, \dots, e_n)$ is the standard base of $\mathbb{F}_q^n$, then $\sigma(e_i) = e_i = \tau(e_i)$, so that $Ae_i = Be_i,\ i = 1, \dots, n$. This implies $A = B$, and $\sigma(u) = \tau(u)$ for all $u \in \mathbb{F}_q^n$. Therefore, with $u = (\alpha, 0, \dots, 0),\ \alpha \in \mathbb{F}_q$, 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

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

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 $\{\gamma_{I_n,e,w} \mid w \in \mathbb{F}_q^n\}$, 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 $\left\{ \begin{array}{ccc} \mathbb{F}_q \times \mathbb{F}_q^n & \to & \mathbb{F}_q^n \\ (\lambda, u) & \mapsto & \lambda u \end{array} \right.$ 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 $\mathbb{F}_p$. $\square$

Ex. 14.3.4 *Let F be any field. The definition of $\mathrm{AGL}(n, \mathbb{F}_q)$ given in the text extend to $\mathrm{AGL}(n, F)$. The goal of this exercise is to prove that $\mathrm{AGL}(n, F)$ is doubly transitive when we regard elements of $\mathrm{AGL}(n, F)$ as permutations of the vector space F^n.*

(a) Use $F^n \subset \mathrm{AGL}(n, F)$ to show that $\mathrm{AGL}(n, F)$ acts transitively on F_n.

(b) Inside $\mathrm{AGL}(n, F)$, we have the isotropy subgroup of $0 \in F_n$. Prove that this isotropy subgroup is $\mathrm{GL}(n, F)$.

(c) Prove that $\mathrm{GL}(n, F)$ acts transitively on $F^n \setminus \{0\}$.

(d) Use Exercise 19 below to conclude that $\mathrm{AGL}(n, F)$ is doubly transitive.

Proof.

(a) Let u, u' be any vectors in F^n. The equality $I_n \cdot u + (u' - u) = u'$ shows that $\gamma_{I_n, u'-u}(u) = u'$, where $\gamma_{I_n, u'-u} \in \mathrm{AGL}(n, F)$.

Therefore $\mathrm{AGL}(n, F)$ acts transitively on F^n.

(b) Write G_0 the isotropy group of 0. Then

$$\gamma_{A,v} \in G_0 \iff A \cdot 0 + v = 0 \iff v = 0.$$

Therefore $G_0 = \{\gamma_{A,0} \mid A \in \mathrm{GL}(n, F)\} \simeq \mathrm{GL}(n, F)$.

In section 14.3.B, we identified $\{\gamma_{A,0} \mid A \in \mathrm{GL}(n, F)\}$ with $\mathrm{GL}(n, F)$, so that

$$G_0 = \mathrm{GL}(n, F).$$

(c) Let $u, v \in F^n \setminus \{0\}$. Since $u \neq 0$, we can compete u in a base $\mathcal{B}_1 = (u_1, \ldots, u_n)$ of F_n, where $u_1 = u$. Similarly, we can complete $v \neq 0$ in a base $\mathcal{B}_2 = (v_1, \ldots, v_n)$, where $v_1 = v$.

Since $\mathcal{B}_1, \mathcal{B}_2$ are two bases, there exists some bijective linear map $f : F^n \to F^n$ such that $f(u_i) = v_i,\ i = 1, \ldots, n$, so that $f(u) = v$.

Let $\mathcal{B} = (e_1, \ldots, e_n)$ be the standard base of F^n. Then the matrix $A = \mathcal{M}_{\mathcal{B}}(f)$ of f satisfies $A \in \mathrm{GL}(n, F)$, and $A \cdot u = v$. This proves that $\mathrm{GL}(n, F)$ acts transitively on $F^n \setminus \{0\}$.

(d) Since the isotropy group G_0 acts transitively on $F^n \setminus \{0\}$, Exercise 14.3.19 (a) shows that $\mathrm{AGL}(n, F)$ acts transitively on F^n, using that $\mathrm{AGL}(n, F)$ can be viewed as a subgroup G of $S_{|F^n|}$. □

Ex. 14.3.5 *Let A and B be non-Abelian simple groups. You will show that $A \times \{e_B\}$ and $\{e_A\} \times B$ are the only nontrivial normal subgroups of $A \times B$. Let $N \subset A \times B$ be a normal subgroup different from $\{(e_A, e_B)\}, A \times \{e_B\}$, and $\{e_A\} \times B$.*

(a) Prove that $A \times \{e_B\}$ and $\{e_A\} \times B$ are normal in $A \times B$. Hence, if we can show that $N = A \times B$, then we will be done.

(b) Prove that we can find $(a, b) \in N$ such that $e_A \neq a \in A$ and $e_B \neq b \in B$.

(c) Let $(a, b) \in N$ be as in part (b). Show that $(a a_1 a^{-1} a_1^{-1}, e_B) \in N$ for any $a_1 \in A$.

(d) Given $e_A \neq a \in A$, prove that there is $a_1 \in A$ such that $a a_1 \neq a_1 a$. Then combine this with parts (b) and (c) to show that $N \cap (A \times \{e_B\}) = A \times \{e_B\}$.

(e) *Part (d) implies that $A \times \{e_B\} \subset N$, and the inclusion $\{e_A\} \times B \subset N$ is proved similarly. Use this to prove that $N = A \times B$.*

Exercise 18 will explore various aspects of this argument.

Proof.

(a) Take (a_0, e_B) in $A \times \{e_B\}$, and $(a, b) \in A \times B$. Then

$$\begin{aligned}(a,b)(a_0,e_B)(a,b)^{-1} &= (a,b)(a_0,e_B)(a^{-1},b^{-1})\\ &= (aa_0a^{-1}, be_Bb^{-1}\\ &= (aa_0a^{-1}, e_B) \in A \times \{e_B\},\end{aligned}$$

thus $A \times \{e_B\}$ is normal in $A \times B$, and similarly $\{e_A\} \times B$ is normal in $A \times B$.

(b) Reasoning by contradiction, suppose that we can't find $(a, b) \in N$ such that $a \neq e_A, b \neq e_B$, then $N \subset (A \times \{e_B\}) \cup (\{e_A\} \times B)$.

Note that $A \times \{e_B\} \simeq A$ is simple. If $N \subset A \times \{e_B\}$, then N is normal in $A \times \{e_B\} \subset A \times B$, thus $N = A \times \{e_A\}$ or $N = \{(e_A, e_B)\}$, but this contradicts the assumptions on N. Therefore $N \not\subset A \times \{e_B\}$, and similarly $N \not\subset \{e_A\} \times B$, so that

$$\begin{aligned}&N \subset (A \times \{e_B\}) \cup (\{e_A\} \times B),\\ &N \not\subset A \times \{e_B\}, \quad N \not\subset \{e_A\} \times B.\end{aligned}$$

Since $N \subset (A\times\{e_B\})\cup(\{e_A\}\times B)$ and $N \not\subset A\times\{e_B\}$, there exists some $n_1 = (a', b) \in N$ such that $n_1 = (a', b) \in \{e_A\} \times B$ and $n_1 = (a', b) \notin A \times \{e_B\}$. Thus $n_1 = (e_A, b) \in N, b \neq e_B$.

Similarly, since $N \subset (A \times \{e_B\}) \cup (\{e_A\} \times B)$ and $N \not\subset \{e_A\} \times B$, there exists some $n_2 = (a, b') \in N$ such that $n_2 = (a, b') \in A \times \{e_B\}$ and $n_2 = (a, b') \notin \{e_A\} \times B$. Thus $n_2 = (a, e_B) \in N, a \neq e_A$.

Then $n = n_1n_2 = (e_A, b)(a, e_B) = (a, b) \in N$, and $a \neq e_A, b \neq e_B$.

(c) N is normal, and $(a^{-1}, b^{-1}) = (a, b)^{-1} \in N$, thus

$$(a_1, e_B)(a, b)^{-1}(a_1, e_B)^{-1} = (a_1a^{-1}a_1^{-1}, b^{-1}) \in N.$$

Left multiplication by $(a, b) \in N$ gives

$$(a, b)[(a_1, e_B)(a, b)^{-1}(a_1, e_B)^{-1}] = (aa_1a^{-1}a_1^{-1}, e_B) \in N.$$

(d) Let $a \neq e_A$ be a fixed element in A.

Consider the center of A:

$$Z(A) = \{x \in A \,|\, \forall y \in A, xy = yx\}.$$

$Z(A)$ is a normal subgroup of A (it is the kernel of $f : A \to \mathrm{Aut(A)}$ defined by $f(y) = \phi_y$, where $\phi_y(x) = yxy^{-1}$ for all $x \in A$). Since A is non-Abelian, $Z(A) \neq A$, and since A is simple, $Z(A) = \{e_A\}$.

Therefore, $a \neq e_A$ implies $a \notin Z(A)$, thus there exists $a_1 \in A$ such that $aa_1 \neq a_1a$.

Since N and $A\times\{e_B\}$ are normal subgroups of $A\times B$, the intersection $N\cap(A\times\{e_B\})$ is normal in $A \times B$, a fortiori in the simple group $A \times \{e_B\}$. Therefore $N \cap (A \times \{e_B\}) = \{(e_A, e_B)\}$ or $N\cap(A\times\{e_B\}) = A\times\{e_B\}$. But $N\cap(A\times\{e_B\}) = \{(e_A, e_B)\}$ is impossible, because $(e_A, e_B) \neq (aa_1a^{-1}a_1^{-1}, e_B) \in N$. Hence $N \cap (A \times \{e_B\}) = A \times \{e_B\}$.

(e) Part (d) implies that $A \times \{e_B\} \subset N$, and the inclusion $\{e_A\} \times B \subset N$ is proved similarly. Let (a, b) be any element in $A \times B$. Then $n_1 = (a, e_B) \in A \times \{e_B\} \subset N$, and $n_2 = (e_A, b) \in \{e_A\} \times B \subset N$, thus $n_1 \in N, n_2 \in N$, so that $n = n_1 n_2 = (a, b) \in N$. This proves $A \times B \subset N$, where $N \subset A \times B$. Therefore $N = A \times B$.

To conclude, if A, B are non-Abelian simple groups, the only non trivial normal subgroups of $A \times B$ are $A \times \{e_B\}$ and $\{e_A\} \times B$. □

Ex. 14.3.6 *Let $A \subset N$ be a minimal normal subgroup, where N is normal in a larger group G. Given $g \in G$, we set $A_g = gAg^{-1}$.*

(a) Prove that A_g is isomorphic to A and is a minimal normal subgroup of N.

(b) Fix $g_1 \in G$ and consider AA_{g_1}. By Exercise 7, we know that AA_{g_1} is a subgroup of N. Assume that $A_g \subset AA_{g_1}$ for all $g \in G$. Prove that AA_{g_1} is normal in G.

(c) Use the following idea to complete the proof of Proposition 14.3.10. Let $\mathcal{A}$ be the set of all subgroups of N of the form $A_{g_1} \cdots A_{g_n}$ such that the map $(a_1, \ldots, a_n) \mapsto a_1 \ldots a_n$ defines an isomorphism

$$A_{g_1} \times \cdots \times A_{g_n} \simeq A_{g_1} \cdots A_{g_n}.$$

Note that $A = A_e \in \mathcal{A}$. Then pick an element of $\mathcal{A}$ of maximal order.

Proof.

(a) Consider

$$\varphi_g \left\{ \begin{array}{ccc} N & \mapsto & N \\ a & \mapsto & gag^{-1}. \end{array} \right.$$

For all $a, b \in N$, $\varphi_g(ab) = gabg^{-1} = gag^{-1}gbg^{-1} = \varphi_g(a)\varphi_g(b)$, thus φ_g is a group homomorphism.

Moreover, $\varphi_g \circ \varphi_{g^{-1}} = 1_N = \varphi_{g^{-1}} \circ \varphi_g$, so that φ is bijective: φ is a group automorphism.

Since A is normal subgroup of N, $A_g = \varphi_g(A)$ is also a normal subgroup of N.

Now take H a non trivial subgroup of A_g. Reasoning by contradiction assume that H is normal in N. Then $K = \varphi_g^{-1}(H) = g^{-1}Hg$ is a non trivial subgroup of A. Since H is normal in N, and φ_g is an automorphism of N, $K = \varphi_g^{-1}(H)$ is normal in N. This contradicts the fact that A is a minimal normal subgroup of N. This contradiction proves that H is not normal in N. We can conclude that A_g is a minimal normal subgroup of N.

(b) Let g be any element of G. The hypothesis gives the inclusions $A_g = gAg^{-1} \subset AA_{g_1}$ and $A_{gg_1} = (gg_1)A(gg_1)^{-1} \subset AA_{g_1}$, therefore, since AA_{g_1} is a subgroup,

$$\begin{aligned} gAA_{g_1}g^{-1} &= gAg^{-1}\ gA_{g_1}g^{-1} \\ &= gAg^{-1}\ gg_1Ag_1^{-1}g^{-1} \subset AA_{g_1}. \end{aligned}$$

This proves that AA_{g_1} is a normal subgroup of G.

(c) Let $\mathcal{A}$ be the set of all subgroups of N of the form $A_{g_1} \cdots A_{g_n}$ such that the map $(a_1, \ldots, a_n) \mapsto a_1 \ldots a_n$ defines an isomorphism

$$A_{g_1} \times \cdots \times A_{g_n} \simeq A_{g_1} \cdots A_{g_n}.$$

Note that $A = A_e \in \mathcal{A}$. Then pick an element H of $\mathcal{A}$ of maximal order. Then

$$H = A_{g_1} \cdots A_{g_n}, \qquad g_1, \dots, g_n \in G \subset N.$$

If $H = N$, then we are done. Assume now that $H \neq N$.

If $A_g \subset H$ for all $g \in G$, then H is normal in G:
for all $g \in G$, $A_{gg_i} = (gg_i)A(gg_i)^{-1} \subset H$, thus

$$gHg^{-1} = gA_{g_1}g^{-1}gA_{g_2}g^{-1} \cdots gA_{g_n}g^{-1} = A_{gg_1} \cdots A_{gg_n} \subset H.$$

Since $H \neq N$, and $H \neq \{e\}$ ($|H| \geq |A| > 1$), this is impossible by the minimality of N. Hence there is $g_{n+1} \in G$ such that $A_{g_{n+1}} \not\subset H$.

We don't know if H is normal in G, but $H = A_{g_1} \cdots A_{g_n}$ is normal in N, since all A_{g_i} are normal in N (see Exercise 7(a)). Hence $H \cap A_{g_{n+1}}$ is a normal subgroup in N, and lies in the minimal normal subgroup $A_{g_{n+1}}$ of N. Since $A_{g_{n+1}} \not\subset H$, $H \cap A_{g_{n+1}} \neq H$, therefore $H \cap A_{g_{n+1}} = \{e\}$. By Exercise 7, this proves that the map $(a_1, \dots, a_{n+1}) \mapsto a_1 \dots a_n$ defines an isomorphism

$$A_{g_1} \times \cdots \times A_{g_n} \times A_{g_{n+1}} \simeq A_{g_1} \cdots A_{g_n} A_{g_{n+1}} \subset N.$$

But $A_{g_{n+1}} \not\subset H$, thus $H = A_{g_1} \cdots A_{g_n} A_{g_{n+1}} \subsetneq A_{g_1} \cdots A_{g_n} A_{g_{n+1}} A_{g_{n+1}}$, and this contradicts the maximality of H. This contradiction proves that $H = N$, so that

$$N = A_{g_1} \cdots A_{g_n} \simeq A^n.$$

□

Ex. 14.3.7 *Let H and K be normal subgroups of a group G.*
Let $HK = \{hk \mid h \in H, k \in K\}$.

(a) Prove that HK is a normal subgroup of G.

(b) Assume that $H \cap K = \{e\}$. Prove that $hk = kh$ for all $h \in H, k \in K$.

(c) As in part (b), assume that $H \cap K = \{e\}$. Prove that the map $H \times K \to HK$ defined by $(h, k) \mapsto hk$ is a group isomorphism.

Proof.

(a)

- Since $e \in H, e \in K$, $e = ee \in HK$, thus $HK \neq \varnothing$.
- Let $x = hk, y = h'k'$ be any elements of HK, where $h, h' \in H,\ k, k' \in K$. Then

$$\begin{aligned} xy &= hkh'k' \\ &= hh'h'^{-1}kh'k' = h''k'', \end{aligned}$$

where $h'' = hh' \in H, k'' = (h'^{-1}kh')k'$, and $h'^{-1}kh' \in K$, since K is normal in G, so that $k'' = (h'^{-1}kh')k' \in K$. Thus $xy \in HK$

- If $x = hk \in HK$, where $h \in H, k \in K$, then

$$x^{-1} = k^{-1}h^{-1} = h^{-1}(hk^{-1}h^{-1}),$$

where $h^{-1} \in H$, and $hk^{-1}h^{-1} \in K$, since H is normal in G. Thus $x^{-1} \in HK$.

We have proved that HK is a subgroup of G. Moreover, if $x = hk \in HK$, and $g \in G$ then

$$gxg^{-1} = ghkg^{-1} = (ghg^{-1})(gkg^{-1}),$$

where $ghg^{-1} \in H, gkg^{-1}$ in K, since H, K are normal subgroups. Therefore HK is a normal subgroup of G.

(b) Assume that $H \cap K = \{e\}$. If $h \in H$, and $k \in K$, consider $z = hkh^{-1}k^{-1} \in G$. Then $z = h(kh^{-1}k^{-1})$, where $h \in H, kh^{-1}k^{-1} \in H$, so that $z \in H$. Similarly $z = (hkh^{-1})k^{-1}$, where $hkh^{-1} \in H$ and $k^{-1} \in K$, so that $z \in H \cap K = \{e\}$. Thus $hkh^{-1}k^{-1} = e$, which proves $hk = kh$.

$$(H \lhd G, K \lhd G, H \cap K = \{e\}) \Rightarrow \forall h \in H, \forall k \in K,\ hk = kh.$$

(c) As in part (b), assume that $H \cap K = \{e\}$. Define

$$\varphi \left\{ \begin{array}{ccc} H \times K & \mapsto & HK \\ (h, k) & \mapsto & hk. \end{array} \right.$$

- If $u = (h, k) \in H \times K, v = (h', k') \in H \times K$, then part (b) shows that $h'k = kh'$, thus

$$\begin{aligned} \varphi(uv) &= \varphi(hh', kk') \\ &= hh'kk' \\ &= hkh'k' \\ &= \varphi(u)\varphi(v), \end{aligned}$$

thus φ is a group homomorphism.

- If x is any element of HK, then by definition there are some $h, k,\ h \in H, k \in K$ such that $x = hk = \varphi(h, k)$, where $(h, k) \in H \times K$. Therefore φ is surjective.
- if $u = (h, k) \in \ker \varphi$, then $hk = e$, thus $h = k^{-1} \in H \cap K = \{e\}$, and $(h, k) = (e, e)$. This proves $\ker \varphi = \{(e, e)\}$, and φ injective.

We have proved that φ is a group isomorphism. ☐

Ex. 14.3.8 *Suppose that $\gamma, \gamma' : T \to \{1, \dots, l\}$ are one-to-one and onto. As explained in the text, these give isomorphisms $\hat{\gamma}, \hat{\gamma}' : S(T) \simeq S_l$.*

(a) Explain why $\sigma = \gamma \circ (\gamma')^{-1}$ is an element of S_l.

(b) Let $\sigma \in S_l$ be as in part (a), and let $\hat{\sigma} : S_l \to S_l$ be conjugation by σ. Thus $\hat{\sigma}(\tau) = \sigma\tau\sigma^{-1}$ for $\tau \in S_l$. Prove that $\hat{\gamma} = \hat{\sigma} \circ \hat{\gamma}'$.

This proves that $\hat{\gamma}$ and $\hat{\gamma}'$ differ by conjugation by an element of S_l.

Proof.

(a) Since $\gamma, \gamma' : T \to \{1, \dots, l\}$ are bijective, then $\sigma = \gamma \circ (\gamma')^{-1} : \{1, \dots, l\} \to \{1, \dots, l\}$ is bijective, so $\sigma \in S_l$.

(b) For all $\varphi \in S(T)$,

$$\begin{aligned} (\hat{\sigma} \circ \hat{\gamma}')(\varphi) &= \hat{\sigma}(\gamma' \circ \varphi \circ (\gamma')^{-1}) \\ &= \sigma \circ \gamma' \circ \varphi \circ (\gamma')^{-1} \circ \sigma^{-1} \\ &= \gamma \circ (\gamma')^{-1} \circ \gamma' \circ \varphi \circ (\gamma')^{-1} \circ \gamma' \circ \gamma^{-1} \\ &= \gamma \circ \varphi \circ \gamma^{-1} \\ &= \hat{\gamma}(\varphi), \end{aligned}$$

thus $\hat{\sigma} \circ \hat{\gamma}' = \hat{\gamma}$.

Note: Let G be a subgroup of $S(T)$, and $G_1 = \hat{\gamma}(G), G_2 = \hat{\gamma}'(G)$ the corresponding subgroups in S_l, then $G_1 = \hat{\sigma}(G_2) = \sigma G_2 \sigma^{-1}$ are conjugate subgroups. $\square$

Ex. 14.3.9 *Let G be a group of order n. In Section 7.4 we constructed a subgroup $H \subset S_n$ isomorphic to G. Prove that H is regular in S_n.*

Proof. Recall the construction of $G \simeq H \subset S_n$ (see ex. 7.4.4, 7.4.6).

Let $f : \{1, \ldots, n\} \to G$ be a bijection, and write $g_i = f(i)$, so that $G = \{g_1, \ldots, g_n\}$.

For each $i \in \{1, \ldots, n\}$ there is some permutation σ_i such that

$$g_i g_j = g_{\sigma_i(j)}.$$

Consider the maps

$$\begin{array}{ccccccc} \{1, \ldots, n\} & \stackrel{f}{\to} & G & \stackrel{\phi}{\to} & G' = \{\phi_g \mid g \in G\} & \stackrel{\psi}{\to} & H \\ i & \mapsto & g = g_i & \mapsto & \sigma = \phi_g \left\{ \begin{array}{ccc} G & \to & G \\ h & \mapsto & gh \end{array} \right. & \mapsto & f^{-1} \circ \phi_g \circ f, \end{array}$$

where $G' = \{\phi_g \mid g \in G\} \subset S(G), H \subset S_n$, and $G \simeq H$. Here f, ϕ, ψ are bijective, and ϕ, ψ are group isomorphisms (Ex .7.4.4).

Note that, as already seen in ex. 7.4.4, for all $j \in \{1, \ldots, n\}$,

$$\begin{aligned} (f^{-1} \circ \phi_{g_i} \circ f)(j) &= (f^{-1} \circ \phi_{g_i})(g_j) \\ &= f^{-1}(g_i g_j) \\ &= f^{-1}(g_{\sigma_i(j)} \\ &= \sigma_i(j), \end{aligned}$$

thus

$$\sigma_i = f^{-1} \circ \phi_{g_i} \circ f,$$

and $H = \{\sigma_1, \ldots, \sigma_n\}$.

Write $\delta = \psi \circ \phi \circ f$, so that $\delta(i) = (\psi \circ \phi \circ f)(i) = f^{-1} \circ \phi_{g_i} \circ f,\ i = 1, \ldots, n$.

We define $\gamma = \delta^{-1}$, thus for all $i \in \{1, \ldots, n\}$,

$$\gamma(f^{-1} \circ \phi_{g_i} \circ f) = i.$$

Here $T = \{1, \ldots, n\}$, since $H \subset S(\{1, \ldots, n\}$. Then $\gamma : G \to T$ induces an isomorphism $\hat{\gamma} : S(G) \to S(T) = S_n$ defined by

$$\hat{\gamma}(\sigma) = \gamma \circ \sigma \circ \gamma^{-1}.$$

Now we compute $\hat{\gamma}(\varphi_h)$, where $h \in H$ is a permutation, and $\varphi_h(k) = hk = h \circ k,\ k \in H$. Since $h \in H$, there is some $i \in \{1, \ldots, n\}$ such that $h = f^{-1} \circ \phi_{g_i} \circ f = \sigma_i$.

For all $j \in \{1, \dots, n\}$,

$$\begin{aligned}
\hat{\gamma}(\varphi_h)(j) &= (\gamma \circ \varphi_h \circ \gamma^{-1})(j)\\
&= (\gamma \circ \varphi_h)(f^{-1} \circ \phi_{g_j} \circ f)\\
&= \gamma(h \circ f^{-1} \circ \phi_{g_j} \circ f)\\
&= \gamma(f^{-1} \circ \phi_{g_i} \circ f \circ f^{-1} \circ \phi_{g_j} \circ f)\\
&= \gamma(f^{-1} \circ \phi_{g_i} \circ \phi_{g_j} \circ f)\\
&= \gamma(f^{-1} \circ \phi_{g_i g_j} \circ f)\\
&= \gamma(f^{-1} \circ \phi_{g_{\sigma_i(j)}} \circ f)\\
&= \sigma_i(j).
\end{aligned}$$

Therefore $\hat{\gamma}(\varphi_h) = \sigma_i = h \in H$.

We have proved that the isomorphism $\hat{\gamma}$ takes $\{\varphi_h \mid h \in H\}$ in H, and since these two subgroups have same order n,

$$\hat{\gamma}(\{\varphi_h \mid h \in H\}) = H.$$

The definition of a regular subgroup of $S(T)$ is satisfied, so H is a regular subgroup of S_n. □

Ex. 14.3.10 *A permutation group $G \subset S_l$ is regular if there is a one-to-one onto map $\gamma : G \to \{1, \dots, l\}$ such that $\hat{\gamma} : S(G) \simeq S_l$ maps $\{\varphi_g \mid g \in G\} \subset S(G)$ to $G \subset S_l$. Recall that $\varphi_g \in S(G)$ is defined by $\varphi_g(h) = gh$ for $h \in G$. The goal of this exercise is to show that G is regular if and only if it is transitive with trivial isotropy subgroups.*

(a) Let $G \subset S_l$ be regular. Prove that G is transitive and that the isotropy subgroups of G are trivial.

(b) For the rest of the exercise, assume that G is transitive with trivial isotropy subgroups. Define $\gamma : G \to \{1, \dots, l\}$ by $\gamma(\tau) = \tau(1)$ for $\tau \in G$. Prove that this map is one-to-one and onto.

(c) The map γ of part (b) gives $\hat{\gamma} : S(G) \simeq S_l$. Show that $\hat{\gamma}(\varphi_g) = g$, and conclude that G is regular.

Proof.

(a) Recall that $\hat{\gamma}(\sigma) = \gamma \circ \sigma \circ \gamma^{-1}$ for all $\sigma \in S_l$.

Let i, j be any elements in $\{1, \dots, l\}$. We must find $g' \in G$ such that $g'(i) = j$.

Take $g = \gamma^{-1}(j)[\gamma^{-1}(i)]^{-1} \in G$, and $g' = \hat{\gamma}(\varphi_g)$. Then $g' \in G$ since $\hat{\gamma}$ maps $\{\varphi_g \mid g \in G\}$ to G.

Then $g\gamma^{-1}(i) = \gamma^{-1}(j)$, thus $(\gamma \circ \varphi_g \circ \gamma^{-1})(i) = j$, that is $g'(i) = (\hat{\gamma}(\varphi_g))(i) = j$, where $g' \in G$. This proves that G is transitive.

Let i be any element in $\{1, \dots, l\}$, and take $g' \in G_i$, where G_i is the isotropy subgroup of i, so that $g'(i) = i$. Since $\hat{\gamma}$ maps $\{\varphi_g \mid g \in G\} \subset S(G)$ to G, there exists some $g \in G$ such that $g' = \hat{\gamma}(\varphi_g) = \gamma \circ \phi_g \circ \gamma^{-1}$.

Then $g'(i) = i$ implies $g\gamma^{-1}(i) = \gamma^{-1}(i)$, thus $g = e, \phi_g = e$, and $g' = \gamma \circ \phi_g \circ \gamma^{-1} = e$, where $e = 1_G$ is the identity element of G. Therefore $G_i = \{e\}$ for all $i \in \{1, \dots, l\}$.

(b) We prove first that γ is injective. Suppose that $\gamma(\tau) = \gamma(\tau')$, where $\tau, \tau' \in G$. Then $\tau(1) = \tau'(1)$, thus $(\tau^{-1} \circ \tau')(1) = 1$, and $\tau^{-1} \circ \tau' \in G_1$, where G_1 is the isotropy subgroup of 1. But $G_1 = \{e\}$, thus $\tau^{-1} \circ \tau' = e$, and $\tau = \tau'$. We have proved that γ is injective.

Now take i be any element in $\{1, \ldots, l\}$. Since G is transitive, there is some $\tau \in G$ such that $\tau(1) = i$, that is $\gamma(\tau) = i, \tau \in G$. This proves that γ is surjective.

$\gamma : G \to \{1, \ldots, n\}$ is bijective.

(c) let i be any element in $\{1, \ldots, l\}$. Since G is transitive, there is some $\tau \in G$ such that $\tau(1) = i$, thus $\gamma(\tau) = i$. Therefore

$$\begin{aligned} [\hat{\gamma}(\varphi_g)](i) &= (\gamma \circ \varphi_g \circ \gamma^{-1})(i) \\ &= (\gamma \circ \varphi_g)(\tau) \\ &= \gamma(g\tau) \\ &= (g\tau)(1) = g(i). \end{aligned}$$

Since this is true for all i,

$$\hat{\gamma}(\varphi_g) = g.$$

This proves that the isomorphism $\hat{\gamma}$ maps $\{\varphi \mid g \in G\}$ in G, and since these two subgroup have same order l, $\hat{\gamma}$ maps $\{\varphi_g \mid g \in G\}$ on G.

G is a regular subgroup of S_l.

□

Note: This proves also that $G \subset S_l$ is regular iff there is some bijective $\gamma : G \to \{1, \ldots l\}$ such that $\hat{\gamma}$ maps φ_g to g, for every $g \in G$.

Ex. 14.3.11 *We can regard $\mathbb{F}_p^n$ as both a group (under addition) and a vector space over $\mathbb{F}_p$ (under addition and scalar multiplication). However, since we are over $\mathbb{F}_p$, scalar multiplication can be buildt out of addition. Use this observation to prove the following:*

(a) Any subgroup of $\mathbb{F}_p^n$ is a subspace.

(b) Any group homomorphism $\gamma : \mathbb{F}_p^n \to \mathbb{F}_p^n$ is linear.

Proof.

(a) Let H be a subgroup of $\mathbb{F}_p^n$. If $v = (\alpha_1, \ldots, \alpha_n) \in H$, we show by induction on $k \in \mathbb{N}$ that $[k]_p v \in H$. First $[0]_p v = (0, \ldots, 0) \in H$. If $[k]_p v \in H$, then $[k+1]_p v = [k]_p v + v \in H$. Therefore

$$\forall k \in \mathbb{N},\ [k]_p v \in H.$$

Since for every $\lambda \in \mathbb{F}_p$, there is some $k \in \mathbb{N}$ such that $\lambda = [k]_p$, we can conclude that, for all $v \in H$, for all $\lambda \in \mathbb{F}_p$, $\lambda v \in H$. Thus H is a subspace of $\mathbb{F}_p^n$.

(b) Let $\gamma : \mathbb{F}_p^n \to \mathbb{F}_p^n$ a group homomorphism. if $v \in \mathbb{F}_p^n$, We show by induction that $\gamma([k]_p v) = [k]_p \gamma(v)$ for $k \in \mathbb{N}$.

For $k = 0$, $\gamma([0]_p v) = 0 = [0]_p \gamma(v)$. If $\gamma([k]_p v) = [k]_p \gamma(v)$ for some $k \in \mathbb{N}$, then, since γ is a group homomorphism,

$$\gamma([k+1]_p v) = \gamma([k]_p v + v) = \gamma([k]_p v) + \gamma(v) = [k]_p \gamma(v) + \gamma(v) = ([k]_p + 1)\gamma(v) = [k+1]_p \gamma(v).$$

Therefore $\gamma([k]_p v) = [k]_p \gamma(v)$ for all $k \in \mathbb{N}$. This proves that $\gamma(\lambda v) = \lambda f(v)$ for all $v \in \mathbb{F}_p^n$, for all $\lambda \in \mathbb{F}_p$, thus γ is linear.

□

Ex. 14.3.12 *This exercise will use the notation of the proof of Proposition 14.3.20.*

(a) Suppose that $V \subset \mathbb{F}_p^n$ is a nontrivial subspace such that $g(V) \subset V$ for all $g \in G_0$. Use the cosets of V in $\mathbb{F}_p^n$ to prove that G is imprimitive.

(b) Explain why $\mathbb{F}_p^n$ is normal in G, and prove that $G/\mathbb{F}_p^n \simeq G_0$. Use this to prove part (b) of Proposition 14.3.20.

Proof. Here
$$\mathbb{F}_p^n \subset G \subset \mathrm{AGL}(n, \mathbb{F}_p) \subset S_{p^n}.$$

(a) Consider a complete system $\{a_1, \dots, a_n\}$ of representatives of cosets of V in $\mathbb{F}_p^n$, so that the cosets of V are the disjoint cosets
$$R_1 = a_1 + V, \dots, R_k = a_k + V.$$

Then $\mathbb{F}_p^n = \bigcup_{i=1}^k (a_i + V)$ is the disjoint union of parallel affine subspaces.

Let $g \in G \subset \mathrm{GL}(n, \mathbb{F}_p)$. Recall (see the text following Corollary 14.3.18) that
$$G = \{\gamma_{A,w} \mid w \in \mathbb{F}_p^n, A \in G_0\},$$

thus $g = \gamma_{A,w}$, for some $w \in \mathbb{F}_p^n$ and $A \in G_0$. For all $v \in V$
$$g \cdot (a_i + v) = A \cdot (a_i + v) + w = A \cdot a_i + w + A \cdot v.$$

Since $A \in G_0$, $A \cdot V \subset V$, thus $g \cdot (a_i + v) \in (A \cdot a_i + w) + V$. The cosets R_i, $1 \leq i \leq k$, partition $\mathbb{F}_p^n$, thus there is some index j such that $A \cdot a_i + w \in R_j = a_j + V$, so that $A \cdot a_i + w + V = a_j + V$, and
$$g(a_i + V) \subset a_j + V.$$

Moreover, the cosets $R_i = a_i + V$ have same cardinality, and g is bijective, therefore $|a_j + V| = |a_i + V| = |g(a_i + V)|$. This proves
$$g(a_i + V) = a_j + V.$$

To conclude, there is a partition of $\mathbb{F}_p^n$ such that for every $1 \leq i \leq k$, we have $g(R_i) = R_j$ for some $1 \leq j \leq k$. Since $1 < |V| < p^n$, then $k > 1$ and $|R_1| = \cdots = |R_k| > 1$. This proves that $G \subset S_{p^n}$ is imprimitive.

(b) We have seen in Exercise 2 that the group homomorphism
$$\varphi \left\{ \begin{array}{ccc} \mathrm{AGL}(n, \mathbb{F}_q) & \to & \mathrm{GL}(n, \mathbb{F}_q) \\ \gamma_{A,v} & \mapsto & A. \end{array} \right.$$

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

Consider the restriction φ_0 of φ, defined by
$$\varphi_0 \left\{ \begin{array}{ccc} G & \to & G_0 \\ \gamma_{A,v} & \mapsto & A. \end{array} \right.$$

Since $G = \{\gamma_{A,w} \mid w \in \mathbb{F}_p^n, A \in G_0\}$, φ_0 is surjective, and $\ker \varphi_0 = \{\gamma_{I_n,w} \mid w \in \mathbb{F}_{p^n}\} \simeq \mathbb{F}_p^n$, thus, with the usual identification $\{\gamma_{I_n,w} \mid w \in \mathbb{F}_{p^n}\} = \mathbb{F}_p^n$, $\mathbb{F}_p^n$ is a normal subgroup of G, and
$$G/\mathbb{F}_p^n \simeq G_0.$$

Now we prove (b).

By Theorem 8.1.4, G is solvable if and only if $\mathbb{F}_p^n$ and $G/\mathbb{F}_p^n$ are normal. Since we know that $\mathbb{F}_p^n$ is a normal subgroup of G, we obtain the equivalence

$$G \text{ is solvable} \iff G_0 \text{ is solvable}.$$

□

Ex. 14.3.13 *Consider the definition of k-transitive given in the Mathematical Notes.*

(a) Prove that S_n is n-transitive.

(b) Prove that A_n is $(n-2)$-transitive when $n \geq 3$.

Proof.

(a) Take any ordered n-tuple $(a_1, \ldots, a_n)$ of distinct elements of $\{1, \ldots n\}$. Then consider the map

$$\sigma \left\{ \begin{array}{ccc} \{1, \ldots, n\} & \to & \{1, \ldots, n\} \\ i & \mapsto & a_i. \end{array} \right.$$

Then $\{a_1, \ldots, a_n\} \subset \{1, \ldots, n\}$ and, since the a_i are distinct, $|\{a_1, \ldots, a_n\}| = n$, so that $\{a_1, \ldots, a_n\} = \{1, \ldots, n\}$. This shows that σ is surjective, and since the a_i are distinct, σ is injective, thus σ is a permutation: $\sigma \in S_n$

($\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ a_1 & a_2 & \cdots & a_n \end{pmatrix}$ is the only permutation such that $\sigma(i) = a_i,\ i = 1, \ldots, n$).

Since

$$\sigma \cdot (1, \ldots, n) = (a_1, \ldots, a_n),$$

the orbit of $(1, \ldots, n)$ is the whole set P_n of ordered n-tuples of distinct elements of $\{1, \ldots, n\}$. This proves that there is only one orbit, and that G acts transtitively on P_n, i.e. S_n is n-transitive.

(b) Take any ordered $(n-2)$-tuple $(a_1, \ldots, a_{n-2})$ of distinct elements of $\{1, \ldots, n\}$. Name a, b the two remaining elements:

$$\{a, b\} = \{1, \ldots, n\} \setminus \{a_1, \ldots, a_{n-2}\}.$$

Consider the two permutations

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n-2 & n-1 & n \\ a_1 & a_2 & \cdots & a_{n-2} & a & b \end{pmatrix},$$

$$\tau = \begin{pmatrix} 1 & 2 & \cdots & n-2 & n-1 & n \\ a_1 & a_2 & \cdots & a_{n-2} & b & a \end{pmatrix}.$$

Then $\sigma \cdot (1, \ldots, n-2) = (a_1, \ldots, a_{n-2}) = \tau \cdot (1, \ldots, n-2)$.

But $\tau = (a\, b)\sigma$, thus one of the two permutations σ, τ is in A_n, therefore $(a_1, \ldots, a_{n-2})$ is in the orbit $A_n \cdot (1, \ldots, n-2)$ of $(1, \ldots, n-2) \in P_{n-2}$. Therefore A_n acts transitively on P_{n-2}. A_n is $(n-2)$-transitive. □

Ex. 14.3.14 *Consider the groups* $\mathrm{GL}(2,\mathbb{F}_q), \mathrm{SL}(2,\mathbb{F}_q), \mathrm{PGL}(2,\mathbb{F}_q)$, *and* $\mathrm{PSL}(2,\mathbb{F}_q)$ *defined in the Mathematical Notes.*

(a) Prove that $|\mathrm{GL}(2,\mathbb{F}_q)| = q(q-1)(q^2-1)$.

(b) Prove that $|\mathrm{SL}(2,\mathbb{F}_q)| = |\mathrm{PGL}(2,\mathbb{F}_q)| = q(q^2-1)$.

(c) Prove that $\mathrm{PSL}(2,\mathbb{F}_q) \simeq \mathrm{SL}(2,\mathbb{F}_q)/\{\pm I_2\}$, *and conclude that*

$$|\mathrm{PSL}(2,\mathbb{F}_q)| = \left\{ \begin{array}{ll} \frac{1}{2}q(q^2-1), & q \ne 2^n \\ q(q^2-1), & q = 2^n. \end{array} \right.$$

(d) Compute $|\mathrm{PSL}(2,\mathbb{F}_q)|$ *for* $q = 2,3,4,5,7$.

(e) Show that $|\mathrm{GL}(3,\mathbb{F}_2)| = |\mathrm{PSL}(3,\mathbb{F}_2)| = 168$.

Proof.

(a) To build an 2×2 matrix $A \in \mathrm{GL}(2,\mathbb{F}_q)$, we must first choose a nonzero vector $u \in \mathbb{F}_q^2$ (the first column of the matrix), then a vector $v \not\in \mathbb{F}_q u$ (the second column). Since $|\mathbb{F}_q^2 \setminus \{0\}| = q^2-1$, and $|\mathbb{F}_q^2 \setminus \mathbb{F}_q u| = q^2 - q$, we obtain

$$|\mathrm{GL}(2,\mathbb{F}_q)| = (q^2-1)(q^2-q) = q(q-1)(q^2-1).$$

(b) $\mathrm{SL}(2,\mathbb{F}_q)$ is the kernel of the surjective homomorphism $det : \mathrm{GL}(2,\mathbb{F}_q) \to \mathbb{F}_q^*$, so that

$$\mathrm{GL}(2,\mathbb{F}_q)/\mathrm{SL}(2,\mathbb{F}_q) \simeq \mathbb{F}_q^*.$$

Therefore $|\mathrm{GL}(2,\mathbb{F}_q)|/|\mathrm{SL}(2,\mathbb{F}_q)| = |\mathbb{F}_q^*|$, thus

$$|\mathrm{SL}(2,\mathbb{F}_q)| = q(q-1)(q^2-1)/(q-1) = q(q^2-1).$$

The definition

$$\mathrm{PGL}(2,\mathbb{F}_q) = \mathrm{GL}(2,\mathbb{F}_q)/\mathbb{F}_q^* I_n$$

gives

$$|\mathrm{PGL}(2,\mathbb{F}_q)| = q(q-1)(q^2-1)/(q-1) = q(q^2-1).$$

(c) Consider the restriction of the canonical projection $\pi : \mathrm{GL}(2,\mathbb{F}_q) \to \mathrm{GL}(2,\mathbb{F}_q)/\mathbb{F}_q^* I_n$ to $\mathrm{SL}(2,\mathbb{F}_q)$. We obtain

$$\varphi \left\{ \begin{array}{ccc} \mathrm{SL}(2,\mathbb{F}_q) & \to & \mathrm{PGL}(2,\mathbb{F}_q) \\ A & \mapsto & [A]. \end{array} \right.$$

If $A \in \mathrm{SL}(2,\mathbb{F}_q)$ is such that $[A] = [I_2]$, then $A = \lambda I_2, \lambda \in \mathbb{F}_q^*$, and $\det(A) = \lambda^2 = 1$, so that $\lambda = \pm 1$. We have proved $\ker(\pi_1) = \{I_2, -I_2\}$ (where $I_2 = -I_2$ if the characteristic is 2). Therefore

$$\mathrm{Im}\,(\varphi) \simeq \mathrm{SL}(2,\mathbb{F}_q)/\{I_2, -I_2\}.$$

Note that φ is not surjective.

By the definition given in the mathematical notes, $\mathrm{Im}\,\varphi = \mathrm{PSL}(2,\mathbb{F}_q)$, thus

$$\mathrm{PSL}(2,\mathbb{F}_q) \simeq \mathrm{SL}(2,\mathbb{F}_q)/\{I_2, -I_2\}.$$

If $q = 2^n$, then the characteristic of $\mathbb{F}_q$ is 2, and $I_2 = -I_2$, so that $|\mathrm{PGL}(2,\mathbb{F}_q)| = |\mathrm{SL}(2,\mathbb{F}_q)|$. Otherwise $|\mathrm{PGL}(2,\mathbb{F}_q)| = \frac{1}{2}|\mathrm{SL}(2,\mathbb{F}_q)|$. This proves

$$|\mathrm{PSL}(2,\mathbb{F}_q)| = \left\{ \begin{array}{ll} \frac{1}{2}q(q^2-1), & q \ne 2^n \\ q(q^2-1), & q = 2^n. \end{array} \right.$$

(d)

q	2	3	4	5	7
$\lvert\mathrm{PSL}(2,\mathbb{F}_q)\rvert$	6	12	60	60	168

(e) The same reasoning as in part (a) shows that

$$|\mathrm{GL}(3,\mathbb{F}_q)| = (q^3-1)(q^3-q)(q^3-q^2),$$

thus, for $q=2$,

$$|\mathrm{GL}(3,\mathbb{F}_2)| = 168.$$

As in parts (b) and (c),

$$\mathrm{GL}(3,\mathbb{F}_q)/\mathrm{SL}(3,\mathbb{F}_q) \simeq \mathbb{F}_q^*, \qquad \mathrm{PSL}(3,\mathbb{F}_q) \simeq \mathrm{SL}(3,\mathbb{F}_q)/\{\pm I_2\}.$$

For $q=2$, $I_2=-I_2$, and $\mathbb{F}_q^* = \{1\}$, thus

$$|\mathrm{PSL}(3,\mathbb{F}_2)| = |\mathrm{SL}(3,\mathbb{F}_2)| = |\mathrm{GL}(3,\mathbb{F}_2)| = 168.$$

□

Ex. 14.3.15 *Prove that* $\mathrm{GL}(2,\mathbb{F}_2) = \mathrm{SL}(2,\mathbb{F}_2) \simeq \mathrm{PSL}(2,\mathbb{F}_2) \simeq S_3$, *and* $\mathrm{PSL}(2,\mathbb{F}_3) \simeq A_4$.

Proof. Since $\mathrm{SL}(2,\mathbb{F}_2)$ is the kernel of the surjective homomorphism $det : \mathrm{GL}(2,\mathbb{F}_2) \to \mathbb{F}_2^*$, where $\mathbb{F}_2^* = \{1\}$ is trivial, we obtain $\mathrm{SL}(2,\mathbb{F}_2) = \mathrm{GL}(2,\mathbb{F}_2)$.

By part (c) of Exercise 14, $\mathrm{PGL}(2,\mathbb{F}_q) \simeq \mathrm{SL}(2,\mathbb{F}_q)/\{I_2,-I_2\}$. For $q=2$, $I_2=-I_2$, thus

$$\mathrm{PGL}(2,\mathbb{F}_2) \simeq \mathrm{SL}(2,\mathbb{F}_2) = \mathrm{GL}(2,\mathbb{F}_2).$$

Moreover,

$$\mathrm{GL}(2,\mathbb{F}_2) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\},$$

thus $|\mathrm{GL}(2,\mathbb{F}_2)| = 6$, and $\mathrm{GL}(2,\mathbb{F}_2)$ is not Abelian:

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}.$$

Since there is only one non Abelian group of order 6, up to isomorphism,

$$\mathrm{GL}(2,\mathbb{F}_2) = \mathrm{SL}(2,\mathbb{F}_2) \simeq \mathrm{PSL}(2,\mathbb{F}_2) \simeq S_3.$$

To prove the last inclusion, we use the action of $\mathrm{PGL}(2,F)$ on $F \cup \{\infty\}$ described in section 7.5. We resume this description in the following lemma:

Lemma. *The operation defined for all* $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ *and* $z \in \dot{F}$ *by*

$$[M]\cdot z = \frac{az+b}{cz+d}, \qquad (z \in F \setminus \{-d/c\}),$$

and also

$$[M]\cdot(-d/c) = \infty, \qquad [M]\cdot\infty = a/c \qquad ([M]\cdot\infty = \infty \textit{ if } c = 0).$$

is a (left) action of $\mathrm{PGL}(2, F)$ *on the projective line* $\dot{F}$.

In this exercise, $F = \mathbb{F}_3$. Consider the restriction of this action to the subgroup $\mathrm{PSL}(2, \mathbb{F}_3)$ on $\dot{\mathbb{F}}_3 = \mathbb{F}_3 \cup \{\infty\} = \{0, 1, 2, \infty\}$.

This action defines a group homomorphism

$$\varphi \left\{ \begin{array}{ccc} \mathrm{PSL}(2, \mathbb{F}_3) & \to & S(\dot{\mathbb{F}}_3) \\ [M] & \mapsto & \varphi([M]) \left\{ \begin{array}{ccc} \dot{\mathbb{F}}_3 & \to & \dot{\mathbb{F}}_3 \\ z & \mapsto & [M] \cdot z. \end{array} \right. \end{array} \right.$$

We show that $\ker(\varphi)$ is trivial (the action is faithful): Let $[M] \in \mathrm{PSL}(2, \mathbb{F}_3)$, with $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{F}_3)$, such that $\varphi([M])$ is the identity of $\dot{\mathbb{F}}_3$. Then, for all $z \in \dot{\mathbb{F}}_3$, $[M] \cdot z = z$. The equality $[M] \cdot \infty = \infty$ shows that $c = 0$. Thus for every $z \in \mathbb{F}_3$,

$$\frac{az + b}{d} = z,$$

and then $az + b = dz$, $(a - d)z + b = 0$. With $z = 0$, we obtain $b = 0$, and with $z = 1$, $a - d = 0$. Therefore $M = aI_2$, $a \in \mathbb{F}_3$, and $[M] = [I_2]$. We have proved that the kernel of the action is trivial, in other words φ is injective, and $\mathrm{PSL}(2, \mathbb{F}_3) \simeq \mathrm{Im}\,(\varphi) \subset S(\dot{\mathbb{F}}_3)$ is isomorphic to a subgroup of $S(\dot{\mathbb{F}}_3) \simeq S_4$, therefore $\mathrm{PSL}(2, \mathbb{F}_3)$ is isomorphic to a subgroup of S_4. By Exercise 14, parts (c) and (d), $|\mathrm{PSL}(2, \mathbb{F}_3) = 12$, and the only subgroup of S_4 of order 12 is A_4. Therefore

$$\mathrm{PSL}(2, \mathbb{F}_3) \simeq A_4.$$

□

Note: We explain why the permutations corresponding to elements of $\mathrm{PSL}(2, \mathbb{F}_3) \simeq A_4$ are even, with another proof of this isomorphism.

Let $[T], [S]$ the two elements of $\mathrm{PSL}(2, \mathbb{F}_3)$ defined by $[T] \cdot z = z + 1$ and $[S] \cdot z = -1/z$, corresponding to the matrices

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \qquad S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad T, S \in \mathrm{SL}(2, \mathbb{F}_3).$$

The permutation of $\dot{\mathbb{F}}_3$ corresponding to $[T], [S]$ by φ are

$$\varphi([T]) = \begin{pmatrix} 0 & 1 & 2 & \infty \\ 1 & 2 & 0 & \infty \end{pmatrix} = (0\,1\,2), \qquad \varphi([S]) = \begin{pmatrix} 0 & 1 & 2 & \infty \\ \infty & 2 & 1 & 0 \end{pmatrix} = (0\,\infty)(1\,2)$$

If we take a numbering of $\dot{\mathbb{F}}_3$ to $\{1, 2, 3, 4\}$, for instance $f : 0 \mapsto 1, 1 \mapsto 2, 2 \mapsto 3, \infty \mapsto 4$, the permutations corresponding to T, S are $(1\,2\,3), (1\,4)(2\,3)$, both even.

A well known theorem shows that the matrices $[T], [S]$ generate $\mathrm{PSL}(2, \mathbb{Z})$: every matrix $M \in \mathrm{SL}(2, \mathbb{Z})$ is of the form

$$M = \pm U_1 \cdots U_k, \quad U_i \in \{T, S\}.$$

Reducing modulo 3, every matrix $M \in \mathrm{SL}(2, \mathbb{F}_3)$ is of the same form, thus $[T], [S]$ generate $\mathrm{PSL}(3, \mathbb{F}_3)$. This proves that the permutations corresponding to $\mathrm{PSL}(3, \mathbb{F}_3) = \langle [S], [T] \rangle$ are all even, and the argument of cardinality shows that $\mathrm{PSL}(3, \mathbb{F}_3) \simeq \mathrm{Im}\,(\varphi) \simeq A_4$.

With Sage:

```
G = PermutationGroup(['(1,4)(2,3)','(1,2,3)'])
G.order()
 12
G.structure_description()
       'A4'
```

This confirms $A_4 = \langle (1\,4)(2\,3), (1\,2\,3)\rangle$, and consequently $\mathrm{PSL}(3, \mathbb{F}_3) = \langle [S], [T]\rangle$.

Note 2: The same method can be applied to prove anew the first isomorphism $\mathrm{PSL}(2, \mathbb{F}_2) \simeq S_3$. Indeed, the action of $\mathrm{PGL}(2, \mathbb{F}_2)$ on $\mathbb{F}_2 \cup \{\infty\} = \{0, 1, \infty\}$, restricted to $\mathrm{PSL}(2, \mathbb{F}_2)$, gives an injective group homomorphism

$$\varphi \left\{ \begin{array}{ccc} \mathrm{PSL}(2,\mathbb{F}_2) & \to & S(\dot{\mathbb{F}}_2) \simeq S_3 \\ {[M]} & \mapsto & \varphi([M]) \left\{ \begin{array}{ccc} \dot{\mathbb{F}}_2 & \to & \dot{\mathbb{F}}_2 \\ z & \mapsto & [M]\cdot z. \end{array} \right. \end{array} \right.$$

Moreover $|\mathrm{PSL}(2, \mathbb{F}_2)| = |S(\dot{\mathbb{F}}_2)| = 6$, thus φ is bijective. Therefore $\mathrm{PSL}(2, \mathbb{F}_2) \simeq S_3$.

Ex. 14.3.16 *Let G be a finite group with socle H. Prove that H is isomorphic to a product of finite simple groups.*

Proof. If G has a unique minimal normal subgroup N, then the socle H is N, and by Proposition 14.3.10, $H = N$ is a product of finite simple groups.

Suppose now that G contains two minimal normal subgroups $N_1 \ne N_2$. Then $N_1 \cap N_2$ is normal in G, and N_1 is a minimal normal subgroup, therefore $N_1 \cap N_2 = N_1$ or $N_1 \cap N_2 = \{e\}$, and using the minimality of N_2, $N_1 \cap N_2 = N_2$ or $N_1 \cap N_2 = \{e\}$. If $N_1 \cap N_2 \ne \{e\}$, then $N_1 = N_1 \cap N_2 = N_2$, in contradiction with the assumption, thus $N_1 \cap N_2 = \{e\}$.

By Exercise 7, N_1N_2 is a normal subgroup of G, such that $(x_1, x_2) \mapsto x_1x_2$ is an isomorphism from $N_1 \times N_2$ to N_1N_2.

Consider $\mathcal{A}$ the set of all subgroups of G of the form $N_1 \cdots N_k$ such that $N_1 \cdots N_k$ is a normal subgroup of G, and such that the map $(x_1, \ldots, x_k) \mapsto x_1 \cdots x_k$ is an isomorphism from $N_1 \times \cdots \times N_k$ to $N_1 \cdots N_k$.

Then pick $A = N_1 \cdots N_k$ an element of $\mathcal{A}$ of maximal order. Reasoning by contradiction, suppose that $A \ne H$. Then there is some minimal normal subgroup N such that $N \not\subset A$, otherwise the socle, which is the subgroup H generated by the minimal normal subgroups of G would be $A = N_1 \cdots N_k$. Write $N_{k+1} = N$.

Then $N_1 \cdots N_k \cap N_{k+1} \ne N_{k+1}$, thus the minimality of N shows that $N_1 \cdots N_k \cap N_{k+1} = \{e\}$. Then Exercise 7 shows that $(N_1 \cdots N_k)N_{k+1}$ is normal, and the map $(x_1, \ldots, x_k) \mapsto x_1 \cdots x_{k+1}$ is an isomorphism from $N_1 \times \cdots \times N_{k+1}$ to $N_1 \cdots N_{k+1}$.

Therefore $N_1 \cdots N_{k+1} \in \mathcal{A}$, and since $|N_1 \cdots N_{k+1}| > |N_1 \cdots N_k| = |A|$, this contradicts the maximality of A.

This proves $H = N_1 \cdots N_k$, so that the socle $H = N_1 \cdots N_k \simeq N_1 \times \cdots N_k$ is a direct product of minimal normal subgroups, and by Proposition 14.3.10, each of them is isomorphic to a direct product of simple group. We have proved that H is isomorphic to a product of finite simple groups.

$\square$

Ex. 14.3.17 *Prove Galois' formula (14.18) for* $\mathrm{AGL}(n, \mathbb{F}_p)$*:*

$$|\mathrm{AGL}(n, \mathbb{F}_p)| = p^n(p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}).$$

Proof. We have seen in Exercise 2 that $\mathrm{AGL}(n, \mathbb{F}_p)/\mathbb{F}_p^n \simeq \mathrm{GL}(n, \mathbb{F}_p)$, thus

$$|\mathrm{AGL}(n, \mathbb{F}_p)| = p^n |\mathrm{GL}(n, \mathbb{F}_p)|.$$

To construct a matrix $A \in \mathrm{GL}(n, \mathbb{F}_p)$, we must choose the successive columns c_i of the matrix A, so that $(c_1, \ldots, c_n)$ is a base of $\mathbb{F}_p^n$. This is equivalent to take $c_1 \neq 0$, then $c_2 \notin \langle c_1 \rangle$, then $c_3 \notin \langle c_1, c_2 \rangle$,..., up to $c_n \notin \langle c_1, \ldots, c_{n-1} \rangle$. Since $|\langle c_1, \ldots, c_k \rangle| = p^k$, when $c_1, \ldots, c_k$ are linearly independent, we obtain $|\mathrm{GL}(n, \mathbb{F}_p)| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1})$, thus

$$|\mathrm{AGL}(n, \mathbb{F}_p)| = p^n(p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}).$$

□

Ex. 14.3.18 *Here are some observations related to Exercise 5.*

(a) Give an example to show that Exercise 5 is false if we drop the assumption that A and B are non-Abelian.

(b) Let $A_1, \ldots, A_r$ be non-Abelian simple groups. Determine all nontrivial normal subgroups of $A_1 \times \cdots \times A_r$.

Proof.

(a) Consider the group $G = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} = A \times B$, where $A = B = \mathbb{Z}/3\mathbb{Z}$ is simple. This is the additive group of the vector space $\mathbb{F}_3^2$. If $v = (1, 2)$ (for instance), the vectorial line

$$N = \mathbb{F}_3 \cdot v = \{(0, 0), (1, 2), (2, 1)\}$$

is a subspace of $\mathbb{F}_3^2$, therefore a subgroup of G. Moreover N is normal and not trivial, and $N \neq \{0\} \times B, N \neq A \times \{0\}$. This counterexample shows that Exercise 5 is false if we drop the assumption that A and B are non-Abelian.

(b) We will follow the steps of Exercise 5.

- First, note that the subsets $H_1 \times \cdots H_r \subset G$, where $H_i = \{e_{A_i}\}$ or $H_i = A_i$ for all $i = 1, \ldots r$, are normal subgroups of $G = A_1 \times \cdots \times A_r$:

  Take $h = (h_1, \ldots, h_r) \in N = H_1 \times \cdots H_r$, and $a = (a_1, \ldots, a_r) \in G$, then $aha^{-1} = (a_1 h_1 a_1^{-1}, \ldots, a_r h_r a_r^{-1})$. If $H_i = \{e_{A_i}\}$, then $a_i h_i a_i^{-1} = a_i a_i^{-1} = e_{A_i} \in H_i$, and if $H_i = A_i$, then $a_i h_i a_i^{-1} \in H_i$, thus $aha^{-1} \in N$.

  We will call these subgroups standard normal subgroups.

- To prove that these standard subgroups are the only normal subgroups of G, we use induction on r. The case $r = 2$ is done is Exercise 5.

  For simplicity, we write e for the identity of each group H_i.

  Now suppose that for any $k < r$, and for any k-tuple $(A_1, \ldots, A_k)$ of non-Abelian simple groups, the only normal subgroups of $A = A_1 \times \cdots \times A_k$ are $H_1 \times \cdots H_k$, where $H_i = \{e\}$ or $H_i = A_i$ for all $i = 1, \ldots k$.

  Now let $A_1, \ldots, A_r$ be non-Abelian simple groups, and let N be a normal subgroup of $A_1 \times \cdots \times A_r$.

- Consider first the case where, for some $i \in \{1, \dots, n\}$,

$$\begin{aligned} N &\subset A_1 \times \cdots \times A_{i-1} \times \{e\} \times A_{i+1} \cdots \times A_r \\ &\simeq A_1 \times \cdots \times A_{i-1} \times A_{i+1} \cdots \times A_r, \end{aligned}$$

where the isomorphism is the map $(a_1, \dots, a_{i-1}, e, a_{i+1}, \dots, a_r) \mapsto (a_1, \dots, a_{i-1}, a_{i+1}, \dots, a_r)$. This isomorphism sends N on a normal subgroup N'.

$A_1 \times A_{i-1} \times A_{i+1} \cdots \times A_r$ is a direct product of $r-1$ simple non-Abelian subgroups, thus we can apply the induction hypothesis: its only normal subgroups are standard subgroups, thus N' is standard. This implies, via the isomorphism, that

$$N = H_1 \times \cdots H_{i-1} \times \{e\} \times H_{i+1} \times \cdots \times H_r, \text{ where } H_j = \{e\} \text{ or } H_j = A_j \text{ for all } j.$$

Therefore N is standard in this case.

- In the remaining case, $N \not\subset A_1 \times \cdots \times A_{i-1} \times \{e\} \times A_{i+1} \times \cdots \times A_r$ for all $i = 1, \dots, r$. We want to prove that N is the whole group G.

- First, we prove that there is some $n = (n_1, \dots, n_r) \in N$ such that $a_i \ne e$ for all $i,\ 1 \le i \le r$.

Fix some $i \in \{1, \dots, r\}$. Since $N \not\subset A_1 \times \cdots \times A_{i-1} \times \{e\} \times A_{i+1} \times \cdots \times A_r$, there exists some $n_i = (a_1, \dots, a_i, \dots, a_r) \in N$ such that $a_i \ne e$.

Since A_i is non-Abelian and simple, the centers Z_i of A_i are different from A_i, and Z_i is normal in the simple group A_i, thus $Z_i = \{e\}$. Using $a_i \ne e$, this shows that there is some $c \in A_i$ such that $a_i c \ne c a_i$. Now take $a = (e, \dots, e, c, e, \dots, e) \in G$. Since N is normal, $n_i(a n_i^{-1} a^{-1}) \in N$, and

$$\begin{aligned} n_i a n_i^{-1} a^{-1} &= (a_1, \dots, a_i, \dots, a_r)(a, \dots, c, \dots, e)(a_1^{-1}, \dots, a_i^{-1}, \dots, a_r^{-1})(e, \dots, b^{-1}, \dots, e) \\ &= (e, \dots, a_i c a_i^{-1} c^{-1}, \dots, e), \end{aligned}$$

thus $n_i a n_i^{-1} a^{-1} = (e, \dots, n_i, \dots, e) \in N$, where $n_i = a_i c a_i^{-1} c^{-1} \ne e$. Since we can find such $n_i \ne e$ for each index i,

$$n = (n_1, \dots, n_r) = (n_1, e, \dots, e)(e, n_2, \dots, e) \cdots (e, \dots, n_r) \in N, \text{ where } n_1 \ne e, \dots, n_r \ne e.$$

- Write $b = n_r$. N is normal in G, thus, for any $a = (a_1, \dots, a_{r-1}, e) \in A_1 \times \cdots \times A_r$,

$$\begin{aligned} n(a n^{-1} a^{-1}) &= (n_1, \dots, n_{r-1}, b)(a_1, \dots, a_{r-1}, e)(n_1^{-1}, \dots, n_{r-1}^{-1}, b^{-1})(a_1^{-1}, \dots, a_{r-1}^{-1}, e) \\ &= (n_1 a_1 n_1^{-1} a_1^{-1}, \dots, n_{r-1} a_{r-1} n_{r-1}^{-1} a_{r-1}^{-1}, e) \in N \end{aligned}$$

Since $Z_i = \{e\}$, we can find $(a_1, \dots, a_{r-1}, e) \in A$ such that $n_i a_i n_i^{-1} a_i^{-1} \ne e$ for every $i, 1 \le i \le r-1$.

Write for simplicity $A = A_1 \times \cdots \times A_{r-1}, B = A_r$, and $e_A = (e, \dots, e)$ the identity of A.

By the induction hypothesis, $N \cap (A \times \{e\})$ is a direct product of trivial subgroups $H_i \subset A_i$:

$$N \cap (A \times \{e\}) = H_1 \times \cdots \times H_{r-1} \times \{e\}, \quad H_i = \{e\} \text{ or } H_i = A_i,\ i = 1, \dots, r-1,$$

Since

$$n a n^{-1} a^{-1} = (n_1 a_1 n_1^{-1} a_1^{-1}, \dots, n_{r-1} a_{r-1} n_{r-1}^{-1} a_{r-1}^{-1}, e) \in N \cap (A \times \{e\}) = H_1 \times \cdots \times H_{r-1} \times \{e\},$$

every H_i contains an element $n_i a_i n_i^{-1} a_i^{-1} \neq e$, thus $H_i = A_i$ for all i, $1 \leq i \leq r-1$. This proves that

$$N \cap (A \times \{e\}) = A \times \{e\},$$

thus $A_1 \times \cdots \times A_{r-1} \times \{e\} \subset N$.

With the same reasoning, $\{e\} \times A_2 \times \cdots \times A_r \subset N$.

- If $a = (a_1, \ldots, a_r)$ is any element of $A_1 \times \cdots \times A_r$, then

$$a = (a_1, \ldots, a_{r-1}, e)(e, \ldots, e, a_r),$$

where $(a_1, \ldots, a_{r-1}, e) \in A_1 \times \cdots A_{r-1} \times \{e\} \subset N$, and $(e, \ldots, e, a_r) \in \{e\} \times A_2 \times \cdots \times A_r \subset N$. Therefore $a \in N$.

This proves $N = A \times B = A_1 \times \cdots \times A_r \times A_{r+1}$: for every normal subgroup N of G such that there is some $n = (n_1, \ldots, n_r) \in N$ where $n_i \neq e$ for all i, N is the whole group G. In this case, N is also standard, and the induction is done.

To conclude, if $A_1, \ldots, A_r$ are non-Abelian simple groups, the only normal subgroups of $A_1 \times \cdots \times A_r$ are the subgroups

$$N = H_1 \times \cdots \times H_r, \text{ where } H_i = \{e_{A_i}\} \text{ or } H_i = A_i \text{ for all } i \in \{1, \ldots, r\}.$$

□

Ex. 14.3.19 *Let $G \subset S_n$ be transitive, and let G_i be the isotropy subgroup of $i \in \{1, \ldots, n\}$. Thus $G_i = \{\sigma \in G \mid \sigma(i) = i\}$.*

(a) Prove that G is doubly transitive if and only if G_i acts transitively on $\{1, \ldots, n\} \setminus \{i\}$.

(b) More generally, let $k \geq 2$. Prove that G is k-transitive if and only if G_i acts $(k-1)$-transitively on $\{1, \ldots, n\} \setminus \{i\}$.

Proof.

(a) Suppose that G is doubly transitive. If $j, k \in \{1, \ldots, n\} \setminus \{i\}$, as $i \neq j, i \neq k$, there exists $\sigma \in G$ such that $\sigma(i) = i, \sigma(j) = k$, so that $\sigma \in G_i$ and $\sigma(j) = k$. This proves that G_i acts transitively on $\{1, \ldots, n\} \setminus \{i\}$.

Conversely, suppose that G_i acts transitively on $\{1, \ldots, n\} \setminus \{i\}$ for some $i \in \{1, \ldots, n\}$. We first show that $G_{i'}$ acts also transitively on $\{1, \ldots, n\} \setminus \{i'\}$ for all $i' \in \{1, \ldots, n\}$.

First, since G is transitive, there is some $\tau \in G$ such that $\tau(i) = i'$.

Let $j', k' \in \{1, \ldots, n\} \setminus \{i'\}$, and define $j = \tau^{-1}(j'), k = \tau^{-1}(k')$. Then $j \neq i, k \neq i$, otherwise $j' = i'$ or $k' = i'$. Then the hypothesis gives $\sigma \in G_i$ such that $\sigma(j) = k$, that is $\sigma(\tau^{-1}(j')) = \tau^{-1}(k')$.

Therefore

$$(\tau\sigma\tau^{-1})(i') = i'$$
$$(\tau\sigma\tau^{-1})(j') = k',$$

which shows that $\sigma' = \tau\sigma\tau^{-1} \in G_{i'}$ satisfies $\sigma'(j') = k'$, thus $G_{i'}$ acts transitively on $\{1, \ldots, n\} \setminus \{i'\}$, and this is true for all i'.

Now we prove that G is doubly transitive. Let $(r, s), (r', s'), r \neq s, r' \neq s'$ be pairs of distinct elements of $\{1, \ldots, n\}$. Since G_r acts transitively on $\{1, \ldots, n\} \setminus \{r\}$, and $r \neq s$, there exists $\sigma_1 \in G_r$ such that $\sigma_1(r) = r, \sigma_1(s) = s'$. Note that $r \neq s'$, otherwise $\sigma_1(r) = \sigma_1(s), r \neq s$, which is impossible since σ_1 is a permutation. Thus there exists $\sigma_2 \in G_{s'}$ such that $\sigma_2(r) = r', \sigma_2(s') = s'$, where $r' \neq s'$. Then $\sigma = \sigma_2\sigma_1$ satisfies $\sigma(r) = r', \sigma(s) = s'$. This proves that G is doubly transitive.

(b) Suppose first that G is k transitive, and let $(i_1,\dots,i_{k-1}),(j_1,\dots,j_{k-1})$ be any $(k-1)$-tuples of distinct elements of $\{1,\dots,n\}\setminus\{i\}$. Then $(i,i_1,\dots,i_{k-1}),(i,j_1,\dots,j_{k-1})$ are k-tuples of distinct elements of $\{1,\dots,n\}$, thus there is some $\sigma\in G$ such that $\sigma\cdot(i,i,i_1,\dots,i_{k-1})=(i,j_1,\dots,j_{k-1})$, so that $\sigma\in G_i$ and $\sigma(i_1)=j_1,\dots,\sigma(i_{k-1})=j_{k-1}$. This proves that G_i acts $(k-1)$-transitively on $\{1,\dots,n\}\setminus\{i\}$.

Conversely, suppose that G_i acts $(k-1)$-transitively on $\{1,\dots,n\}\setminus\{i\}$ for some $i\in\{1,\dots,n\}$. As in part (a), we first show that $G_{i'}$ acts $(k-1)$-transitively on $\{1,\dots,n\}\setminus\{i'\}$ for all $i'\in\{1,\dots,n\}$, using a permutation $\tau\in G$ satisfying $\tau(i)=i'$. Take $(i'_1,\dots,i'_{k-1}),(j'_1,\dots,j'_{k-1})$ two $(k-1)$-tuples of distinct elements in $\{1,\dots,n\}\setminus\{i'\}$. We define $i_l=\tau^{-1}(i'_l),j_l=\tau^{-1}(j'_l),\ l=1,\dots,k-1$. Since τ^{-1} is a permutation, $(i,i_1,\dots,i_{k-1})$ and $(i,j_1,\dots,j_{k-1})$ are k-tuples of distinct elements. The hypothesis gives $\sigma\in G_i$ such that $\sigma(i_l)=j_l,\ l=1,\dots,k-1$. Then $\sigma'=\tau\sigma\tau^{-1}$ satisfies

$$(\tau\sigma\tau^{-1})(i'_l)=j'_l,\ l=1,\dots,k-1,\ \text{and } \sigma'(i')=i'.$$

Therefore $G_{i'}$ acts $(k-1)$-transitively on $\{1,\dots,n\}\setminus\{i'\}$, for all $i'\in\{1,\dots,n\}$.

Now let $(r_1,\dots,r_k),(s_1,\dots,s_k)$ be any k-tuples of distinct elements. There exists $\sigma_1\in G_{r_k}$ such that

$$\sigma_1\cdot(r_1,\dots,r_{k-1},r_k)=(s_1,\dots,s_{k-1},r_k),$$

where $s_1,\dots,s_{k-1},r_k$ are distinct, since $r_k=s_i$ for some $i\neq k$ implies $\sigma_1^{-1}(r_k)=\sigma_1^{-1}(s_i)$, that is $r_k=r_i$, which is false. Thus there exists $\sigma_2\in G_{s_1}$ such that

$$\sigma_2\cdot(s_1,s_2,\dots,s_{k-1},r_k)=(s_1,s_2,\dots,s_{k-1},s_k).$$

Then $\sigma=\sigma_2\sigma_1$ satisfies $\sigma\cdot(r_1,\dots,r_k)=(s_1,\dots,s_k)$. This proves that G is k-transitive. □

Ex. 14.3.20 *Let $G\subset S_n$ be doubly transitive. Proposition 14.3.3 implies that G is transitive. Prove that G is transitive directly from the definition of doubly transitive.*

Proof. If $n=1$,then $G=\{e\}$ is transitive. Suppose now that $n\geq 2$, and that $G\subset S_n$ is doubly transitive.

Let i,j be any elements in $\{1,\dots,n\}$. Since $n\geq 2$, there is some $i'\in\{1,\dots,n\}$ such that $i\neq i'$, and some j' such that $j\neq j'$. By definition of doubly transitive, there is $\sigma\in G$ such that $\sigma(i)=j$ and $\sigma(i')=j'$. We have proved

$$\forall i\in\{1,\dots,n\},\ \forall j\in\{1,\dots,n\},\ \exists\sigma\in G,\ \sigma(i)=j,$$

so that G is transitive. □

Ex. 14.3.21 *Generalize (14.15) by showing that we have inclusions*

$$\mathbb{F}_p^{mn}=\mathbb{F}_{p^m}^n\subset \mathrm{AGL}(n,\mathbb{F}_{p^m})\subset \mathrm{A\Gamma L}(n,\mathbb{F}_{p^m})\subset \mathrm{AGL}(nm,\mathbb{F}_p)\subset S_{p^{nm}}.$$

Proof. We write $q=p^m$.

- Let $\mathcal{B}=(e_1,\dots,e_m)$ 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

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

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 $\mathcal{B}$). So we can write

$$\mathbb{F}_p^{mn} = \mathbb{F}_{p^m}^n.$$

- $\mathbb{F}_{p^m}^n = \mathbb{F}_q^n$ is identified with $\{\gamma_{I_n,v} \mid v \in \mathbb{F}_q^n\} \subset \mathrm{AGL}(n, \mathbb{F}_q)$, via the isomorphism

$$\left\{ \begin{array}{ccc} \mathbb{F}_q^n & \to & \{\gamma_{I_n,v} \mid v \in \mathbb{F}_q^n\} \\ v & \mapsto & \gamma_{I_n,v}. \end{array} \right.$$

This shows that

$$\mathbb{F}_{p^m}^n \subset \mathrm{AGL}(n, \mathbb{F}_{p^m}).$$

- If $f = \gamma_{A,v}$ is any element of $\mathrm{AGL}(n, \mathbb{F}_q)$, then $f = \gamma_{A,e,v} \in \mathrm{A\Gamma L}(n, \mathbb{F}_q)$ (where e is the identity is S_q). Therefore

$$\mathrm{AGL}(n, \mathbb{F}_{p^m}) \subset \mathrm{A\Gamma L}(n, \mathbb{F}_{p^m}).$$

- By Exercise 3(c), we know that elements of $\mathrm{A\Gamma L}(n, \mathbb{F}_q)$ give maps $\mathbb{F}_q^n = \mathbb{F}_p^{nm} \to \mathbb{F}_q^n = \mathbb{F}_p^{nm}$ that are affine linear over $\mathbb{F}_p$, so that these elements are in $\mathrm{AGL}(nm, \mathbb{F}_p)$.

$$\mathrm{A\Gamma L}(n, \mathbb{F}_{p^m}) \subset \mathrm{AGL}(nm, \mathbb{F}_p).$$

- The elements of $\mathrm{AGL}(nm, \mathbb{F}_p)$ are bijective maps from $\mathbb{F}_p^{nm}$ to $\mathbb{F}_p^{nm}$, thus $\mathrm{AGL}(nm, \mathbb{F}_p) \subset S(\mathbb{F}_p^{nm})$.

  Via an arbitrary numbering of $\mathbb{F}_p^{nm}$, say $\gamma : \{1, \ldots, p^{nm}\} \to \mathbb{F}_p^{nm}$, we obtain the isomorphism $\psi : S(\mathbb{F}_p^{nm}) \to S_{nm}$ defined by $\psi(\sigma) = \gamma^{-1} \circ \sigma \circ \gamma$, which allows us to identify $S(\mathbb{F}_p^{nm}) \simeq S_{nm}$.

$$\mathrm{AGL}(nm, \mathbb{F}_p) \subset S_{p^{nm}}.$$

To conclude, using several improper non-canonical identifications, we write

$$\mathbb{F}_p^{mn} = \mathbb{F}_{p^m}^n \subset \mathrm{AGL}(n, \mathbb{F}_{p^m}) \subset \mathrm{A\Gamma L}(n, \mathbb{F}_{p^m}) \subset \mathrm{AGL}(nm, \mathbb{F}_p) \subset S_{p^{nm}}.$$

$\square$

Ex. 14.3.22 *Show that* $\mathrm{AGL}(n, \mathbb{F}_q)$ *is isomorphic to the subgroup*

$$\left\{ \begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix} \mid A \in \mathrm{GL}(n, \mathbb{F}_q), v \in \mathbb{F}_q^n \right\} \subset \mathrm{GL}(n+1, \mathbb{F}_q),$$

where $\begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix}$ *is the* $(n+1) \times (n+1)$ *matrix such that the upper left* $n \times n$ *corner is* A*, the first* n *entries of the last column are* v*, and the first* n *entries of the last row are all zero.*

Proof. Consider the map

$$\varphi \left\{ \begin{array}{ccc} \mathrm{AGL}(n, \mathbb{F}_q) & \to & \mathrm{GL}(n+1, \mathbb{F}_q) \\ \gamma_{A,v} & \mapsto & \begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix} \end{array} \right.$$

This map is well defined, since $\gamma_{A,v} = \gamma_{B,w} \Rightarrow (A, v) = (B, w)$. We verify first that φ is an injective group homomorphism. Since (see (1) in Exercise 2)

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

(see (1) in Exercise 2), we obtain

$$\begin{aligned}\varphi(\gamma_{A,v} \circ \gamma_{B,w}) &= \varphi(\gamma_{AB,Aw+v}) \\ &= \begin{pmatrix} AB & Aw+v \\ 0 & 1 \end{pmatrix}.\end{aligned}$$

Moreover,

$$\begin{aligned}\varphi(\gamma_{A,v})\varphi(\gamma_{B,w}) &= \begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix}\begin{pmatrix} B & w \\ 0 & 1 \end{pmatrix} \\ &= \begin{pmatrix} AB & Aw+v \\ 0 & 1 \end{pmatrix} \\ &= \varphi(\gamma_{A,v} \circ \gamma_{B,w}).\end{aligned}$$

φ is a group homomorphism, and if $\gamma_{A,v} \in \ker(\varphi)$ then

$$\begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} I_n & 0 \\ 0 & 1 \end{pmatrix},$$

Therefore $A = I_n, v = 0$, so that $\gamma_{A,v} = \gamma_{I_n,0} = 1_{F_q}$. We have proved that φ is an injective group homomorphism, thus

$$\mathrm{Im}\,(\varphi) = \left\{ \begin{pmatrix} A & v \\ 0 & 1 \end{pmatrix} \mid A \in \mathrm{GL}(n, \mathbb{F}_q), v \in \mathbb{F}_q^n \right\},$$

is a subgroup of $\mathrm{GL}(n+1, \mathbb{F}_q)$ isomorphic to $\mathrm{AGL}(n, \mathbb{F}_q)$. $\square$

Ex. 14.3.23 *Use Theorem 14.3.21 to show that* $\mathrm{AGL}(2, \mathbb{F}_p)$ *is not solvable for* $p > 3$.

Proof. Let p be a prime such that $p > 3$. By Theorem 14.3.21, we know that $\mathrm{PSL}(2, \mathbb{F}_p)$ is simple, and non-Abelian, therefore $\mathrm{PSL}(2, \mathbb{F}_p)$ is not solvable.

Since

$$\mathrm{PSL}(2, \mathbb{F}_p) \subset \mathrm{PGL}(2, \mathbb{F}_p),$$

$\mathrm{PGL}(2, \mathbb{F}_p)$ is not solvable.

Moreover,

$$\mathrm{PGL}(2, \mathbb{F}_p) = \mathrm{GL}(2, \mathbb{F}_p)/\mathbb{F}_p^* I_n.$$

Since $\mathbb{F}_p^* I_n$ is cyclic, therefore solvable, $\mathrm{GL}(2, \mathbb{F}_p)$ is not solvable.

But $\mathrm{AGL}(2, \mathbb{F}_p)$ contains the subgroup $\{\gamma_{A,0} \mid A \in \mathrm{GL}(2, \mathbb{F}_p)\} \simeq \mathrm{GL}(2, \mathbb{F}_p)$.

This proves that $\mathrm{AGL}(2, \mathbb{F}_p)$ is not solvable if $p > 3$. $\square$

Ex. 14.3.24 *The action of* $\mathrm{PGL}(2, F)$ *on* $\hat{F} = F \cup \{\infty\}$ *was introduced in Section 7.5 In particular, Exercise 11 of that section implies that the isotropy subgroup of* $\mathrm{PGL}(2, F)$ *at the point* ∞ *can be identified with* $\mathrm{AGL}(1, F)$. *Use part (c) of Exercise 4 and Exercise 19 to prove that the action of* $\mathrm{PGL}(2, F)$ *on* $\hat{F}$ *is 3-transitive (also called triply transitive).*

Proof. By Exercise 4 (c), $\mathrm{GL}(2, F)$ acts transitively on $F^2 \setminus \{0\}$. This proves that $\mathrm{PGL}(2, F)$ acts transitively on the projective line $\mathbb{P}_1(F)$, so that the action of $\mathrm{PGL}(2, F)$ on $\hat{F}$ is transitive.

This allows us to apply Exercise 19 (b). To prove that the action of $\mathrm{PGL}(2, F)$ on $\hat{F}$ is triply transitive, it is sufficient to prove that the isotropy group $G_\infty = \mathrm{AGL}(1, F)$ acts 2-transitively on $\hat{F} \setminus \{\infty\} = F$. Example 14.3.2 shows that this is true. Therefore the action of $\mathrm{PGL}(2, F)$ on $\hat{F}$ is 3-transitive. $\square$

Ex. 14.3.25 *Prove that* $\mathrm{AGL}(1,\mathbb{F}_4) \simeq A_4$ *and* $\mathrm{A\Gamma L}(1,\mathbb{F}_4) \simeq S_4$.

Proof. $\mathrm{AGL}(1,\mathbb{F}_4)$ acts on $\mathbb{F}_4$, via the action defined by

$$\gamma_{a,b} \cdot i = \gamma_{a,b}(i) = ai + b,$$

where $a \in \mathbb{F}_4^*, b \in \mathbb{F}_4$.

Since $\gamma_{a,b}$ is bijective, $\mathrm{AGL}(1,\mathbb{F}_4) \subset S(\mathbb{F}_4) \simeq S_4$.

Moreover, $|\mathrm{AGL}(1,\mathbb{F}_4)| = 3 \times 4 = 12$, and the only subgroup with 12 elements of S_4 is A_4. Therefore

$$\mathrm{AGL}(1,\mathbb{F}_4) \simeq A_4.$$

Similarly, $\mathrm{A\Gamma L}(1,\mathbb{F}_4)$ acts on $\mathbb{F}_4$, via the action defined by

$$\gamma_{a,\sigma,b} \cdot i = \gamma_{a,\sigma,b}(i) = a\sigma(i) + b,$$

where $a \in \mathbb{F}_4^*, b \in F_4, \sigma \in \mathrm{Gal}(F_4/F_2) = \{e, F\}$, F being the Frobenius isomorphism $i \mapsto i^2$.

Since $\gamma_{a,\sigma,b}$ is bijective, $\mathrm{AGL}(1,\mathbb{F}_4) \subset S(\mathbb{F}_4) \simeq S_4$.

By Exercise 3(a), $\mathrm{AGL}(2,\mathbb{F}_4)$ is a subgroup of $\mathrm{A\Gamma L}(2,\mathbb{F}_4)$ of index 2, therefore $|\mathrm{A\Gamma L}(2,\mathbb{F}_4)| = 24$. This proves that $\mathrm{A\Gamma L}(2,\mathbb{F}_4) = S(\mathbb{F}_4)$, thus

$$\mathrm{AGL}(2,\mathbb{F}_4) \simeq S_4.$$

□

Ex. 14.3.26 *Compute the orders of the groups in (14.15).*

$$(14.15) \qquad \mathbb{F}_p^2 = \mathbb{F}_{p^2} \subset \mathrm{AGL}(1,\mathbb{F}_{p^2}) \subset \mathrm{A\Gamma L}(1,\mathbb{F}_{p^2}) \subset \mathrm{AGL}(2,\mathbb{F}_p) \subset S_{p^2}.$$

Proof.

- $|\mathbb{F}_p^2| = |\mathbb{F}_{p^2}| = p^2$.
- Every element of $\mathrm{AGL}(1,\mathbb{F}_{p^2})$ is of the unique form $\gamma_{a,b},\ a \in \mathbb{F}_{p^2}^*, b \in \mathbb{F}_{p^2}$, thus

$$|\mathrm{AGL}(1,\mathbb{F}_{p^2})| = p^2(p^2 - 1).$$

- By Exercise 3(a), $\mathrm{AGL}(1,\mathbb{F}_{p^2})$ has index 2 in $\mathrm{A\Gamma L}(1,\mathbb{F}_{p^2})$, therefore

$$|\mathrm{A\Gamma L}(1,\mathbb{F}_{p^2})| = 2p^2(p^2 - 1).$$

- Every element of $\mathrm{AGL}(2,\mathbb{F}_p)$ is of the unique form $\gamma_{A,v},\ A \in \mathrm{GL}(2,\mathbb{F}_p), v \in \mathbb{F}_p^2$. Moreover, by Exercise 14(a), $|\mathrm{GL}(2,\mathbb{F}_p)| = p(p-1)(p^2-1)$, therefore

$$|\mathrm{AGL}(2,\mathbb{F}_p)| = p^3(p-1)(p^2-1).$$

- To be complete, $|S_{p^2}| = (p^2)!$. □

14.4 PRIMITIVE POLYNOMIALS OF PRIME-SQUARED DEGREE

Ex. 14.4.1 *Prove that $M_1 = \mathrm{A\Gamma L}(1, \mathbb{F}_{p^2})$ is solvable, and compute its order.*

Proof. Recall that $\mathrm{AGL}(1, \mathbb{F}_{p^2})/\mathbb{F}_p \simeq \mathbb{F}_p^*$, where $(\mathbb{F}_p, +)$ and $(\mathbb{F}_p^*, \times)$ are cyclic, thus solvable, hence $\mathrm{AGL}(1, \mathbb{F}_{p^2})$ is solvable by Theorem 8.1.4.

By Exercise 14.3.3(a), $\mathrm{AGL}(1, \mathbb{F}_{p^2})$ has index 2 in $\mathrm{A\Gamma L}(1, \mathbb{F}_{p^2})$, therefore $\mathrm{AGL}(1, \mathbb{F}_{p^2})$ is a normal subgroup of $\mathrm{AGL}(1, \mathbb{F}_{p^2})$, and

$$\mathrm{A\Gamma L}(1, \mathbb{F}_{p^2})/\mathrm{AGL}(1, \mathbb{F}_{p^2}) \simeq \{-1, 1\}.$$

The group $\{-1, 1\}$ is cyclic, of prime order 2, therefore is solvable, and $\mathrm{AGL}(1, \mathbb{F}_{p^2})$ is solvable. The same Theorem 8.1.4 shows that $M_1 = \mathrm{A\Gamma L}(1, \mathbb{F}_{p^2})$ is solvable.

By Exercise 14.3.26,

$$|M_1| = 2p^2(p^2 - 1).$$

$\square$

Ex. 14.4.2 *This exercise will study the subgroup $M_2 \subset \mathrm{AGL}(2, \mathbb{F}_p)$ defined in (14.21).*

(a) *Prove that the map δ defined in (14.2) gives an element of $\mathrm{AGL}(2, \mathbb{F}_p)$.*

(b) *Prove that $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ has order 2 and normalizes $\mathrm{AGL}(1, \mathbb{F}_p) \times \mathrm{AGL}(1, \mathbb{F}_p) \subset \mathrm{AGL}(2, \mathbb{F}_p)$.*

(c) *Prove that M_2 is solvable, and compute its order.*

(d) *Prove that $(M_2)_0$ is generated by the matrices in (14.22).*

(e) *Prove that $\mathrm{AGL}(1, \mathbb{F}_p) \times \mathrm{AGL}(1, \mathbb{F}_p) \subset \mathrm{AGL}(2, \mathbb{F}_p)$ is imprimitive in S_{p^2}.*

Proof.

(a) Write $\gamma = \gamma_{a,b}, \gamma' = \gamma_{a',b'}$, where $a, a' \in \mathbb{F}_p^*,\ b, b \in \mathbb{F}_p$.
Then

$$\delta(\alpha, \beta) = (a\alpha + b, a'\beta + b'), \qquad \text{for all } (\alpha, \beta) \in \mathbb{F}_p^2.$$

Since

$$\begin{pmatrix} a\alpha + b \\ a'\beta + b' \end{pmatrix} = \begin{pmatrix} a & 0 \\ 0 & a' \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \end{pmatrix} + \begin{pmatrix} b \\ b' \end{pmatrix},$$

$\delta = \gamma_{A,v} \in \mathrm{AGL}(2, \mathbb{F}_p)$, where $A = \begin{pmatrix} a & 0 \\ 0 & a' \end{pmatrix} \in \mathrm{GL}(2, \mathbb{F}_p)$ (since $\det(A) = aa' \neq 0$), and $v = (b, b') \in \mathbb{F}_p^2$.

(b) $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = I_2$, thus $B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ has order 2, and is identified with the element $\gamma_{B,0} \in \mathrm{AGL}(2, \mathbb{F}_p)$.

Let $\delta = \gamma_{A,v}$ be any element of $\mathrm{AGL}(1, \mathbb{F}_p) \times \mathrm{AGL}(1, \mathbb{F}_p)$. With the same notations as in part (a), using (1),

$$\begin{aligned} \gamma_{B,0} \circ \delta \circ \gamma_{B,0}^{-1} &= \gamma_{B,0} \circ \gamma_{A,v} \circ \gamma_{B,0} \\ &= \gamma_{B,0} \circ \gamma_{AB,v} \\ &= \gamma_{BAB,Bv} \end{aligned}$$

where

$$BAB = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a' \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} a' & 0 \\ 0 & a \end{pmatrix}$$

normalize is diagonal, therefore $\gamma_{B,0} \circ \delta \circ \gamma_{B,0}^{-1} \in \mathrm{AGL}(1, \mathbb{F}_p) \times \mathrm{AGL}(1, \mathbb{F}_p)$. This proves that B normalizes $\mathrm{AGL}(1, \mathbb{F}_p) \times \mathrm{AGL}(1, \mathbb{F}_p)$:

$$B\,(\mathrm{AGL}(1, \mathbb{F}_p) \times \mathrm{AGL}(1, \mathbb{F}_p))\,B^{-1} = \mathrm{AGL}(1, \mathbb{F}_p) \times \mathrm{AGL}(1, \mathbb{F}_p).$$

(c) Since M_2 is the subgroup of $\mathrm{AGL}(2, \mathbb{F}_p)$ generated by $\mathrm{AGL}(1, \mathbb{F}_p) \times \mathrm{AGL}(1, \mathbb{F}_p)$ and B, part (b) shows that $H = \mathrm{AGL}(1, \mathbb{F}_p) \times \mathrm{AGL}(1, \mathbb{F}_p)$ is a normal subgroup of M_2.

Note that, if $A \in H$, $AB = B(BAB) = BA'$, where $A' = BAB = BAB^{-1} \in H$. Therefore every element of M_2 is of the form A or BA, where $A \in H$. This proves that $M_2 = H \cup (B \cdot H)$, so that the group homomorphism

$$\pi \left\{ \begin{array}{ccc} \{I_2, B\} & \to & M_2/H \\ I_2 & \mapsto & H \\ B & \mapsto & B \cdot H \end{array} \right.$$

is surjective. Since $B \notin H, B \cdot H \neq H$, thus $\ker(\pi) = \{I_2\}$. This proves that π is an isomorphism, and

$$M_2/(\mathrm{AGL}(1, \mathbb{F}_p) \times \mathrm{AGL}(1, \mathbb{F}_p)) \simeq \{I_2, B\}.$$

This gives $|M_2| = 2|\mathrm{AGL}(1, \mathbb{F}_p)|^2$, so

$$|M_2| = 2p^2(p-1)^2.$$

Since $(\mathrm{AGL}(1, \mathbb{F}_p) \times \mathrm{AGL}(1, \mathbb{F}_p))/\mathrm{AGL}(1, \mathbb{F}_p) \simeq \mathrm{AGL}(1, \mathbb{F}_p)$, where $\mathrm{AGL}(1, \mathbb{F}_p)$ is solvable, the group $\mathrm{AGL}(1, \mathbb{F}_p) \times \mathrm{AGL}(1, \mathbb{F}_p)$ is solvable.

The group $\{I_2, B\}$ is cyclic, therefore solvable. By Theorem 8.1.4, the isomoprphism $M_2/(\mathrm{AGL}(1, \mathbb{F}_p) \times \mathrm{AGL}(1, \mathbb{F}_p)) \simeq \{I_2, B\}$ shows that M_2 is solvable.

(d) Note that $\delta \in H$ defined by $\delta(\alpha, \beta) = (\lambda\alpha + b, \mu\beta + b')$ fixes 0 if and only if $b = b' = 0$. Therefore $H \cap (M_2)_0$ is generated by the matrices $\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$, $\lambda, \mu \in \mathbb{F}_p^*$.

By part (c), $M_2 = H \cup (B \cdot H)$, and $B \in (M_2)_0$, therefore $(M_2)_0 \subset \mathrm{GL}(2, \mathbb{F}_p)$ is generated by the matrices

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}, \ \lambda, \mu \in \mathbb{F}_p^*.$$

(e) If H is the smaller subgroup $\mathrm{AGL}(1, \mathbb{F}_p) \times \mathrm{AGL}(1, \mathbb{F}_p)$, then the isotropy group H_0 is generated by the matrices $\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$, $\lambda, \mu \in \mathbb{F}_p^*$, therefore is the subgroup of diagonal matrices in $\mathrm{GL}(2, \mathbb{F}_p)$.

We prove that H_0 is not irreducible. The nontrivial subspace $V = \mathbb{F}_p \times \{0\} \subset \mathbb{F}_p^2$ is such that $h(V) \subset V$ for all $h = \begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} \in H_0$: For all $(\gamma, 0) \in V$,

$$\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix} \begin{pmatrix} \gamma \\ 0 \end{pmatrix} = \begin{pmatrix} \lambda\gamma \\ 0 \end{pmatrix} \in V.$$

□

Ex. 14.4.3 *Let M_1 and M_2 be the subgroups defined in the text, and assume that $p > 3$. Prove that M_2 is not doubly transitive and not isomorphic to a subgroup of M_1.*

Proof. By Theorem 14.3.4, if $M_2 \subset S_{p^2}$ was doubly transitive, then

$$p^2(p^2-1) \mid |M_2| = 2p^2(p-1)^2.$$

Then $p+1 \mid 2(p-1)$, thus $p+1 \mid 2(p+1) - 2(p-1) = 4$, where p is prime. The only solution is $p = 3$. We can conclude:

If $p > 3$, then M_2 is not doubly transitive.

If M_2 was isomorphic to a subgroup of M_1, then, by Lagrange's Theorem,

$$\frac{|M_1|}{|M_2|} = \frac{p+1}{p-1} \in \mathbb{Z}.$$

In this case, $p-1 \mid p+1$, therefore $p-1 \mid (p+1)-(p-1) = 2$, which is only possible if $p = 2$ or $p = 3$. Here $p > 3$, so we can conclude:

If $p > 3$, then M_2 is not isomorphic to a subgroup of M_1.

□

Ex. 14.4.4 *Let V be a vector space of dimension 2 over a field F, and let $T : V \to V$ be a linear map that is not a multiple of the identity. Also assume that T is an isomorphism. Prove that there is $v \in V$ such that v and $T(v)$ form a basis of V over F.*

Proof. Consider a basis $\mathcal{B} = (e, f)$ of V.

Reasoning by contradiction, suppose that for all $v \in V$, the vectors $v, T(v)$ are linearly dependent. Then, since $e \neq 0, f \neq 0, e + f \neq 0$, there are some $\lambda, \mu, \nu \in F$ such that

$$T(e) = \lambda e, \qquad T(f) = \mu f, \qquad T(e+f) = \nu(e+f).$$

Since T is linear,

$$\nu e + \nu f = T(e+f) = T(e) + T(f) = \lambda e + \mu f;$$

But (e, f) is a basis, therefore $\lambda = \mu = \nu$, so that the matrix of T in the basis $\mathcal{B}$ is $\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} = \lambda I_2$, and T would be a multiple of the identity, which is in contradiction with the hypothesis.

This proves that there is some $v \in V$ such that $v, T(v)$ are linearly independent. Since the dimension of V is 2, v and $T(v)$ form a basis of V over F. □

Note: The hypothesis "T is an isomorphism" was useless.

Ex. 14.4.5 *Fix $a \in \mathbb{F}_p, p > 2$. The goal of this exercise is to find $s, t \in \mathbb{F}_p$ with $s^2 + t^2 = a$.*

(a) Let $S = \{s^2 \mid s \in \mathbb{F}_p\}$. Prove that $|S| = (p+1)/2$.

(b) Let $S' = \{a - s^2 \mid s \in \mathbb{F}_p\}$. Show that $S \cap S' \neq \varnothing$, and use this to prove the existence of $s, t \in \mathbb{F}_p$ such that $s^2 + t^2 = a$.

Proof.

(a) Consider the map

$$\varphi \left\{ \begin{array}{ccc} \mathbb{F}_p^* & \to & \mathbb{F}_p^* \\ s & \mapsto & s^2. \end{array} \right.$$

For all $s, t \in \mathbb{F}_p^*$, $\varphi(st) = (st)^2 = s^2t^2 = \varphi(s)\varphi(t)$, thus φ is a group homomorphism.

Not that, $\mathrm{Im}\,(\varphi) = \{s^2 \mid s \in \mathbb{F}_p^*\} = S \setminus \{0\}$. Moreover $s \in \ker(\varphi)$ iff $s^2 = 1$, that is $(s-1)(s+1) = 0$. Since $\mathbb{F}_p$ is a field, this is equivalent to $s = 1$ or $s = -1$, thus $\ker(\varphi) = \{-1, 1\}$, where $-1 \neq 1$ since $p > 2$. By the first Isomorphism Theorem,

$$\mathbb{F}_p^*/\{-1, 1\} \simeq \{s^2 \mid s \in \mathbb{F}_p^*\} = S \setminus \{0\}.$$

This shows that there are $(p-1)/2$ squares in $\mathbb{F}_p^*$. If we add the square $0 = 0^2$, we obtain

$$|S| = \frac{p+1}{2}.$$

(b) The two maps $u, t_a : \mathbb{F}_p \to \mathbb{F}_p$ defined for all $s \in \mathbb{F}_p$ by $u(s) = -s$, and $t_a(s) = a + s$ are bijective (since $u \circ u = 1_{\mathbb{F}_p}$ and $t_a \circ t_{-a} = t_{-a} \circ t_a = 1_{\mathbb{F}_p}$). Therefore

$$f = t_a \circ u \left\{ \begin{array}{ccc} \mathbb{F}_p & \to & \mathbb{F}_p \\ s & \mapsto & a - s^2 \end{array} \right.$$

is bijective.

Since $S' = \{f(s) \mid s \in \mathbb{F}_p\} = f(S)$,

$$|S'| = |S| = \frac{p+1}{2}.$$

Reasoning by contradiction, if $S \cap S' = \varnothing$, then the inclusion $S \cup S' \subset \mathbb{F}_p$ shows that

$$p + 1 = |S| + |S'| = |S \cup S'| \leq |\mathbb{F}_p| = p,$$

and $p + 1 \leq p$ gives a contradiction. Therefore $S \cap S' \neq \varnothing$, so that we can find some $c \in \mathbb{F}_p$ such that $c \in S \cap S'$. Such an element c verifies $c = s^2$ and $c = a - t^2$ for some $s, t \in \mathbb{F}_p$. This proves that the equation $s^2 + t^2 = a$ has a solution $(s, t) \in \mathbb{F}_p \times \mathbb{F}_p$. $\square$

Ex. 14.4.6 *Let $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ be a 2×2 matrix with entries in a field F.*

(a) Prove that the characteristic polynomial of A is $P(x) = x^2 - \mathrm{tr}(A)x + \det(A)$, where $\mathrm{tr}(A) = a + d$ and $\det(A) = ad - bc$ are the trace and determinant of A.

(b) Prove that $P(A) = A^2 - \mathrm{tr}(A)A + \det(A)I_2$ is the zero matrix.

The Cayley-Hamilton Theorem generalizes part (b) by showing that $P(A)$ is the zero matrix when $P(x)$ is the characteristic polynomial of an $n \times n$ matrix A.

Proof.

(a) By definition of the characteristic polynomial,

$$\begin{aligned} P(x) &= \begin{vmatrix} a-x & b \\ c & d-x \end{vmatrix} \\ &= (a-x)(d-x) - bc \\ &= x^2 - (a+d)x + ad - bc \\ &= x^2 - \operatorname{tr}(A)x + \det(A). \end{aligned}$$

(b) Moreover,

$$\begin{aligned} P(A) &= A^2 - \operatorname{tr}(A)A + \det(A)I_2 \\ &= \begin{pmatrix} a & b \\ c & d \end{pmatrix}^2 - (a+d)\begin{pmatrix} a & b \\ c & d \end{pmatrix} + (ad-bc)I_2 \\ &= \begin{pmatrix} a^2+bc & ab+bd \\ ca+dc & cb+d^2 \end{pmatrix} + \begin{pmatrix} -a^2-da & -ab-db \\ -ac-dc & -ad-d^2 \end{pmatrix} + \begin{pmatrix} ad-bc & 0 \\ 0 & ad-bc \end{pmatrix} \\ &= 0. \end{aligned}$$

□

Ex. 14.4.7 *Complete the proof of $C(H) = H$ from Proposition 14.4.4 begun in the text.*

Proof. Recall the context:

Here $g, h \in \mathrm{GL}(2, \mathbb{F}_p)$ are such that

$$gh = -hg, g^2 = h^2 = -I_2, \det(g) = \det(h) = 1. \tag{10}$$

$$H = \langle [g], [h] \rangle = \{[I_2], [g], [h], [g][h]\rangle \subset \mathrm{PGL}(2, \mathbb{F}_p).$$

By (14.23),

$$[m] \in C(H) \iff \left\{ \begin{array}{ll} [m][g] & = [g][m] \\ [m][h] & = [h][m] \end{array} \right. \iff \left\{ \begin{array}{ll} mg & = \pm gm \\ mh & = \pm hm. \end{array} \right.$$

Let $[m] \in C(H)$. There are four cases.

- If $mg = gm, mh = hm$, then by Lemma 14.4.3,

$$m = aI_2 + bg = cI_2 + dh, \qquad a, b, c, d \in \mathbb{F}_p.$$

If $b \neq 0$, then $g = b^{-1}(c-a)I_2 + b^{-1}dh) \in \mathrm{Vect}(I_2, h)$, thus $gh = hg$. This is impossible since $gh = -hg \neq 0$ and $p > 2$. Thus $b = 0$, and $m = aI_2$, so that $[m] = [I_2] \in H$.

- If $mg = -gm, mh = hm$, then

$$\begin{aligned} &(mh)g = m(hg) = m(-gh) = (-mg)h = (gm)h = g(mh) \\ &(mh)h = (hm)h = h(mh), \end{aligned}$$

thus mh is in the centralizer of g and h. By the first bullet, $[mh] = [I_2]$, and using $[h]^2 = [I_2]$, we obtain $[m] = [h] \in H$.

- If $mg = gm, mh = -hm$, exchanging g and h in the previous case, we obtain similarly $[m] = [g] \in H$.
- If $mg = -gm, mh = -hm$, then, using (10),

$$(mgh)g = mg(hg) = mg(-gh) = m(-g^2)h = mh,$$
$$g(mgh) = (gm)(gh) = (-mg)gh = m(-g^2)h = mh,$$

$$(mgh)h = mg(h^2) = -mg,$$
$$h(mgh) = (hm)(gh) = (-mh)(-hg) = mh^2g = -mg.$$

Therefore mgh commutes with g and h. By the first bullet, $[mgh] = [I_2]$, thus $[mg] = [-(mgh)h] = [-h]$, and $[m] = [-mg^2] = [mg][-g] = [-h][-g] = [h][g] = [g][h] \in H$.

We have proved $C(H) \subset H$. Since H is Abelian $H \subset C(H)$. Thus $C(H) = H$. $\square$

Ex. 14.4.8 *Let G be a group with a normal subgroup $H \simeq (\mathbb{Z}/2\mathbb{Z})^2$ such that $C_G(H) = H$ and the map $G \to \mathrm{Aut}(H)$ given by conjugation is onto. The goal of this exercise is to prove that $G \simeq S_4$. Note that $|G| = 24$ by the proof of Proposition 14.4.4.*

(a) Use the Sylow Theorems to show that G has one or four 3-Sylow subgroups. Then use $C_G(H) = H$ to show that the number is four.

(b) Let H_1 be a 3-Sylow subgroup of G. Use part (a) and the Sylow Theorem to show that its normalizer has order 6.

(c) Now consider the homomorphism $\phi : G \to S_4$ given by the action of G by conjugation on the 3-Sylow subgroups. Use part (b) to prove that $\ker(\phi)$ cannot contain an element of order 3.

(d) Conclude that the image of ϕ contains A_4. It follows that if ϕ is not an isomorphism, then G contains a normal subgroup of order 2.

(e) Prove that G cannot contain a normal subgroup of order 2. Thus $\phi : G \simeq S_4$.

This exercise is closely related to Exercise 3 of Section 14.2.

Proof. First, we try to understand the first sentence, and why this is related to the proof of Proposition 14.4.4.

Note that every permutation of $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ fixing $(0,0)$ is an outer automorphism (the Cayley tables are identical if we exchange the two elements of any pair of nonzero elements). Since $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is Abelian, there is no non trivial inner automorphism. Thus $\mathrm{Aut}(H) \simeq S_3$.

In the proof of Proposition 14.4.4, if we write $G = N(H) = N_{\mathrm{PGL}(2,\mathbb{F}_p)}(H)$, then we proved that

$$\varphi \left\{ \begin{array}{ccc} G & \to & \mathrm{Aut}(H) \simeq S_3 \\ g & \mapsto & \varphi_g \left\{ \begin{array}{ccc} H & \to & H \\ g & \mapsto & ghg^{-1} \end{array} \right. \end{array} \right.$$

is surjective (onto). Note that φ is well defined because H is a normal subgroup of G, so $ghg^{-1} \subset H$ for all $g \in G$ and for all $h \in H$.

By hypothesis, φ is surjective. As in the text, $\ker(\varphi) = C_G(H) = H$, thus

$$S_3 \simeq \mathrm{Aut}(H) \simeq G/\ker(\varphi) = G/H.$$

This proves $|G| = |H| \times |S_3| = 4 \times 6 = 24$.

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

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

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

If $N = 1$, then there is only one 3-Sylow subgroup, say K. Since gKg^{-1} is also a 3-Sylow subgroup, $gKg^{-1} = K$, so K is normal in G.

Since $|K| = 3$ and $|H| = 4$, then $|H \cap K|$ divides 4 and 3, thus $H \cap K = \{e\}$.

By Exercise 14.3.7, knowing that H, K are normal in G, and that $H \cap K = \{e\}$, then HK is a normal subgroup of G, and $HK \simeq H \times K$. Moreover H and K are Abelian subgroups, thus $HK \simeq H \times K$ is abelian. This shows that $K \subset C_G(H)$, thus $H = C_G(H) \supset HK \supsetneq H$. This is a contradiction.

We have proved that G has four 3-Sylow subgroups.

(b) Let H_1, H_2, H_3, H_4 be the 3-Sylow subgroup of G. For all $g \in G$, gH_ig^{-1} is a 3-Sylow of G, thus G acts on the set $\{H_1, H_2, H_3, H_4\}$.

By the second Sylow Theorem, all 3-Sylow subgroups are conjugate, thus G acts transitively on $\{H_1, H_2, H_3, H_4\}$, thus the orbit of H_1 is

$$\mathcal{O}_{H_1} = \{H_1, H_2, H_3, H_4\}.$$

By definition of the normalizer, the isotropy group of H_1 is $G_{H_1} = N_G(H_1)$. The Fundamental Theorem of Group Actions gives

$$4 = |\mathcal{O}_{H_1}| = (G : N_G(H_1)),$$

thus $|N_G(H_1)| = |G|/4 = 6$.

(c) Write $E = \{H_1, H_2, H_3, H_4\}$. Consider the homomorphism

$$\psi \left\{ \begin{array}{ccc} G & \to & S(E) \simeq S_4 \\ g & \mapsto & \psi_g \left\{ \begin{array}{ccc} E & \to & E \\ M & \mapsto & gMg^{-1}. \end{array} \right. \end{array} \right.$$

$(M = H_i,\ i = 1, 2, 3, 4)$.

Reasoning by contradiction, suppose that $\ker(\psi)$ contains an element h of order 3.

For all $g \in G$, $g \in \ker(\psi)$ if and only if ψ_g is the identity of $S(E)$, thus

$$\ker(\psi) = N_G(H_1) \cap N_G(H_2) \cap N_G(H_3) \cap N_G(H_3).$$

Therefore $\{e, h, h^2\}$ is a subgroup of $N_G(H_1)$. But $H_1 \subset N_G(H_1)$ is another subgroup of $N_G(H_1)$ of order 3.

Since $N_G(H_1) = 6$, $N_G(H_1)$ has a unique subgroup of order 3: the number n of 3-Sylow subgroups of $N_G(H_1)$ satisfies $n \mid 6, n \equiv 1 \pmod 3$, thus $n = 1$. Therefore $H_1 = \{e, h, h^2\}$. Reasoning with $H_2 \subset N_G(H_2)$, we obtain similarly $H_2 = \{e, h, h^2\}$. Thus $H_1 = H_2$. This is a contradiction since the 3-Sylow subgroups H_1, H_2, H_3, H_4 are distinct. Therefore $\ker(\psi)$ cannot contain an element of order 3.

(d) By part (b), $\ker(\psi)$ is a subgroup of the group $N_G(H_1)$, whose order is 6. By part (c), $\ker(\psi)$ has no element of order 3, hence the order of $\ker(\psi)$ is not 3 or 6, otherwise, by Cauchy Theorem, $\ker(\psi)$ would contain an element of order 3. Thus the order of $\ker(\phi)$ is 1 or 2. This implies that

$$|\operatorname{Im}(\psi)| = |G|/|\ker(\psi)| = 12 \text{ or } 24.$$

If we choose some numbering γ of E, where $\gamma : \{1,2,3,4\} \to E$ is given by $\gamma(i) = H_i$, then $\hat{\gamma} : S(E) \to S_4$ defined by $\hat{\gamma}(\sigma) = \gamma^{-1} \circ \sigma \circ \gamma$ is an isomorphism. Thus $\phi = \hat{\gamma} \circ \psi$, $\phi : G \to S_4$, is a group homomorphism, such that $|\operatorname{Im}(\phi)| = |\operatorname{Im}(\psi)| = 12$ or 24. Since S_4 has only one subgroup of order 12, we obtain that

$$\operatorname{Im}(\phi) = A_4 \text{ or } \operatorname{Im}(\phi) = S_4.$$

We have proved $\operatorname{Im}(\phi) \supset A_4$.

If $\operatorname{Im}(\phi) = S_4$, then $\phi : G \to S_4$ is surjective, and since $|G| = |S_4|$, ϕ is bijective, thus ϕ is a group isomorphism and $G \simeq S_4$.

It follows that if ϕ is not an isomorphism, then $\operatorname{Im}(\phi) = A_4$, and $|\ker(\varphi)| = 2$. Then $K = \ker(\varphi)$ is a normal subgroup of G of order 2.

(e) It remains to show that G cannot contain a normal subgroup K of order 2. Reasoning by contradiction, suppose that there exists such a subgroup K. Write $K = \{e, a\}, a \neq e$.

Since K is normal in G, for every $g \in G$, $gag^{-1} \in K = \{e, a\}$, and $gag^{-1} \neq e$, otherwise $a = e$. Thus $gag^{-1} = a$.

$$\forall g \in G, \ ga = ag.$$

This means that a in in the center of G, a fortiori, $a \in C_G(H)$. Since $C_G(H) = H$, it follows that

$$K \subset H.$$

Write $H = \{e, a, b, c\}$.

Consider anew the homomorphism $\varphi : G \to \operatorname{Aut}(H) \simeq S_3$ described in the introduction. By hypothesis, φ is surjective. But for all $g \in G$, $\varphi_g(a) = gag^{-1} = a$, thus any automorphism χ of G such that $\chi(a) \neq a$, for instance the automorphism defined by $\chi(e) = e, \chi(a) = b, \chi(b) = c, \chi(c) = a$, is not in $\operatorname{Im}(\phi)$, in contradiction with the surjectivity of φ.

This proves that G has no normal subgroup of order 2. By part (d), it follows that $S(E) \simeq S_4$. □

Ex. 14.4.9 *Let g and $C(g)$ be as in the proof of part (c) of Proposition 14.4.4.*

(a) Show that $C(g)$ is Abelian and contains $\mathbb{F}_p^* I_2$.

(b) If $m \in C(g)$, then it is easy to see that $\det(m)m^{-2} \in C(g)$. By part (a), it follows that $\phi(m) = \det(m)m^{-2}$ defines a group homomorphism $\phi : C(g) \to C(g)$. Prove that $\ker(\phi) = \mathbb{F}_p^* I_2$ and $|\operatorname{Im}(\phi)| = |C(g)|/(p-1)$.

(c) Prove that $\operatorname{Im}(\phi) \subset \{w \in C(g) \mid \det(w) = 1\}$.

(d) Explain why we may assume that $g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Then use Lemma 14.4.3 and Exercise 5 to show that $\det : C(g) \to \mathbb{F}_p^*$ is onto. Conclude that

$$\operatorname{Im}(\phi) = \{w \in C(g) \mid \det(w) = 1\}.$$

The equality proved in part (d) shows that every element of $C(g)$ of determinant 1 is of the form $\det(m)m^{-2}$ for some $m \in C(g)$. This will be used in the proof of part (c) of Proposition 14.4.4.

Proof.

(a) Since $g^2 = -I_2$, $g \in \mathrm{GL}(2, \mathbb{F}_p)$, and since $gh = -hg \neq hg (p > 2)$, $g \notin \mathbb{F}_p^* I_2$. Then Lemma 14.4.3 shows that

$$C(g) = \{m \in \mathrm{GL}(2, \mathbb{F}_p) \mid \exists a \in \mathbb{F}_p,\ \exists b \in \mathbb{F}_p,\ m = aI_2 + bg\} = \mathrm{GL}(2, \mathbb{F}_p) \cap \mathrm{Vect}_{\mathbb{F}_p}(I_2, g).$$

if $m, m' \in C(g)$, then $m = aI_2 + bg, m' = a'I_2 + b'g,\ a, b, a, b,' \in F_p$, thus

$$mm' = (aI_2 + bg)(a'I_2 + b'g) = aa'I_2 + ba'g + ab'g + bb'g^2 = (a'I_2 + b'g)(aI_2 + bg),$$

so $C(g)$ is Abelian.

Moreover, $C(g)$ contains the matrices $aI_2 \in \mathrm{GL}(2, \mathbb{F}_p)$, which is equivalent to $a \in \mathbb{F}_p^*$.

$$C(g) \supset \mathbb{F}_p^* I_2.$$

(b) If $m \in C(g)$, then $m^2 g = gm^2$, thus $gm^{-2} = m^{-2} g$ and $(\det(m)m^{-2})g = g(\det(m)m^{-2})$, so that $\det(m)m^{-2} \in C(g)$. This permits us to define

$$\phi \left\{ \begin{array}{ccc} C(g) & \to & C(g) \\ m & \mapsto & \det(m)m^{-2}. \end{array} \right.$$

For $m, m' \in C(g)$, $\phi(mm') = (\det(mm')(mm')^{-2} = (\det(m)m^{-2})(\det(m')m'^{-2})$, thus ϕ is a group homomorphism.

If $m = \lambda I_2, \lambda \in \mathbb{F}_p^*$, then $\phi(m) = \lambda^2 (\lambda I_2)^{-2} = I_2$. Therefore $\mathbb{F}_p^* I_2 \subset \ker(\phi)$.

Conversely, if $m \in \ker(\phi)$, $\det(m)m^{-2} = I_2$, thus $m^2 = \mu I_2$, where $\mu = \det(m) \in \mathbb{F}_p^*$.

Reasoning by contradiction, suppose that $m \notin \mathbb{F}_p^* I_2$. Since $m \in C(g)$, Lemma 14.4.3 shows that $m = aI_2 + bg$, where $b \neq 0$.

Then $(aI_2 + bg)^2 = \mu I_2$, which gives, using $g^2 = -I_2$,

$$(a^2 - b^2 - \mu)I_2 + 2abg = 0.$$

If $a \neq 0$, then $g = -(2ab)^{-1}(a^2 - b^2 - \mu)I_2 \in \mathbb{F}_p^* I_2$, which is false. Therefore $a = 0$, and $m = bg$. Then

$$\begin{aligned} I_2 = \phi(m) &= \det(bg)(bg)^{-2} \\ &= \det(g)g^{-2}, \end{aligned}$$

thus $-I_2 = g^2 = \det(g)I^2$, and $\det(g) = -1$, which contradicts $\det(g) = 1$ $(p > 2)$. This contradiction shows that $m \in \mathbb{F}_p^* I_2$. To conclude,

$$\ker(\phi) = \mathbb{F}_p^* I_2.$$

Since $\mathrm{Im}\,(\phi) \simeq C(g)/\ker(\phi) = C(g)/\mathbb{F}_p^* I_2$,

$$|\,\mathrm{Im}\,(\phi)| = |C(g)|/(p-1).$$

(c) If $w \in \mathrm{Im}\,(\phi)$, then $w = \det(m)m^{-2}$ for some $m \in C(g)$. Then

$$\det(w) = \det(m)^2 \det(m)^{-2} = 1,$$

thus

$$\mathrm{Im}\,(\phi) \subset \{w \in C(g) \mid \det(w) = 1\}.$$

(d) In the proof of part (c) of Proposition 14.4.4, we saw that there is some $Q \in \mathrm{GL}(2, \mathbb{F}_p)$ such that

$$g' = Q^{-1} g Q = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Note that

$$C(g') = Q^{-1} C(g) Q.$$

Indeed, if $m \in C(g)$, then $mg = gm$, thus

$$\begin{aligned} (Q^{-1} m Q) g' &= (Q^{-1} m Q)(Q^{-1} g Q) \\ &= Q^{-1} m g Q = Q^{-1} g m Q \\ &= (Q^{-1} g Q)(Q^{-1} m Q) \\ &= g'(Q^{-1} m Q). \end{aligned}$$

This proves $Q^{-1} C(g) Q \subset C(g')$. Symmetrically, $Q C(g') Q^{-1} \subset C(g)$, thus $C(g') = Q^{-1} C(g) Q$.

Let $\phi' : C(g') \to C(g')$ the group homomorphism defined by $\phi'(m') = \det(m') m'^{-2}$. Suppose that we can prove that $\mathrm{Im}\,(\phi') = \{w' \in C(g') \mid \det(w') = 1\}$. Now, take $w \in C(g)$ such that $\det(w) = 1$. Since $C(g) = Q C(g') Q^{-1}$, there is some $w' \in C(g')$ such that

$$w = Q w' Q^{-1}, \qquad w' \in C(g'), \det(w') = 1.$$

By our hypothesis, $w' \in \mathrm{Im}\,(\phi')$, so that $w' = \det(m') m'^2, m' \in C(g')$.

Put $m = Q m' Q^{-1}$. Then $m \in C(g)$, and

$$\begin{aligned} w &= Q w' Q^{-1} \\ &= \det(Q m' Q^{-1})(Q m' Q^{-1})^2 \\ &= \det(m) m^2 \\ &= \phi(m) \end{aligned}$$

This proves that $\mathrm{Im}\,(\phi) = \{w \in C(g) \mid \det(w) = 1\}$, if we can show first that $\mathrm{Im}\,(\phi') = \{w' \in C(g') \mid \det(w') = 1\}$. This explain why we may assume now that $g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

For all $a, b \in \mathbb{F}_p$,

$$\det(a I_2 + b g) = \begin{vmatrix} a & -b \\ b & a \end{vmatrix} = a^2 + b^2.$$

By Exercise 5, for all $\lambda \in \mathbb{F}_p$, there is some pair $(a, b) \in \mathbb{F}_p^2$ such that $a^2 + b^2 = \lambda$. If $\lambda \in \mathbb{F}_p^*$, then $\det(aI + bg) = \lambda \neq 0$, thus $a I_2 + b g \in \mathrm{GL}(2, \mathbb{F}_p)$. Moreover $a I_2 + b g \in C(g)$ (this is the easy part of Lemma 14.4.3), thus $\det : C(g) \to \mathbb{F}_p^*$ is a surjective homomorphism.

For any $w \in \mathrm{GL}(2, \mathbb{F}_p)$,

$$\begin{aligned} w \in C(g) &\iff \begin{pmatrix} r & t \\ s & u \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} r & t \\ s & u \end{pmatrix} \\ &\iff \begin{pmatrix} t & -r \\ u & -s \end{pmatrix} = \begin{pmatrix} -s & -u \\ r & t \end{pmatrix} \\ &\iff \begin{cases} t &= -s, \\ u &= r. \end{cases} \end{aligned}$$

Thus

$$C(g) = \left\{ w \in \mathrm{GL}(2, \mathbb{F}_p) \mid \exists r \in \mathbb{F}_p,\ \exists s \in \mathbb{F}_p,\ w = \begin{pmatrix} r & -s \\ s & r \end{pmatrix} \right\}.$$

Now take any $w = \begin{pmatrix} r & t \\ s & u \end{pmatrix} \in C(g)$ such that $\det(w) = 1$.

Then $w = \begin{pmatrix} r & -s \\ s & r \end{pmatrix}$, $r^2 + s^2 = 1$, and $w^{-1} = \begin{pmatrix} r & s \\ -s & r \end{pmatrix}$.

Put $m = \begin{pmatrix} 1+r & s \\ -s & 1+r \end{pmatrix}$ (we found this matrix by trigonometrical analogy). By the previous remark, $m \in C(g)$, and $\det(m) = (1+r)^2 + s^2 = 2(1+r)$.

Then, using $r^2 + s^2 = 1$,

$$\begin{aligned} m^2 &= \begin{pmatrix} 1+r & s \\ -s & 1+r \end{pmatrix} \begin{pmatrix} 1+r & s \\ -s & 1+r \end{pmatrix} \\ &= \begin{pmatrix} (1+r)^2 - s^2 & 2s(1+r) \\ -2s(1+r) & (1+r)^2 - s^2 \end{pmatrix} \\ &= \begin{pmatrix} 2r^2 + 2r & 2s(1+r) \\ -2s(1+r) & 2r^2 + 2r \end{pmatrix} \\ &= 2(1+r) \begin{pmatrix} r & s \\ -s & r \end{pmatrix} \\ &= \det(m) w^{-1} \end{aligned}$$

Thus $w = \det(m) m^{-2} = \phi(m)$, where $m = \begin{pmatrix} 1+r & s \\ -s & 1+r \end{pmatrix} \in C(g)$.

(We have not used with this method the surjectivity of $\det : C(g) \to \mathbb{F}_p^*$.)

We can conclude, using also part (c),

$$\mathrm{Im}\,(\phi) = \{w \in C(g) \mid \det(w) = 1\}.$$

(for $g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, and by the above remark, for any $g \in \mathrm{GL}(2, \mathbb{F}_p)$ such that $g^2 = -I_2$.)

This equality shows that every element of $C(g)$ of determinant 1 is of the form $\det(m) m^{-2}$ for some $m \in C(g)$. $\square$

Ex. 14.4.10 *Consider the subgroup $N(H) \subset \mathrm{PGL}(2, \mathbb{F}_p)$ defined in Proposition 14.4.4.*

(a) Prove that the images of the matrices (14.25) generate $N(H)$ when $p \equiv 1 \pmod 4$.

(b) Prove that generators of H and the images of the matrices

$$\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \text{ and } \begin{pmatrix} s & t+1 \\ t-1 & -s \end{pmatrix}$$

from [17, p.163] generate $N(H)$ when $p \equiv 3 \pmod 4$.

Proof.

(a) In this part, $p \equiv 1 \pmod 4$. Then $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = 1$, therefore there exists some element $i \in \mathbb{F}_p$ such that $i^2 = 1$.

By Proposition 14.4.4, $H \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is given, up to conjugacy, by

$$H = \langle [g], [h] \rangle = \{[I_2], [g], [h], [k]\},$$

where

$$g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad h = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \qquad k = gh = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

since $s = i, t = 0$ is a solution of the equation $s^2 + t^2 = -1$.

Then $N(H)$ is the normalizer of H in $\mathrm{PGL}(2, \mathbb{F}_p)$. Write

$$a = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \qquad b = \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix}, \qquad c = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}.$$

We verify first that $\langle [a], [b], [c] \rangle \subset N(H)$.

$$\begin{aligned}
aga^{-1} &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = -g, \\
aha^{-1} &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -i & 0 \\ 0 & i \end{pmatrix} = -h, \\
bgb^{-1} &= \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} = -k, \\
bhb^{-1} &= \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} = h, \\
cgc^{-1} &= \frac{1}{2} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = g, \\
chc^{-1} &= \frac{1}{2} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = k.
\end{aligned}$$

Therefore

$$\begin{array}{lll}
[a][g][a]^{-1} = [g], & [a][h][a]^{-1} = [h], & (\Rightarrow [a][k][a]^{-1} = [k]), \\
[b][g][b]^{-1} = [k], & [b][h][b]^{-1} = [h], & (\Rightarrow [b][k][b]^{-1} = [g]), \\
[c][g][c]^{-1} = [g], & [c][h][c]^{-1} = [k], & (\Rightarrow [c][k][c]^{-1} = [h]).
\end{array}$$

Since $g, h, k \in H$, we have proved $\langle [a], [b], [c] \rangle \subset N(H)$.

Note that $H \subset K = \langle [a], [b], [c] \rangle$:

$[k] = [ia] = [a] \in H$, thus $[b][g][b]^{-1} = [k] = [a]$, so that

$$\begin{aligned}
[g] &= [b]^{-1}[a][b] \in K, \\
[h] &= [g]^{-1}[gh] = [b]^{-1}[a]^{-1}[b][a] \in K.
\end{aligned}$$

This proves

$$H = \langle g, h \rangle \subset K = \langle a, b, c \rangle.$$

Consider the action of $K = \langle [a], [b], [c] \rangle \subset N(H)$ on $H \setminus \{[I_2]\}$ by conjugation. This gives a group homomorphism

$$\varphi \left\{ \begin{array}{ccc} \langle [a], [b], [c] \rangle & \to & S(\{[g], [h], [k]\} \simeq S_3 \\ m & \mapsto & \varphi_m \left\{ \begin{array}{ccc} \{[g], [h], [k]\} & \to & \{[g], [h], [k]\} \\ x & \mapsto & mxm^{-1}. \end{array} \right. \end{array} \right.$$

- φ is surjective: $\varphi_{[b]}$ is the transposition $(g\,k)$, and $\varphi_{[c]}$ is the transposition $(h\,k)$. Since S_3 is generated by any pair of distinct transpositions, $S(\{[g], [h], [k]\} = \langle (g\,k), (h\,k) \rangle$. This proves that φ is surjective.

- Since H is Abelian, the elements of H fix $[g],[h],[k]$ by conjugation, therefore $H \subset \ker(\varphi)$. To prove the converse, we note that $\ker(\varphi) \subset C(H) = H$, because every element of $\ker(\varphi)$ fixes $[I_2],[g],[h],[k]$, thus is in $C(H)$, which is H (Proposition 14.4.4).

$$\ker(\varphi) = H.$$

Therefore $S_3 \simeq \mathrm{Im}\,(\varphi) \simeq K/\ker(\varphi) = K/H$. This gives

$$|\langle [a],[b],[c]\rangle| = |K| = |S_3||H| = 6 \times 4 = 24.$$

Since $\langle [a],[b],[c]\rangle \subset N(H)$, and $|\langle [a],[b],[c]\rangle| = 24 = |N(H)|$, we obtain

$$N(H) = \left\langle \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} i & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix} \right\rangle.$$

If we replace our g and h by any pair g, h satisfying the conditions of Proposition 14.4.4, then $N(H)$ is a conjugate subgroup of $K = \langle [a],[b],[c]\rangle$ by part (c) of this Proposition.

(b) In this part, $p \equiv 3 \pmod 4$. There is no element i of order 4, but by Proposition 14.1.4, there exist $s, t \in \mathbb{F}_p$ such that

$$H = \langle [g],[h]\rangle,$$

where

$$g = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad h = \begin{pmatrix} s & t \\ t & -s \end{pmatrix}, \qquad s^2 + t^2 = -1,$$

and

$$k = gh = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} s & t \\ t & -s \end{pmatrix} = \begin{pmatrix} -t & s \\ s & t \end{pmatrix}.$$

Write

$$c = \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \qquad d = \begin{pmatrix} s & t-1 \\ t+1 & -s \end{pmatrix}.$$

Put $K = \langle [g],[h],[c],[d]\rangle$. We want to show that $N(H) = K = \langle [g],[h],[c],[d]\rangle$.

We know that $H \subset N(H)$, so $[g],[h] \in N(H)$. It remains to verify that $[c],[d] \in N(H)$.

$$\begin{aligned}
cgc^{-1} &= \frac{1}{2}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = g, \\
chc^{-1} &= \frac{1}{2}\begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}\begin{pmatrix} s & t \\ t & -s \end{pmatrix}\begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} -t & s \\ s & t \end{pmatrix} = k, \\
dgd^{-1} &= \frac{1}{2}\begin{pmatrix} s & t-1 \\ t+1 & -s \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} -s & -t+1 \\ -t-1 & s \end{pmatrix} = \begin{pmatrix} s & t \\ t & -s \end{pmatrix} = h, \\
dhd^{-1} &= \frac{1}{2}\begin{pmatrix} s & t-1 \\ t+1 & -s \end{pmatrix}\begin{pmatrix} s & t \\ t & -s \end{pmatrix}\begin{pmatrix} -s & -t+1 \\ -t-1 & s \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = g.
\end{aligned}$$

Since $g, h, k \in H$, it follows that

$$\begin{aligned}
[c][g][c]^{-1} &= [g], \qquad [c][h][c]^{-1} = [k] \qquad (\Rightarrow [c][k][c]^{-1} = [h]), \\
[d][g][d]^{-1} &= [h], \qquad [d][h][d]^{-1} = [g] \qquad (\Rightarrow [d][k][d]^{-1} = [k]),
\end{aligned}$$

$$K = \langle [g],[h],[c],[d]\rangle \subset N(H).$$

As in part (a), consider the homomorphism

$$\phi \left\{ \begin{array}{ccc} \langle [g],[h],[c],[d]\rangle & \to & S(\{[g],[h],[k]\} \simeq S_3 \\ m & \mapsto & \phi_m \left\{ \begin{array}{ccc} \{[g],[h],[k]\} & \to & \{[g],[h],[k]\} \\ x & \mapsto & mxm^{-1}. \end{array} \right. \end{array} \right.$$

Then $\phi_{[c]}$ is the transposition $(h\,k)$, and $\phi_{[d]}$ is the transposition $(g\,h)$. Since S_3 is generated by any pair of two distinct transpositions, $S([g],[h],[k]) = \langle (h\,k),(g\,h)\rangle$, thus ϕ is surjective. Since $H \subset K$, as in part (a), $\ker(\varphi) = H$.

Therefore $S_3 \simeq \mathrm{Im}\,(\varphi) \simeq K/\ker(\varphi) = K/H$. This gives

$$|\langle [g],[h],[c],[d]\rangle| = |K| = |S_3||H| = 6 \times 4 = 24.$$

Since $\langle [g],[h],[c],[d]\rangle \subset N(H)$, and $|\langle [g],[h],[c],[d]\rangle| = 24 = |N(H)|$, we obtain

$$N(H) = \left\langle \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} s & t \\ t & -s \end{pmatrix}, \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} s & t-1 \\ t+1 & -s \end{pmatrix} \right\rangle.$$

□

Ex. 14.4.11 *Let M_3 be as in Proposition 14.4.5. Show that M_3 is solvable of order $24p^2(p-1)$.*

Proof. By definition, $M_3 = \pi^{-1}(N(H))$, where

$$\pi \left\{ \begin{array}{ccc} \mathrm{AGL}(2,\mathbb{F}_p) & \to & \mathrm{PGL}(2,\mathbb{F}_p) \\ \gamma_{A,v} & \mapsto & [A]. \end{array} \right.$$

Consider the restriction (and co-restriction) of π, given by

$$\tilde{\pi} \left\{ \begin{array}{ccc} M_3 & \to & N(H) \\ \gamma_{A,v} & \mapsto & [A]. \end{array} \right.$$

Since $M_3 = \pi^{-1}(N(H))$, $\tilde{\pi}$ is surjective. Moreover, $\gamma_{A,v} \in \ker(\tilde{\pi})$ if and only if $[A] = [I_2]$, that is $A \in \mathbb{F}_p * I_2$, thus

$$\ker(\tilde{\pi}) = \{\gamma_{\lambda I_2, v} \mid \lambda \in \mathbb{F}_p^*, v \in \mathbb{F}_p^2\}.$$

We know that $\gamma_{A,v} = \gamma_{B,w} \Rightarrow A = B, v = w$, therefore the map

$$\psi \left\{ \begin{array}{ccc} \mathbb{F}_p^2 \times \mathbb{F}_p^* & \to & \ker(\tilde{\pi}) \\ (v,\lambda) & \mapsto & \gamma_{\lambda I_2, v} \end{array} \right.$$

is bijective. This gives

$$|\ker(\tilde{\pi})| = |\mathbb{F}_p^*| \times |\mathbb{F}_p^2| = (p-1)p^2\}.$$

The First Isomorphism Theorem gives

$$S_4 \simeq N(H) \simeq M_3/\ker(\tilde{\pi}),$$

therefore

$$|M_3| = 24p^2(p-1).$$

Moreover, if we give the structure of semidirect product to $\mathbb{F}_p^2 \times \mathbb{F}_p^*$, we see that

$$\psi \left\{ \begin{array}{ccc} \mathbb{F}_p^2 \rtimes \mathbb{F}_p^* & \to & \ker(\tilde{\pi}) \\ (v, \lambda) & \mapsto & \gamma_{\lambda I_2, v} \end{array} \right.$$

is a group isomorphism: By formula (1) in Ex. 14.3.2, we obtain

$$\gamma_{\lambda I_2, v} \circ \gamma_{\mu I_2, w} = \gamma_{\lambda\mu I_2, Aw+v}.$$

We have seen that ψ is bijective, and, following the formula (6.9) for the semidirect product,

$$(v, \lambda)(w, \mu) = (v + \lambda w, \lambda\mu).$$

Therefore

$$\begin{aligned} \psi^{-1}(\gamma_{\lambda I_2, v})\psi^{-1}(\gamma_{\mu I_2, w}) &= (v, \lambda)(w, \mu) \\ &= (v + \lambda w, \lambda\mu) \\ &= \psi^{-1}(\gamma_{\lambda\mu I_2, Aw+v}) \\ &= \psi^{-1}(\gamma_{\lambda I_2, v} \circ \gamma_{\mu I_2, w}). \end{aligned}$$

This proves that ψ is a group isomorphism, and $\ker(\tilde{\pi}) \simeq \mathbb{F}_p^2 \rtimes \mathbb{F}_p^*$.

By exercise 6.4.8, we know that $\mathbb{F}_p^2 \rtimes \mathbb{F}_p^*/\mathbb{F}_p^2 \times \{1\} \simeq \mathbb{F}_p^*$, where $\mathbb{F}_p^2 \times \{1\} \simeq \mathbb{F}_p^2$. Since $\mathbb{F}_p^*$ is cyclic, $\mathbb{F}_p^*$ is solvable, and $\mathbb{F}_p^2$ is also cyclic and solvable, Theorem 8.1.4 shows that the semidirect product $\mathbb{F}_p^2 \rtimes \mathbb{F}_p^*$ is solvable, thus $\ker(\tilde{\pi})$ is solvable.

We know that S_4 is solvable (Exercise 8.1.1), thus $N(H) \simeq S_4$ is solvable.

Using again Theorem 8.1.4 with $N(H) \simeq M_3/\ker(\tilde{\pi})$, we obtain that M_3 is solvable.

□