Exercises 8:

③ $\mu\sigma^2$: $\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 5 & 6 & 2 & 1 \end{pmatrix}$

$$\boxed{\mu\sigma^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 1 & 6 & 2 & 5 \end{pmatrix} = (1\ 3)(2\ 4\ 6\ 5)}$$

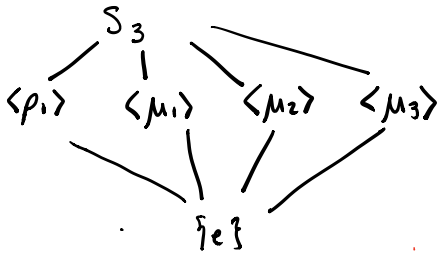
④ $\sigma^{-2}\tau$: $\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 3 & 4 & 5 \end{pmatrix}$, $\sigma^{-2} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 2 & 1 & 3 & 4 \end{pmatrix}$

$$\boxed{\sigma^2\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 1 & 6 & 2 & 4 & 3 \end{pmatrix} = (1\ 5\ 4\ 2)(3\ 6)}$$

⑦ $\tau^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 1 & 5 & 6 \end{pmatrix}$, $\tau^4 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = e \Rightarrow |\langle \tau^2 \rangle| = 2$

⑱ (a) $\langle \rho_1 \rangle = \{e, (1\,2\,3), (1\,3\,2)\} = \{e, \rho_1, \rho_2\}$ (Note: This is the alternating gp, A_3)
$\langle \rho_2 \rangle = \langle \rho_1 \rangle$
$\langle \mu_1 \rangle = \{e, (2\,3)\} = \{e, \mu_1\}$

(b)



⑩ $\{\sigma \in S_A \mid \sigma(b) = b\}$. Yes.
- closure: if $\sigma_1(b) = b$ & $\sigma_2(b) = b$, then $\sigma_1(\sigma_2(b)) = \sigma_1(b) = b$. ✓
- identity: the identity fixes b.
- inverses: if $\sigma(b) = b$, then $\sigma^{-1}(b) = \sigma^{-1}(\sigma(b)) = b$ ✓

⑬ $\{\sigma \in S_A \mid \sigma(B) = B\}$. Yes.
- closure: If $\sigma_1(B) = B$ & $\sigma_2(B) = B$, then $\sigma_1(\sigma_2(B)) = \sigma_1(B) = B$. ✓
- identity: the identity fixes every elt in B. ✓
- inverses: $\sigma(B) = B \Rightarrow \sigma^{-1}(\sigma(B)) = \sigma^{-1}(B) \Rightarrow B = \sigma^{-1}(B)$ ✓

⑯ For any $n \geq 3$, $(1\,2), (2\,3) \in S_n$.
$(1\,2)(2\,3) = (1\,2\,3)$ and $(2\,3)(1\,2) = (1\,3\,2)$. Since $(1\,2\,3) \neq (1\,3\,2)$, S_n is non-abelian.

⑰ Let $\sigma \in S_n$. We will construct a transposition that does not commute w/ σ whenever $\sigma \neq e$. Since $\sigma \neq e$, there is some $k \in \{1, \ldots, n\}$ s.t. $\sigma(k) \neq k$. Then $\exists\ l \in \{1, \ldots, n\}$ s.t. $\sigma(l) = k$, b/c σ is a permutation. Choose q to be any elt of $\{1, \ldots, n\}$ s.t. $q \neq l$ & $q \neq k$, and consider the transposition $(k\,q)$. Then since $l \neq k$ & $l \neq q$,
$(\sigma \cdot (k\,q))(l) = \sigma(l) = k$,

and $((kq)\circ\sigma)(\ell) = (kq)(k) = q \neq k$.

Thus $\sigma \not\in (k,q)$ do not commute, so σ doesn't commute w/ all elts of S_n. As such a transposition can be constructed for any $\sigma \neq e$, e is the only elt which commutes w/ all elts of S_n.

(49) Let A be a set, $A = \{a_1, a_2, \dots, a_k\}$, & let $\sigma = (a_1\ a_2 \cdots a_k)$. We will show that $|\langle\sigma\rangle| = k = |A|$.

Thinking of σ as a bijection $A \to A$, it is clear that $\sigma^k = id_A$, so $|\sigma| \leq k$. Moreover, $\sigma^m(a_i) = a_{i+m}$, where the subscript is considered mod k. Since $a_{i+m} \neq a_i$ $\forall$ $m < k$, it follows that $|\sigma| = k$. Thus $|\langle\sigma\rangle| = k = |A|$.

We will now show $\langle\sigma\rangle$ acts transitively on A. Let $a_i, a_j \in A$, & assume $j > i$. Then $\sigma^{j-i}(a_i) = a_{i+j-i} = a_j$. Since $\sigma^{j-i} \in \langle\sigma\rangle$, the result is proved.

Exercises 9:

(3) $(1\ 5\ 2)$, (3), $(4\ 6)$

(5) $\{\dots -3, -1, 1, 3, \dots\}$, $\{\dots, -2, 0, 2, 4, \dots\}$

(9) $(1\ 5\ 8)(2\ 4\ 7)$

(11) $(1\ 3\ 4)(2\ 6)(5\ 8\ 7) = (1\ 4)(1\ 3)(2\ 6)(5\ 7)(5\ 8)$

(12) $(1\ 3\ 4\ 7\ 8\ 6\ 5\ 2) = (1\ 2)(1\ 5)(1\ 6)(1\ 8)(1\ 7)(1\ 4)(1\ 3)$

(36) Let $a \in G$, $\lambda_a(g) = ag$. We need to show λ_a is a bijection.
- inj: Let $g_1, g_2 \in G$ s.t. $\lambda_a(g_1) = \lambda_a(g_2)$. Then $ag_1 = ag_2$, so by left cancellation, $g_1 = g_2$ ✓.
- surj: Let $g \in G$. Then $a^{-1}g \in G$, & $\lambda_a(a^{-1}g) = aa^{-1}g = g$ ✓.

Therefore, λ_a is a permutation of G.

(37) $H = \{\lambda_a \mid a \in G\}$.
- closure: let $\lambda_a, \lambda_b \in H$. Then for any $g \in G$, $\lambda_a \circ \lambda_b(g) = \lambda_a(\lambda_b(g)) = \lambda_a(bg) = abg = \lambda_{ab}(g)$. Since $ab \in G$, $\lambda_a\lambda_b = \lambda_{ab} \in H$.
- identity: $e \in G$, so $\lambda_e \in H$. For any $g \in G$, $\lambda_e(g) = eg = g$, so this is the identity permutation.
- inverses: let $\lambda_a \in H$. Then $a \in G$, so $a^{-1} \in G$ & $\lambda_{a^{-1}} \in H$. For any $g \in G$, $\lambda_a\lambda_{a^{-1}}(g) = \lambda_a(a^{-1}g) = aa^{-1}g = g = a^{-1}ag = \lambda_{a^{-1}}(\lambda_a(g)) = \lambda_{a^{-1}}\lambda_a(g)$, so $\lambda_{a^{-1}}$ is the inverse of λ_a.

Therefore H is a subgp of S_G.

Additional Exercises:

① Let O_n be the set of odd permutations in S_n, & define a map $\varphi: A_n \to O_n$ by $\varphi(\sigma) = \sigma(1\ 2)$. We will show φ is a bijection

- well-defined: Let $\sigma_1, \sigma_2 \in A_n$ s.t. $\sigma_1 = \sigma_2$. Then $\varphi(\sigma_1) = \sigma_1(12) = \sigma_2(12) = \varphi(\sigma_2)$.
- injective: Let $\sigma_1, \sigma_2 \in A_n$ s.t. $\varphi(\sigma_1) = \varphi(\sigma_2)$.
  Then $\sigma_1(12) = \sigma_2(12)$, so $\sigma_1(12)(12) = \sigma_2(12)(12) \Rightarrow \sigma_1 = \sigma_2$ (b/c $(12)(12) = e$).
- surjective: Let $\alpha \in O_n$. Then $\alpha = \tau_1\tau_2 \cdots \tau_{2k+1}$ for some k, τ_i a transp. Consider $\sigma = \alpha(12)$. Then $\sigma = \tau_1\tau_2 \cdots \tau_{2k+1}(12)$ can be written as the product of $2k+2$ transpositions, so $\alpha(12) \in A_n$. Moreover, $\varphi(\alpha(12)) = \alpha(12)(12) = \alpha$. ✓

Thus φ is a bijection, & so $|A_n| = |O_n|$. Since $A_n \cup O_n = S_n$ & $|S_n| = n!$, $|A_n| = n!/2$.

Note: we now know that O_n is a coset of A_n ($O_n = A_n(12)$), so they must have the same cardinality. Note that $|S_n : A_n| = 2$, i.e. there are only 2 right cosets of A_n: A_n & O_n.

② (a) Let $G = \langle a \rangle$ be an infinite cyclic group. Define a map $\varphi: \mathbb{Z} \to G$ defined by $\varphi(n) = a^n$. We will show φ is an isomorphism.
- well-def: let $n = m$. Then $a^n = a^m$ ✓.
- homomorphism: let $n, m \in \mathbb{Z}$. Then $\varphi(n+m) = a^{n+m} = a^n a^m = \varphi(n)\varphi(m)$ ✓
- inj: let $n, m \in \mathbb{Z}$ s.t. $\varphi(n) = \varphi(m)$. Then $a^n = a^m$. Since G is an infinite cyclic gp, this implies that $n = m$ (this is a thm in the book).
- surj: let $b \in G$. Then since G is cyclic, $b = a^k$ for some $k \in \mathbb{Z}$. Thus $\varphi(k) = a^k = b$.

Therefore φ is an isomorphism, & $G \cong \mathbb{Z}$.

(b) Let $G = \langle b \rangle$ be a cyclic gp of order n. Define a map $\varphi: \mathbb{Z}_n \to G$ defined by $\varphi(\overline{m}) = b^m$. We will show φ is an isom.
- well-def: let $\overline{m}, \overline{k} \in \mathbb{Z}_n$ s.t. $\overline{m} = \overline{k}$. Then $\exists q_1, q_2 \in \mathbb{Z}^+$ & $0 \le r < n$ s.t. $m = q_1 n + r$ & $k = q_2 n + r$.
  $\varphi(\overline{m}) = b^m = b^{q_1 n + r} = (b^n)^{q_1} \cdot b^r = e \cdot b^r = b^r$
  $\varphi(\overline{k}) = b^k = b^{q_2 n + r} = (b^n)^{q_2} \cdot b^r = e \cdot b^r = b^r$
  $\Rightarrow \varphi(\overline{m}) = \varphi(\overline{k})$.
- hom: let $\overline{m}, \overline{k} \in \mathbb{Z}_n$ as above. Then
  $\varphi(\overline{m} + \overline{k}) = \varphi(\overline{m+k}) = b^{m+k} = b^{q_1 n + r + q_2 n + r} = (b^n)^{q_1} b^r (b^n)^{q_2} b^r = e b^r e b^r = b^{2r}$.
  $\varphi(\overline{m})\varphi(\overline{k}) = b^m b^k = b^{q_1 n + r} b^{q_2 n + r} = (b^n)^{q_1} b^r (b^n)^{q_2} b^r = e b^r e b^r = b^{2r}$.
  Thus $\varphi(\overline{m} + \overline{k}) = \varphi(\overline{m})\varphi(\overline{k})$.
- inj: let $\overline{m}, \overline{k} \in \mathbb{Z}_n$ s.t. $\varphi(\overline{m}) = \varphi(\overline{k})$. Then $b^m = b^k$. Since G is a cyclic gp of order n, this $b^m = b^k \Leftrightarrow n$ divides $m-k$ (this is a thm we proved in class). This implies that m & k must have the same remainder when divided by n (because $m \equiv k \pmod n \Leftrightarrow m - k \equiv 0 \pmod n \Leftrightarrow n$ divides $m-k$), & therefore $\overline{m} = \overline{k}$.
- surj: let $c \in G$. Then $c = b^i$ for some $0 \le i < n$. Thus $\overline{i} \in \mathbb{Z}_n$, & $\varphi(\overline{i}) = b^i = c$.

Therefore, φ is an isomorphism & $G \cong \mathbb{Z}_n$.

③ • associative: let $g_1, g_2, g_3 \in G_1$ & $h_1, h_2, h_3 \in G_2$. Then

$$\begin{aligned}[(g_1,h_1)(g_2,h_2)](g_3,h_3) &= (g_1 * g_2, h_1 \star h_2)(g_3,h_3)\\ &= ((g_1 * g_2) * g_3, (h_1 \star h_2) \star h_3)\\ &= (g_1 * (g_2 * g_3), h_1 \star (h_2 \star h_3)) \quad \text{b/c } * \text{ \& } \star \text{ are}\\ &= (g_1,h_1)[(g_2,h_2)(g_3,h_3)]. \quad \text{associative.}\end{aligned}$$

• identity: let e_1, e_2 be the identity elts of G_1, G_2, respectively. Then $\forall g \in G_1 \; \forall h \in G_2$,

$$\begin{aligned}(g,h)(e_1,e_2) &= (g * e_1, h \star e_2)\\ &= (g, h)\\ &= (e_1 * g, e_2 \star h)\\ &= (e_1,e_2)(g,h),\end{aligned}$$

so $(e_1,e_2) \in G_1 \times G_2$ is the identity elt.

• inverses: let $(g,h) \in G_1 \times G_2$. Then $g \in G_1$ & $h \in G_2$. Then $\exists$ inverses $g^{-1} \in G_1$ & $h^{-1} \in G_2$. Thus

$$\begin{aligned}(g,h)(g^{-1},h^{-1}) = (g * g^{-1}, h \star h^{-1}) &= (e_1,e_2) = (g^{-1} * g, h^{-1} \star h)\\ &= (g^{-1},h^{-1})(g,h).\end{aligned}$$

Thus $(g^{-1},h^{-1}) \in G_1 \times G_2$ is the inverse of (g,h).

Therefore, $G_1 \times G_2$ is a group.

Exercises 11:

④ $|(\bar{0},\bar{0})| = 1$
$|(\bar{1},\bar{0})| = |(\bar{2},\bar{0})| = 3$
$|(\bar{1},\bar{1})| = |(\bar{1},\bar{3})| = |(\bar{2},\bar{1})| = |(\bar{2},\bar{3})| = 12$
$|(\bar{1},\bar{2})| = |(\bar{2},\bar{2})| = 6$
$|(\bar{0},\bar{1})| = |(\bar{0},\bar{3})| = 4$
$|(\bar{0},\bar{2})| = 2$

I calculated all of these using lcms. For example,

$$|(\bar{2},\bar{2})| = \operatorname{lcm}(|\bar{2}|,|\bar{2}|) = \operatorname{lcm}(3,2) = 6.$$

($\bar{2}$ has order 3 in $\mathbb{Z}_3$; $\bar{2}$ has order 2 in $\mathbb{Z}_4$)

④ $|(\bar{2},\bar{3})| = \operatorname{lcm}(|\bar{2}|,|\bar{3}|) = \operatorname{lcm}\left(\frac{6}{\gcd(2,6)}, \frac{15}{\gcd(3,15)}\right)$
$= \operatorname{lcm}(6/2, 15/3)$
$= \operatorname{lcm}(3,5)$
$= 15.$

⑥ $|(\bar{3},\bar{10},\bar{9})| = \operatorname{lcm}(|\bar{3}|,|\bar{10}|,|\bar{9}|)$
$= \operatorname{lcm}\left(\frac{4}{\gcd(3,4)}, \frac{12}{\gcd(10,12)}, \frac{15}{\gcd(9,15)}\right)$
$= \operatorname{lcm}\left(\frac{4}{1}, \frac{12}{2}, \frac{15}{3}\right)$
$= \operatorname{lcm}(4,6,5)$
$= 60$

⑧ if $\bar{a} \in \mathbb{Z}_6$, then $|\bar{a}| = 1, 2, 3,$ or 6
if $\bar{b} \in \mathbb{Z}_8$, then $|\bar{b}| = 1, 2, 4,$ or 8
The largest the $\text{lcm}(|\bar{a}|, |\bar{b}|)$ can be is 24, which is the order of $(\bar{1}, \bar{1})$.

if $\bar{c} \in \mathbb{Z}_{12}$, then $|\bar{c}| = 1, 2, 3, 4, 6,$ or 12.
if $\bar{d} \in \mathbb{Z}_{15}$, then $|\bar{d}| = 1, 2, 3, 5,$ or 15.
The largest $\text{lcm}(|\bar{c}|, |\bar{d}|)$ can be is 60, which is the order of $(\bar{1}, \bar{1})$.