Algorithms HW

1. Let G be a group, and let $\Gamma^\bullet G$ be its descending central series. Show that:

   - each $\Gamma^i G$ is a normal subgroup of G;
   - each $\Gamma^{i+1} G$ is contained in $\Gamma^i G$; and
   - each $\Gamma^i G/\Gamma^{i+1} G$ is contained in the centre of $G/\Gamma^{i+1} G$.

- We show that $\Gamma^i G \trianglelefteq G$ by induction on i. Since $\Gamma^1 G = G$ our base case is $i = 2$. Recall that $\gamma^2 G$ is generated by commutators $[g, h]$ where $g, h \in G$. Now let $k \in G$ and consider

  $$k[g,h]k^{-1} = kghg^{-1}h^{-1}k^{-1} = (kgk^{-1})(khk^{-1})(kg^{-1}k^{-1})(kh^{-1}k^{-1}) = [kgk^{-1}, khk^{-1}] \in \Gamma^2 G.$$

  And so, $\Gamma^2 G \trianglelefteq G$ by definition.

  Now suppose $\Gamma^i G \trianglelefteq G$ and consider $\Gamma^{i+1} G$, which is generated by elements $[g, h]$ where now $g \in G$ and $h \in \Gamma^i G$. Let $k \in G$ and notice that, since $\Gamma^i G$ is normal by the induction hypothesis, we have $khk^{-1} \in \Gamma^i G$. Thus the above calculation gives that $k[g,h]k^{-1} = [kgk^{-1}, khk^{-1}] \in \Gamma^{i+1} G$. Thus, each $\Gamma^i G \trianglelefteq G$ by induction.

- We show that $\Gamma^{i+1} G \subseteq \Gamma^i G$. Let $[g, h]$ be a generator of $\Gamma^{i+1} G$ so that $g \in G$ and $h \in \Gamma^i G$. Above we showed that $\Gamma^i G \trianglelefteq G$ and so $ghg^{-1} \in \Gamma^i G$. Moreover, $h \in \Gamma^i G$ implies $h^{-1} \in \Gamma^i G$ since $\Gamma^i G$ is a group. Thus

  $$[g,h] = ghg^{-1}h^{-1} = (ghg^{-1})h \in \Gamma^i G.$$

  Then, since each generator of $\Gamma^{i+1} G$ is contained in $\Gamma^i G$, we have $\Gamma^{i+1} G \subseteq \Gamma^i G$.

- todo

■

> 2. (CMN Example 2.8) What is the derived series for the dihedral group D_{2n}? What is the descending central series?

I'm sorry I'm going to use D_n to denote the dihedral group which has $2n$ elements. Recall the presentation

$$D_n = \langle r, s : r^n = s^2 = e \quad rs = sr^{-1} \rangle$$

First note that D_1 and D_2 are abelian. We have $D_1 = \{e, s\}$ a single non-trivial element, and so is trivially abelian. Meanwhile $D_2 = \{e, s, r, rs\}$, the relation $rs = sr^{-1}$ becomes $rs = sr$, i.e. $[r, s] = e$. Likewise we have $[r, rs] = r(rs)r(rs)^{-1} = r^2(rs)(rs)^{-1} = e$ and $[s, rs] = s(rs)s(rs)^{-1} = s^2(rs)(rs)^{-1} = e$[1]. Hence, D_2 is also abelian. Question: was it sufficient to show that r, s commute to show that D_n is abelian? And generally speaking, if a group is generated by n elements $g_1, \cdots g_n$ which all commute, is that sufficient to show that the group is abelian? (later), okay I have convinced myself. I think in general showing that all the generators of a finite group commute with each other is enough to show that every commutator of a group is trivial.

It follows that the derived subgroup $G' = \Gamma^2 G$ is trivial for $G = D_1$ or $G = D_2$. Moreover, since $\Gamma^3 G$ is generated by $[g, e] = geg^{-1}e = e$ for each $g \in G$, it follows that $\Gamma^i G$ is trivial for each $i > 1$ for both of these groups.

Now suppose $n \geq 3$ is odd. We show first that $\Gamma^2 G = \langle r \rangle$ by computing all the commutators. Recall that $\Gamma^2 G = G'$ is the subgroup generated by all commutators $[g, h]$ where $g \in G$ and $h \in \Gamma^1 G = G$. We need to compute the following commutators: $[r^k, s], [r, r^k s], [s, r^k s]$ where $k = 1, \cdots, n-1$. First recall the relation $rs = sr^{-1}$ and then consider the following

$$[r^k, s] = r^k s r^{-k} s = r^k r^{-k} s^2 = r^{-2k} \neq e$$

where the last equality follows from the fact that n is odd. In particular $k = 1$ shows that

[1] I later realized that computing $[g, h]$ is enough to determine $[h, g]$. In particular if $[g, h] = x$ for some $x \in G$ then we have $ghg^{-1}h^{-1} = x \implies x^{-1} = hgh^{-1}g^{-1} = [h, g]$. Alas, there is some redundent calculation above.

$r^2 \in \Gamma^2 G$. Very similar calculations give the following

$$[r, r^k s] = r(r^k s)r^{-1}(sr^{-k}) = r^2 \neq e$$
$$[s, r^k s] = s(r^k s)s(sr^{-k}) = r^{-2k} \neq e$$

Then, since we have already shown that $r^2 \in \Gamma^2 G$ we have that $\Gamma^2 G = \langle r^2 \rangle$. The situation is even better than this because for $n \geq 3$ odd we have $\langle r^2 \rangle = \langle r \rangle$. We have $r^2 = r \cdot r \in \langle x \rangle$. Moreover, consider there are n distinct powers of r in $\langle r^2 \rangle$, we have

$$\langle r^2 \rangle = \{r^2, r^4, \cdots, r^{n+1} = r, r^{n+3}, \cdots, r^{2n-2}, e\},$$

since, again, n is odd. That is, we have $r \in \langle r^2 \rangle$ and so indeed we have

$$\Gamma^2 G = \langle r^2 \rangle = \langle r \rangle.$$

Next we show that when $\Gamma^{i-1} G = \langle r \rangle$ then we must have $\Gamma^i G = \langle r \rangle$ for $i = 3, 4, \ldots$ Recall that $\Gamma^i G$ is generated by $[g, h]$ where $g \in G$ and $h \in \Gamma^{i-1} G$. Since $\Gamma^{i-1} G$ is only generated by a single element we only need to compute the following:

$$[r^k, r] = e$$
$$[s, r] = r^{-2}$$
$$[r^k s, r] = r^{-2},$$

following similar calculations to above. That is $\Gamma^i G = \langle r^2 \rangle$ and we still have $\langle r^2 \rangle = \langle r \rangle$, since this was a property of the group D_n for $n \geq 3$ odd. That is, we have shown $\Gamma^i G = \langle r \rangle$ for $i \geq 2$.

Now we consider the case when $n \geq 4$ is even. First notice that we can split this case into two further cases — either $n = 2^k$ for some k or $n = 2^k m$ for some k and some $m \geq 3$ odd. If n is not a power of 2 then its prime factor decomposition is $2^k m$ where m is the product of all of its odd prime factors.

Now first consider the case where $n = 2^k m$. Our above calculation shows that $\Gamma^2 D_{2^k m} = \langle r^2 \rangle$ but now $\langle r^2 \rangle \neq \langle r \rangle$ since r^2 has even order. In particular $\langle r^2 \rangle = \{r^2, r^4, \cdots, r^{2 \cdot (2^{k-1} m)} =$

$e\}$. Now we compute $\Gamma^3 G$ via direct computation of the generators $[g,h]$ where $g \in G$ and $h \in \Gamma^2 G = \langle r^2 \rangle$. Following the now usual strategy, we have

$$
\begin{aligned}
[r^k, r^2] &= e \\
[s, r^2] &= sr^2sr^{-2} = r^{-4} \\
[r^k s, r^2] &= r^{-4}.
\end{aligned}
$$

That is, $\Gamma^3 G = \langle r^4 \rangle$. Essentially the same calculation will give $\Gamma^i G = \langle r^{2^{(i-1)}} \rangle$ for $2 \leq i$. The book claims that this simplifies to $\langle r^{2^k} \rangle$ when $i \geq k+1$, but im having trouble seeing why.

Now suppose $n = 2^k$ for some k. The same computation as above gives $\Gamma^i G = \langle r^{2^{(i-1)}} \rangle$ for $i \geq 2$. However, now when $i \geq k+1$ we have $r^{2^{(i-1)}} = r^{2^{(k+\ell)}} = (r^{2^k})^{\ell} = e^{\ell} = e$. And so, when $i \geq k+1$ we have $\Gamma^i G = e$. This last fact also follows since when $i = k+1$ we have $\Gamma^i G = \langle r^{2^k} \rangle = e$ and in question 1 we showed that $\Gamma^i G \subseteq \Gamma^{i-1} G$ and so it would then follow that all $\Gamma^i G = e$ for all $i > k+1$. That is, when $n = 2^k$ we have that D_n is nilpotent, and in particular solvable.

Now we consider the derived series for D_n. Recall that $(D_n)^{(1)} = \Gamma^2 D_n$, and then $(D_n)^{(i)}$ is generated by $[g,h]$ for each $g,h \in (D_n)^{(i-1)}$. For $n = 1,2$ we showed above that D_n is abelian. It follows that all commutators are trivial, i.e., $G^{(1)} = e$ and then $G^{(i)} = 1$ for all $i \geq 1$. For $n \geq 3$ we showed above that the derived subgroup $G' = \langle x \rangle$ is a cyclic subgroup, for either $x = r$ or $x = r^{2k}$. In particular G' is abelian, and so it follows that all commutators $[g,h]$ with $g,h \in G'$ are trivial. And so for $n \geq 3$ we have $(D_n)^{(1)} = \langle x \rangle$ and $(D_n)^{(i)} = e$ for $i > 1$, where x depends on the exact form of n, as discussed above.

∎

3

■

4. Let
$$1 \to N \to G \xrightarrow{\pi} H \to 1$$
be an extension of groups. Show that there is a homomorphism
$$\rho \colon H \to \mathrm{Out}(N)$$
sending an element $h \in H$ to the outer automorphism of N given by conjugation by any $\tilde{h} \in G$ such that $\pi(\tilde{h}) = h$. In the particular case that $G = N \rtimes_\theta H$ is the semidirect product of H by N via θ, show that ρ is equal to the composition
$$H \xrightarrow{\theta} \mathrm{Aut}(N) \to \mathrm{Out}(N)\,.$$

Firstly, we will show that ρ is a well defined map $H \to Out(N)$. Let $h \in H$ and $\tilde{h}_1, \tilde{h}_2 \in G$ such that $\pi(\tilde{h}_1) = \pi(\tilde{h}_2) = h$. We have $\rho(\tilde{h}_1) = f := (n \mapsto \tilde{h}_1 n \tilde{h}_1^{-1})$ and $\rho(\tilde{h}_2) = g := (n \mapsto \tilde{h}_2 n \tilde{h}_2^{-1})$. Note that these are indeed automorphisms of N, as in the previous homework we showed that conjugation by a fixed element is an automorphism. If we show that $\rho(\tilde{h}_1)$ and $\rho(\tilde{h}_2)$ lie in the same coset of $Inn(N)$ then ρ is well-defined. (Note: I believe this map is not well defined as a map $H \to Aut(N)$).

Recall that two elements g, h of a group lie in the same coset of a normal subgroup N if $g^{-1}h \in N$. For our automorphisms f, g we have $g^{-1} = (n \mapsto \tilde{h}_2^{-1} n \tilde{h}_2)$. And so we have $(g^{-1} \circ f)(n) = \tilde{h}_2^{-1} \tilde{h}_1 n \tilde{h}_1^{-1} \tilde{h}_2$. Recall that $N \trianglelefteq G$ and so is closed under conjugation by definition. In particular then $\tilde{h}_1 n \tilde{h}_1^{-1} \in N$ and $\tilde{h}_2^{-1}(\tilde{h}_1 n \tilde{h}_1^{-1})\tilde{h}_2 \in N$ since $\tilde{h}_1, \tilde{h}_2 \in G$. Thus f, g have the same image in $Out(N)$ and so ρ is well defined with respect to the choice of $\tilde{h}$.

Next we show that ρ is a group homomorphism. Let $h_1, h_2 \in H$ and $\tilde{h}_1, \tilde{h}_2 \in G$ such that $\pi(\tilde{h}_1) = h_1$ and $\pi(\tilde{h}_2) = h_2$. Moreover, since π is a group homomorphism we have $\pi(\tilde{h}_1 \tilde{h}_2) = \tilde{h}_1 \tilde{h}_2$. Following a similar, calculation to last week's homework, consider the following

$$
\begin{aligned}
\rho(h_1 h_2) &= \gamma_{\tilde{h}_1 \tilde{h}_2} \\
&= (n \mapsto \tilde{h}_1 \tilde{h}_2 n (\tilde{h}_1 \tilde{h}_2)^{-1}) \\
&= (n \mapsto \tilde{h}_1 \tilde{h}_2 n \tilde{h}_2^{-1} \tilde{h}_1^{-1}) \\
&= \gamma_{\tilde{h}_1} \circ \gamma_{\tilde{h}_2} \\
&= \rho(h_1)\rho(h_2).
\end{aligned}
$$

Thus, the given ρ is indeed a group homomorphism.

Now suppose $G = N \rtimes_\theta H$. We can state more precisely the outer automorphism given by ρ. Let $h \in H$ and then all lifts are of the form $\tilde{h} = (m, h)$ for some $m \in N$. Then, being explicit about the details of the semidirect product, our map $\rho(h) : \iota(N) \to \iota(N)$ acts as follows

$$
\begin{aligned}
\rho_h(n) &= (m, h) \cdot_\theta (n, e_H) \cdot_\theta (m, h)^{-1} \\
&= (m, h)(n, e_H)(\theta_{h^{-1}}(m^{-1}), h^{-1}) \\
&= (m\theta_h(n), h)(\theta_{h^{-1}}(m^{-1}), h^{-1}) \\
&= (m\theta_h(n)(\theta_h \circ \theta_{h^{-1}}(m^{-1}), hh^{-1}) \\
&= (m\theta_h(n)m^{-1}, e_H).
\end{aligned}
$$

Which induces the automorphism $f = (n \mapsto m\theta_h(n)m^{-1}) : N \to N$. Note that $(\theta_h \theta_{h^{-1}}) = id_H$ since θ is a group homomorphism $H \to Aut(N)$.

We show that this is the same as the composition $H \to Aut(N) \to Out(N)$. We have $h \mapsto \theta_h \mapsto \overline{\theta_h}$. Notice now that θ_h and f are lie in the same coset of $Inn(N)$. In particular

$$
\overline{\theta_h} = \overline{\gamma_m \theta_h} = \overline{f}
$$

since $\gamma_m = (n \mapsto mnm^{-1})$ is one of the inner automorphisms of N. Hence, in the case where $G = N \rtimes_\theta H$ we have ρ and $H \to Aut(N) \to Out(N)$ give the same map.

One interpretation of this is that, whilst ρ is a well defined map $H \to Out(N)$, it is not a well defined map $H \to Aut(N)$. However, in the case where G is a semidirect product of

N and H via θ, we have a preferred lift $h \mapsto (e_N, h) \in G$, and in fact there is a well defined map $H \to Aut(N)$, namely θ, whose projection gives the same map as ρ.

$\blacksquare$

5. (Aluffi Exercise IV.5.15) Let G be a group of order 28.

- Prove that G contains a subgroup of order 4, and a normal subgroup of order 7. Deduce that G is either a split extension of C_4 by C_7, or is a split extension of $C_2 \times C_2$ by C_7.
- Prove that there are only two homomorphisms $C_4 \to \mathrm{Aut}(C_7)$ and only two homomorphisms $C_2 \times C_2 \to \mathrm{Aut}(C_7)$, up to changing the choice of generators for C_4 and $C_2 \times C_2$.
- Deduce that there are exactly four groups of order 28, up to isomorphism.

- Sylow's theorem I gives us that there exists a subgroup of order 7 in G, since $|H| = 7^1 \cdot 4$ and $7 \not| 4$. Alternatively, Cauchy's theorem gives us that there exists an element $g \in G$ with $|g| = 7$, hence we have $|\langle g \rangle| \leq G$. Moreover, Sylow III gives us that there's only a single Sylow 7 group. Consider, if n_7 is the number of Sylow 7 groups in G then Sylow III gives us that $n_7 \equiv 1 \mod 7$ and $n_7 | 4$. The only integer solving both these conditions is $n_p = 1$. Likewise if we write $|G| = 28 = 2^2 \cdot 7$ and notice $2 \not| 7$ then Sylow I gives us that there exists a subgroup of order $2^2 = 4$.

  Next we argue that N is normal. If $g \in G$ then recall $\gamma_g = (\ell \mapsto g\ell g^{-1}) \in Aut(G)$. Therefore $\left|\gamma_g(N)\right| = |N|$. However, there's a unique subgroup of order 7 in G and so the image $\gamma_g(N) = N$ for all $g \in G$. That is, N is closed under conjugation by elements in G and so N is normal by definition. We have shown that G has a normal subgroup of order 7 and in fact we have found that $N \cong C_7$.

- Recall or perhaps I shall prove that $Aut(N) = Aut(C_7) \cong C_6$. Consider C_4, once we have specified where a generator $\sigma \in C_4$ is mapped to in C_6 then we have determined the homomorphism $C_4 \to C_6$. Since $|\sigma| = 4$ we must have $|\theta(\sigma)| = 4$ or $|\theta(\sigma)| = 2$, for θ non-trivial, since a homomorphism must map an element to an element whose order divides the original order. Notice that there's only a single element of order 2 in C_6. And so there's one trivial map and one non-trivial map $\overline{\theta} : C_4 \to N$. Since $\overline{\theta}(\sigma)$ has order two we can deduce that it is the automorphism which sends each element of C_7 to its inverse. That is $\overline{\theta}(\sigma) = (n \mapsto 7 - n)$. And, of course, the trivial map $\theta_{\text{triv}}(\sigma) = (n \mapsto 0)$ for each $\sigma \in C_4$.

  We use similar reasoning to determine the maps $\theta : C_2 \times C_2 \to Aut(N) \cong C_6$.

One generating set of $C_2 \times C_2$ is $\{(0,1),(1,0)\}$ and again, once we determine where these elements are mapped to by θ we have determine the entire homomorphism $\theta : C_2 \times C_2 \to C_6$. Now each generating element has order two, and so any non-trivial θ maps both the generating elements to the unique element of order 2 in C_6. And so, again, we have one trivial map $\theta_{\text{triv}} : C_2 \times C_2 \to C_6$ and one non-trivial map $\tilde{\theta} : C_2 \times C_2 \to C_6$. The automorphisms $\tilde{\theta}((0,1)) = \tilde{\theta}(1,0)$ are both the same as the one described above — $(n \mapsto 7 - n \equiv -n)$.

- Determining all the possible semi-direct products $C_7 \rtimes H$ with $H = C_4$ or $H = C_2 \times C_2$ will tell us the possible group laws on G. Notice that $N \cap H = \{e\}$ for $H = C_4$ or $C_2 \times C_2$, this follows since every element of $N \cong C_7$ is the identity or is order 7, meanwhile there are no elements of order 7 in either C_4 or $C_2 \times C_2$. We also need to show that $NH = G$. Then it follows that $G \cong N \rtimes_\theta H$ for $H = C_4$ or $H = C_2 \times C_2$ and one of the θ described above.

  With all possible homomorphisms $H \to Aut(N)$ described above, we can determine all the semi-direct products $N \rtimes H$. First suppose $H = C_4$ and $\theta : C_4 \to C_6$ the trivial map. That is $\theta(h) = (n \mapsto n)$ for each $h \in H$. We have the following group product for $N \rtimes_\theta H$:

$$
\begin{aligned}
(n_1, h_1) \cdot_\theta (n_2, h_2) &= (n_1 \theta_{h_1}(n_2), h_1 h_2) \\
&= (n_1 n_2, h_1 h_2).
\end{aligned}
$$

  That is, then $N \rtimes_\theta H$ is isomorphic to $C_7 \times C_4 \cong G$. The same calculation will give us that when $H = C_2 \times C_2$ and $\theta : C_2 \times C_2 \to Aut(N)$ is the trivial map, we also have $G \cong C_7 \times C_2 \times C_2$.

  Now we determine the products given by the non-trivial $H \to Aut(N)$.

∎

4

■

4

■

8. In this problem, we will find a presentation for the symmetric group S_n. Let Σ_n denote the group generated by $n-1$ elements $a_1, a_2, \ldots, a_{n-1}$, subject to the relations:

- $a_i^2 = 1$ for $1 \leq i \leq n-1$;
- $(a_i a_j)^2 = 1$ for $1 \leq i \leq j-1 \leq n-2$; and
- $(a_i a_{i+1})^3 = 1$ for $1 \leq i \leq n-2$.

(a) Show that there is a surjective homomorphism $\Sigma_n \twoheadrightarrow S_n$, sending a_i to the transposition $(i, i+1)$ for all $1 \leq i \leq n-1$.

(b) Show that the elements $a_i, a_j \in \Sigma_n$ commute for $|i-j| \neq 1$. Show also that

$$a_{i+1} a_i a_{i+1} = a_i a_{i+1} a_i$$

for $1 \leq i \leq n-2$.

(c) Show that every element of Σ_n can be written in the form

$$w \quad \text{or} \quad a_{n-1} w \quad \text{or} \quad a_{n-2} a_{n-1} w \quad \text{or} \quad \ldots \quad \text{or} \quad a_1 a_2 \ldots a_{n-2} a_{n-1} w,$$

where w is contained in the subgroup generated by $a_1, a_2, \ldots, a_{n-2}$.

(d) Show that there is a homomorphism $\Sigma_{n-1} \to \Sigma_n$ whose image is equal to the subgroup generated by the elements $a_1, a_2, \ldots, a_{n-2} \in \Sigma$. Using the previous part, show that Σ_n is a finite group of order $\leq n!$.

(e) Conclude that the homomorphism $\Sigma_n \to S_n$ you constructed is an isomorphism.

(a) Let ϕ denote the suggested map $\phi(a_i) = (i, i+1)$. We take the suggested map and extend it so that it's a homomorphism, i.e., $\phi(a_i \cdot a_j) = (j, j+1)(i, i+1)$ (note, here my elements of S_n act on the right of permutations of $[n]$, I do this so that my notation for transposition decomposition is correct later). Note that there are exactly $n-1$ transpositions of the form $(i, i+1)$ in S_n, namely $(1,2), (2,3), \cdots, (n-1, n)$. It then follows that Σ_n bijects onto the set of $(i, i+1)$ transpositions in S_n.

We argue that this homomorphism is indeed surjective. Next recall that any element $\sigma \in S_n$ has a disjoint cycle decomposition. That is we can always write $\sigma = ((a_1)_1, (a_1)_2, \cdots, (a_1)_(r_1)) \cdots ((a_k)_1, \cdots, (a_k)_(r_k))$ (apologies for this notation). Thus, we are done if we can show that every cycle is equal to some product of transpositions in S_n. If $(a_1, \cdots, a_k)$ is a cycle in S_n then we have

$$(a_1, \cdots, a_k) = (a_1, a_2)(a_1, a_3) \cdots (a_1, a_k)$$

Now, notice that (a_1, a_2) may not be of the form $(i, i+1)$, we could have, say, $(a_1, a_2) = (1, 4)$ if $n \geq 4$. However, we can decompose this further. Suppose (a_1, a_2) is a transposition in S_n with $a_1 < a_2$, then we have

$$\begin{aligned}(a_1, a_2) =& [(a_1, a_1+1)(a_1+1, a_1+2) \\ & \cdots (a_2-2, a_2-1)](a_2-1, a_2)[(a_2-2, a_2-1)\cdots(a_1+1, a_1+2)(a_1, a_1+1)],\end{aligned}$$

where, recall, our transpositions act on the right of a given permutation. Note that since each transposition is order two, this is really a conjugation of $(a_2 - 1, a_2)$ by the element $(a_1, a_1+1)\cdots(a_2-2, a_2-1)$. The equality above is probably easiest to see with an example. Suppose $n = 4$ and notice that indeed

$$(1,4) = (1,2)(2,3)(3,4)(2,3)(1,2) = [(1,2)(2,3)](3,4)[(1,2)(2,3)]^{-1}.$$

In any case, we've reaclled that every element of S_n has a disjoint cycle decomposition, every cycle has a transposition decomposition, and every transposition has a $(i, i+1)$ decomposition. It follows then that every element of S_n has a $(i, i+1)$-transposition decomposition, and so ϕ is surjective since it surjects onto the set of $(i, i+1)$ transpositions in S_n.

(b) First suppose $|i - j| \neq 1$ and without loss of generality suppose $0 \geq i+1 < j \leq n-1$. Then consider

$$a_i a_j = a_i (a_i a_j)^2 a_j = (a_i)^2 a_j a_i (a_j)^2 = a_j a_i,$$

using the given relations. In other words, each such a_i, a_j commute. Using a similar idea, consider

$$\begin{aligned} a_{i+1}a_ia_{i+1} &= a_{i+1}a_i(a_ia_{i+1})^3a_{i+1} \\ &= a_{i+1}a_i(a_ia_{i+1})(a_ia_{i+1})(a_ia_{i+1})a_{i+1} \\ &= a_{i+1}(a_i)^2a_{i+1}a_ia_{i+1}a_i(a_{i+1})^2 \\ &= (a_{i+1})^2a_{i+1}a_ia_{i+1} \\ &= a_{i+1}a_ia_{i+1}, \end{aligned}$$

holds for each $1 \leq i \leq n_2$.

(c) If w is a word which does not contain a_{n-1} then we are trivially done. First let w be a word in Σ_n which contains a_{n-1} but no instances of the letter a_{n-2}. That is w is a word such that $|n-1-j| > 1$ for all $a_j \in w$, where we use the notation $a_j \in w$ to mean "w contains the letter a_j". Note that the given relations imply that $(a_i)^{-1} = a_i$ for all $i \in [n]$, in particular, we do not have $a_j = (a_{n-1})^{-1}$ for some $j < n-1$. That is $\Sigma_{n-1} \leq \Sigma_n$. Since $a_{n-2} \notin w$ we have that a_n commutes with every letter in w and so we can write $w = a_n w'$ where $w' \in \Sigma_{n-1}$.

Now suppose $a_{n-2}, a_{n-1} \in w$ with $a_{n-2} <_w a_{n-1}$ (meaning, a_{n-2} is "to the left of" a_{n-1} in w), but $a_{n-3} \notin w$. That is $w = \bar{a}_1\bar{a}_2 \cdots a_{n-2} \cdots a_{n-1} \cdots \bar{a}_k$ where each $a_{n-3}\bar{a}_i \in \Sigma_{n-1}$. Now a_{n-1} commutes with everything to its left until "it hits" a_{n-2}. That is $w = \bar{a}_1 \cdots a_{n-2}a_{n-1} \cdots \bar{a}_k$. And, a_{n-1} does not commute with a_{n-2}, however, we can "push them down the word together", that is $w = \cdots \bar{a}_\ell a_{n-2}a_{n-1} \cdots = \cdots a_{n-2}\bar{a}_\ell a_{n-1} \cdots = \cdots a_{n-2}a_{n-2}\bar{a}_\ell \cdots$, Since $\ell < n-2 < n-1$. And so it follows that $w = a_{n-2}a_{n-1}w$ where $w \in \Sigma_{n-1}$.

The same logic above applies to any word of the form[2] $w = \cdots w_{n-k} \cdots w_{n-(k+1)} \cdots w_{n-1} \cdots$ (note, although i was too lazy to write, w is a finite word). That is, the logic above applies so that we can "push down a_{n-1} until it hits a_{n-2}, and then push the block $a_{n-2}a_{n-1}$ until they hit a_{n-3}, etc, until the block $a_{n-k} \cdots a_{n-1}$ is at the left of the word". That is, we can write

$$\begin{aligned}
w &= \cdots w_{n-k} \cdots w_{n-(k+1)}\bar{a} \cdots \bar{a}w_{n-2} \cdots w_{n-1} \cdots && \text{where } \bar{a} \in \Sigma_{n-1} \text{ possibly distinct} \\
&= \cdots w_{n-k} \cdots w_{n-(k+1)}\bar{a} \cdots \bar{a}w_{n-2}w_{n-1} \cdots \\
&= \cdots w_{n-k} \cdots w_{n-(k+1)} \cdots w_{n-2}w_{n-1} \cdots \\
&= \cdots w_{n-k}w_{n-(k+1)} \cdots w_{n-2}w_{n-1} \cdots \\
&= w_{n-k}w_{n-(k+1)} \cdots w_{n-2}w_{n-1} \cdots \\
&= w_{n-k}w_{n-(k+1)} \cdots w_{n-2}w_{n-1}w' && w' \in \Sigma_{n-1},
\end{aligned}$$

for $1 \leq k \leq n-1$. (Apologies for the cumbersome notation.)

[2]Note that we only care about the existence of letters w_{k-1} to the left relative to w_k, since we are attempting to "push the letters to the left of the word".

(d) Following the definition in the question Σ_{n-1} is the group generated by $n-2$ elements $\tilde{a}_1, \cdots, \tilde{a}_{n-2}$ satisfying the relations $(\tilde{a}_i)^2 = (\tilde{a}_i\tilde{a}_j)^2 = (\tilde{a}_i\tilde{a}_{i+1})^3 = 1$ for appropriate indices. Define a map $\Sigma_{n-1} \to \Sigma_n$ by $\tilde{a}_i \mapsto a_i$ for each i, and extend this so that it's a homomorphism, i.e., $(\tilde{a}_i\tilde{a}_j) \mapsto a_ia_j$. Then the relations of Σ_{n-1} are satisfied by the relations in Σ_n by definition. Hence the image of this map is the subgroup generated by a_i for $i = 1, \cdots, n-2$. Moreover, this map is injective.

We then have a chain of inclusions

$$\Sigma_1 = 1 \hookrightarrow \Sigma_2 \hookrightarrow \cdots \hookrightarrow \Sigma_{n-1} \hookrightarrow \Sigma_n.$$

Now consider, $|\Sigma_2| = 2$ by definition. The previous part shows that the words in Σ_3 are of the form $e \cdot w', a_1 \cdot w', a_1a_2 \cdot w'$, where $w' \in \Sigma_2$. Therefore, there are at most $3 \cdot |\Sigma_2| = 3 \cdot 2 = 6$ words in Σ_3. Generally, the previous part shows that there are at most $k\,|\Sigma_{k-1}|$ words in Σ_k. In particular, unpacking the recursion,

$$|\Sigma_n| \leq n\,|\Sigma_{n-1}| \leq n!$$

(e) In part (a) we showed that ϕ is a homomorphism and that it surjected onto S_n, which has $n!$ elements. It follows then that $|\Sigma_n| \geq n!$. Combined with the statement in the previous part, it follows that in fact $|\Sigma_n| = n!$. And so ϕ is in fact an isomorphism. I.e. $\Sigma_n \cong S_n$, and the description of Σ_n given in the question is then actually a presentation for S_n.

∎