Lecture XXXIV: Symmetric and Alternating Groups

§34.1 The Symmetric group S_n:

Recall S_n has the following generating sets

① $\{(i_1, \dots i_k) \,;\, 1 \le k \le n\}$ (cycles)

② $\{\sigma_{ij} = (i\ j) \quad 1 \le i < j \le n\}$ (Transpositions)

③ $\{s_i := (i\ i{+}1) \quad 1 \le i < n\}$ (simple transpositions)

- In §3.2, we showed ① & ②, and gave a pictorial proof of ③.
- Algebraic argument for ③: It's enough to show each σ_{ij} can be written as a product of simple transpositions. Indeed

$$(1\ n) = (n{-}1\ n)\,(1\ n{-}1)\,(n{-}1\ n) \quad \text{by direct computation.}$$
$$= (n{-}1\ n)\,(n{-}2\ n{-}1)\,(1\ n{-}2)\,(n{-}2\ n{-}1)\,(n{-}1\ n)$$
$$= \cdots = s_{n-1}\, s_{n-2}\, s_{n-3} \cdots s_2\, s_1\, s_2\, s_3 \cdots s_{n-1}.$$

Similarly, $(i\ j) = (j{-}1\ j)\,(i\ j{-}1)\,(j{-}1\ j)$
$$= \cdots = s_{j-1}\, s_{j-2} \cdots s_{i+1}\, s_i\, s_{i+1} \cdots s_{j-2}\, s_{j-1}.$$

Corollary: S_n can be generated by any of the following sets:

(1) $\{(1 2), (1 3), \dots, (1 n)\}$

(2) $\{(1 2), (2 3), \dots, (n{-}1, n)\}$

(3) $\{(1 2), (1 2 3 \cdots n)\}$

Proof: Exercise

Q: What are the relations among s_i's?

- $s_i^2 = e$ (obvious)
- $s_i s_j = s_j s_i$ if $\{i\ i{+}1\} \cap \{j\ j{+}1\} = \emptyset$ (write $|i-j|>1$)
  (disjoint cycles commute)
- $s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$ because $s_i s_{i+1} s_i = (i\ i{+}2) = s_{i+1} s_i s_{i+1}$

Theorem:
$$S_n = \left\langle s_1, \dots, s_{n-1} \;\middle|\; \begin{array}{ll} s_i^2 = e & \forall i = 1, \dots, n-1 \\ s_i s_j = s_j s_i & \text{if } |i-j|>1 \\ s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1} & \forall i = 1, \dots, n-2 \end{array} \right\rangle$$

We provide a proof at the end of these notes (See § 34.4)

§ 34.2 The sign of a permutation:

We consider a function of n variables $f: \mathbb{Z}^n \longrightarrow \mathbb{Z}$ so we can evaluate $f_{(x_1,\ldots,x_n)}$

We define the function
$$\pi: S_n \longrightarrow \operatorname{Aut}_{\text{Set}}(\{f: \mathbb{Z}^n \to \mathbb{Z}\})$$
$$\sigma \longmapsto (\pi(\sigma): f \longmapsto \pi(\sigma)f_{(\underline{x})} = f(x_{\sigma(1)},\ldots,x_{\sigma(n)}))$$

where $\underline{x} = (x_1,\ldots,x_n)$.

Note: $\{f: \mathbb{Z}^n \to \mathbb{Z}\}$ is a group under $+$ induced by pointwise evaluation. We also have a pointwise multiplication on this set.

Indeed: $(f+g)_{(\underline{x})} = f_{(\underline{x})} + g_{(\underline{x})}$ $\forall \underline{x} \in \mathbb{Z}^n$; $0_{(\underline{x})}$ = constant zero function; inverse of $f = -f$.

Lemma 1: π is a group homomorphism ie $\pi(\sigma \circ \tau) = \pi(\sigma) \circ \pi(\tau)$.

In particular, $\pi(\mathrm{id}) = \mathrm{id}$ on functions & $S_n \circlearrowright \{f: \mathbb{Z}^n \to \mathbb{Z}\}$

Proof: $\pi(\sigma \circ \tau)(f)_{(\underline{x})} = f(x_{\sigma\circ\tau(1)},\ldots,x_{\sigma\circ\tau(n)}) = \pi_{(\sigma)}(f(x_{\tau(1)},\ldots,x_{\tau(n)}))$

$= \pi(\sigma)(f(x_{\tau(1)},\ldots,x_{\tau(n)})) = \pi(\sigma)(\pi(\tau)(f)_{(\underline{x})})$ $\square$.

Ex: $f = x_1$ $\quad \pi(\sigma\circ\tau)(f) = x_{\sigma\circ\tau(1)} = \pi_{(\sigma)}(x_{\tau(1)}) = \pi(\sigma)(\pi(\tau)(x_1)) = \pi_{(\sigma)}(\pi(\tau)(f))$.

Lemma 2: (1) The action respects the $+$ & $\cdot$ on $\{f: \mathbb{Z}^n \to \mathbb{Z}\}$
$$\sigma\cdot(f+g) = \sigma\cdot f + \sigma\cdot g$$
$$\sigma\cdot(fg) = (\sigma\cdot f)(\sigma\cdot g)$$

(2) If $c \in \mathbb{Z}$ constant $\sigma\cdot(cf) = c(\sigma\cdot f)$

Proof: $\sigma\cdot(f+g)_{(\underline{x})} = (f+g)_{(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})}$

$= f_{(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})} + g_{(x_{\sigma(1)}, x_{\sigma(2)}, \ldots, x_{\sigma(n)})}$

$= \sigma\cdot f_{(\underline{x})} + \sigma\cdot g_{(\underline{x})} = (\sigma\cdot f + \sigma\cdot g)_{(\underline{x})}$

Same idea works for $\cdot$.

$\sigma\cdot cf_{(\underline{x})} = (cf)_{(x_{\sigma(1)},\ldots,x_{\sigma(n)})} = c\, f_{(x_{\sigma(1)},\ldots,x_{\sigma(n)})} = c(\sigma\cdot f)_{(\underline{x})}$. $\square$

Proposition: Let $n \geq 2$. Then, $\exists$ unique surjective group homomorphism $\varepsilon: S_n \twoheadrightarrow \{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z}$ such that every transposition τ has $\varepsilon(\tau) = -1$.

Proof: We consider the function $\Delta(x_1,\ldots,x_n) = \prod_{1\leq i<j\leq n}(x_i - x_j)$

Take $\tau = (r\ s)$ with $r < s$.

Q: What is $\tau \cdot \Delta$?

$$(\tau\cdot\Delta)(\underline{x}) = \prod_{1\le i<j\le n} (x_{\tau(j)} - x_{\tau(i)})$$

We separate the factors involving r, s or neither

- if $|\{i,j\}\cap\{r,s\}| = 0$ $\quad (x_{\tau(j)} - x_{\tau(i)}) = (x_j - x_i)$
- if $|\{i,j\}\cap\{r,s\}| = 2 \Rightarrow i = r$ & $j = s$ because $i<j$ & $r<s$

$$\Rightarrow (x_{\tau(i)} - x_{\tau(j)}) = (x_s - x_r) = -(x_r - x_s) \quad \rightsquigarrow 1 \text{ sign change}$$

- if $|\{i,j\}\cap\{r,s\}| = 1$, we have options (they come in pairs)

$$\begin{cases} \cdot\ i = r < j < s & (x_{\tau(j)} - x_{\tau(i)}) = (x_j - x_s) = -(x_s - x_j) \rightsquigarrow s-r-1 \text{ choices} \\ \cdot\ r < i < j = s & (x_{\tau(j)} - x_{\tau(i)}) = (x_r - x_i) = -(x_i - x_r) \rightsquigarrow s-r-1 \text{ choices} \end{cases}$$

$$\begin{cases} \cdot\ i = r < s < j & (x_{\tau(j)} - x_{\tau(i)}) = (x_j - x_s) \\ \cdot\ i < r < j = s & (x_{\tau(j)} - x_{\tau(i)}) = (x_r - x_i) \end{cases}$$

$$\begin{cases} \cdot\ i < j = r < s & (x_{\tau(j)} - x_{\tau(i)}) = (x_s - x_i) \\ \cdot\ r < i = s < j & (x_{\tau(j)} - x_{\tau(i)}) = (x_j - x_r) \quad (r<s<j) \end{cases}$$

$\Rightarrow$ Putting these signs together we get $(-1)^{1+(s-r-1)+(s-r-1)} = -1$

$$\tau\cdot\Delta(x) = -\Delta(x)$$

We define $\varepsilon(\sigma)$ be the sign ± 1 such that $\sigma\cdot\Delta = \varepsilon(\sigma)\Delta$ for each permutation σ. In particular, $\varepsilon(\tau) = -1$ $\forall \tau$ transposition.

Since $\pi(\sigma\circ\tau) = \pi(\sigma)\circ\pi(\tau)$ & $\sigma\cdot(-\Delta) = -\sigma\cdot\Delta$ $\forall \sigma\in S_n$ we conclude that ε is a group homomorphism. Note $\varepsilon(12) = -1$ & $\varepsilon(id) = 1$.

Since S_n is generated by transpositions & $\varepsilon(ij) = -1$ $\forall i\neq j$, we conclude that ε is uniquely determined from this condition if it is a group homomorphism. $\square$

Remark: If $\sigma = \tau_1\circ\cdots\circ\tau_m$ is a product of transpositions, then $\varepsilon(\sigma) = (-1)^m$.

Definition: We say $\sigma\in S_n$ is __even__ if $\varepsilon(\sigma) = 1$, and __odd__ if $\varepsilon(\sigma) = -1$

Corollary: $\varepsilon((i_1 \cdots i_m)) = (-1)^{m-1} \quad \forall m \geq 1$

Proof: $(i_1 \cdots i_m) = (i_1 i_2) \cdots (i_{m-2} i_{m-1})(i_{m-1} i_m)$ is a product of $m-1$ many transpositions

§34.3 The Alternating group:

Definition: The alternating group $A_n = \operatorname{Ker} \varepsilon$, ie the set of even permutations.

Corollary: A_n is a normal subgroup of S_n of index 2, thus $|A_n| = \frac{n!}{2}$

Examples: (1) $A_2 = \{id\} \trianglelefteq S_2$

(2) $A_3 = \langle (123) \rangle \trianglelefteq S_3 \qquad A_3 \simeq \mathbb{Z}/_{3\mathbb{Z}}$ (no transposition lies in A_3, but even product of transpositions do: $(123) = (12)(23)$ & $(123)^2 = (12)(23)(12)(23)$)

(3) A_4 consists of id, all 3-cycles ($\binom{4}{3} \cdot 2 = 8$ options)

$$\left.\begin{array}{l} (12)(34) =: x \\ (13)(24) =: y \\ (14)(23) =: z \end{array}\right\} \text{ product of 2 disjoint transpositions (3 options)}$$

TOTAL = 12 elements.

Remark: $\{e, x, y, z\} \trianglelefteq A_4$

Lemma: (1) For $n \geq 3$, A_n is generated by 3-cycles

(2) For $n \geq 5$, all 3-cycles (in A_n) are conjugate to each other in A_n.

Proof: (1) $(abc) = (ab)(bc) \Rightarrow$ every 3-cycle lies in A_n

Conversely, if $\sigma \in A_n$, then σ = a product of an even number of transpositions

A product of 2 transpositions comes in 3 flavors

- $(ac)(ac) = e$
- $(ac)(ab) = (abc)$ if $c \neq b$
- $(ab)(cd) = (abc)(bcd)$ if $|\{a,b,c,d\}| = 4$ (only valid if $n \geq 4$)

Thus, any $\sigma \in A_n$ is a product of 3-cycles. for $n \geq 3$

(2) Fix $n \geq 5$. We show any 2 3-cycles are conjugate in A_n by explicit computation.

Assume $(a_1\, b_1\, c_1)$ & $(a_2\, b_2\, c_2)$ are two 3-cycles. Choose $\gamma \in S_n$ such that $\gamma(a_1) = a_2$, $\gamma(b_1) = b_2$ & $\gamma(c_1) = c_2$. Then $\gamma\,(a_1\, b_1\, c_1)\,\gamma^{-1} = (a_2\, b_2\, c_2)$

- If $\varepsilon(\gamma) = +1$, then $\gamma \in A_n$ and there is nothing to prove
- If $\varepsilon(\gamma) = -1$, choose $x, y \notin \{a_2, b_2, c_2\}$ with $x \neq y$ (note: x, y exists because $n \geq 5$)

Then $\sigma := (x\,y)\gamma$ satisfies $\varepsilon(\sigma) = +1$, so $\sigma \in A_n$

$$\sigma\,(a_1\, b_1\, c_1)\,\sigma^{-1} = (x y)\,\gamma\,(a_1\, b_1\, c_1)\,\gamma^{-1}\,(x y)^{-1} = (x y)\,(a_2\, b_2\, c_2)\,(x y)$$
$$= (a_2\, b_2\, c_2)\,(x y)^2 = (a_2\, b_2\, c_2)$$

disjoint cycles commute

□

Theorem 1: A_n is simple $\forall\, n \geq 5$

Proof: Assume K is a non-trivial subgroup of A_n with $K \trianglelefteq A_n$. We will show $K = A_n$

We consider the set $X = \{1, 2, \ldots, n\}$. Then $K \curvearrowright X$ by restricting the action $S_n \curvearrowright X$.

Choose $\sigma \in K \setminus \{e\}$ for which $|X^\sigma|$ is largest among all elements of $K \setminus \{e\}$.

$X^\sigma = \{x \in X : \sigma(x) = x\}$

Claim: σ is a 3-cycle

Assuming the claim, Lemma (2) combined with the fact that $K \trianglelefteq A_n$, shows that all 3-cycles are in K. In turn, Lemma (1) then implies $A_n = \langle \text{3-cycles} \rangle \leq K \leq A_n$, so $K = A_n$.

Proof of the Claim: We write σ as a product of disjoint cycles. We consider 2 cases:

① First, assume σ contains a cycle of length $m \geq 3$, ie $\sigma = (a_1\, a_2\, a_3 \cdots)\underbrace{\cdots}_{\text{other cycles}}$

- If $\sigma = (a_1, a_2, a_3)$ we are done
- Otherwise, we claim that $\exists\; a_4, a_5 \notin \{a_1, a_2, a_3\}$ with $a_4 \neq a_5$ and $\sigma(a_4) \neq a_4$, $\sigma(a_5) \neq a_5$

(Pf/ If σ is an m-cycle, by Corollary § 34.2, $m \geq 5$ so $a_4 = \sigma(a_3)$ & $a_5 = \sigma(a_4)$ will do.
If σ is a product of 2 or more non-trivial cycles, then any other cycle $(a_4\, a_5 \cdots)$ that is part of σ will do)

Let $\tau = (a_3\, a_4\, a_5)$ and consider $\sigma' = \underbrace{\tau \sigma \tau^{-1}}_{\in K} \underset{\in K}{\sigma^{-1}} \in K$ $(K \trianglelefteq A_n)$

Note: $\sigma' \neq e$ because $\tau\sigma \neq \sigma\tau$ since $\tau\sigma(a_2) = \tau(a_3) = a_4$
$\sigma\tau(a_2) = \sigma(a_2) = a_3$.

(with $a_4 \neq a_3$)

Claim: $X^\sigma \subsetneq X^{\sigma'}$ with $a_2 \in X^{\sigma'} \setminus X^\sigma$, contradicting the maximality of $|X^\sigma|$

Pf/ • $\sigma(x) = x \implies x \notin \{a_1, a_2, a_3, a_4, a_5\}$ so $\tau(x) = x$ by construction

Then, $\tau\sigma\tau^{-1}\sigma^{-1}(x) = \tau\sigma\tau^{-1}(x) = \tau\sigma(x) = \tau(x) = x$, ie $x \in X^{\sigma'}$

• $a_2 \notin X^{\sigma}$ since $\sigma(a_2) = a_3 \neq a_2$

• $a_2 \in X^{\sigma'}$ since $\tau\sigma\tau^{-1}\sigma^{-1}(a_2) = \tau\sigma\tau^{-1}(a_1) = \tau\sigma(a_1) = \tau(a_2) = a_2$. $\square$

(2) In the remaining case, all cycles in σ have length ≤ 2, so σ is a product of disjoint transpositions (evenly many of them, since $\sigma \in K \leq A_n$).

Write $\sigma = (ab)(cd)\underbrace{\cdots}_{\text{remaining transpositions}}$

Choose $k \notin \{a, b, c, d\}$ (such k exists because $n \geq 5$).

Let $\tau = (c\ d\ k)$ and consider $\sigma' = \underbrace{\tau\sigma\tau^{-1}}_{\in K}\underbrace{\sigma^{-1}}_{\in K} \in K$ $(K \trianglelefteq A_n)$

Note: $\sigma' \neq e$ because $\tau\sigma \neq \sigma\tau$ since $\tau\sigma(c) = \tau(d) = k$
$\sigma\tau(c) = \sigma(d) = c$. ($k \neq c$)

__Claim:__ $X^{\sigma} \setminus \{k\} \subseteq X^{\sigma'}$ with $a, b \in X^{\sigma'} \setminus X^{\sigma}$, again contradicting the maximality of $|X^{\sigma}|$

Pf/ • Pick $x \neq k$ with $x \in X^{\sigma}$, ie $\sigma(x) = x$. In particular, $x \notin \{a, b, c, d, k\}$

Then $\tau\sigma\tau^{-1}\sigma^{-1}(x) = \tau\sigma\tau^{-1}(x) \underset{x \notin \{c,d,k\}}{=} \tau\sigma(x) = \tau(x) = x$ so $x \in X^{\sigma'}$.

• $a \notin X^{\sigma}$ & $b \notin X^{\sigma}$ since $\sigma(a) = b$ & $\sigma(b) = a$

• $a \in X^{\sigma'}$ because $\tau\sigma\tau^{-1}\sigma^{-1}(a) = \tau\sigma\tau^{-1}(b) = \tau\sigma(b) = \tau(a) = a$

• $b \in X^{\sigma'}$ ——— $\tau\sigma\tau^{-1}\sigma^{-1}(b) = \tau\sigma\tau^{-1}(a) = \tau\sigma(a) = \tau(b) = b$

$\Rightarrow X^{\sigma'} \supseteq \{a, b\} \sqcup (X^{\sigma} \setminus \{k\})$ gives $|X^{\sigma'}| \geq 2 + |X^{\sigma} \setminus \{k\}| \geq 2 + |X^{\sigma}| - 1 = |X^{\sigma}| + 1$.

__Corollary 2:__ If $n \geq 5$, then S_n is not solvable

__Proof:__ By construction $[S_n : S_n] \subseteq A_n$ since $\varepsilon(\sigma\tau\sigma^{-1}\tau^{-1}) = 1$ $\forall \sigma, \tau \in S_n$.

Furthermore, $[S_n : S_n] \trianglelefteq S_n$ so $[S_n : S_n] \trianglelefteq A_n$.

Now $[S_n : S_n] \neq \{e\}$ because S_n is not abelian. Thus, $[S_n : S_n] = A_n$ because A_n is simple for $n \geq 5$.

Again $[A_n : A_n] \neq \{e\}$ because A_n is not abelian $\left(\begin{array}{l}(123)(124) = (13)(24) \\ (124)(123) = (14)(23)\end{array}\right)$

& $[A_n : A_n] \trianglelefteq A_n \implies [A_n : A_n] = A_n$

__Conclusion:__ $G^{(0)} = S_n$, $G^{(1)} = G^{(2)} = \cdots = A_n \neq \{e\}$ so S_n is not solvable if $n \geq 5$.

§34.4 A presentation for S_n (optimal):

Theorem: $$S_n = \left\langle s_1,\dots,s_{n-1} \;\middle|\; \begin{array}{ll} s_i^2 = e & \forall i=1,\dots,n-1 \\ s_is_j = s_js_i & \text{if } |i-j|>1 \\ s_is_{i+1}s_i = s_{i+1}s_is_{i+1} & \forall i=1,\dots,n-2 \end{array} \right\rangle$$

Proof: Define $\mathcal{G}_n := \langle \sigma_1,\dots,\sigma_{n-1} \mid \sigma_i^2 = e,\ \sigma_i\sigma_j = \sigma_j\sigma_i \text{ if } |i-j|>1,\ \sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \rangle$

Then, by construction, we have a surjective group homomorphism $\pi_n : \mathcal{G}_n \longrightarrow S_n$, $\sigma_i \longmapsto s_i \ \forall i$.

Since π_n is surjective $|\mathcal{G}_n| \geq |S_n| = n!$

(Note: We do not even know yet if $\mathcal{G}_n$ is even a finite group!)

To prove π_n is an iso, it is enough to confirm that $|\mathcal{G}_n| \leq n!$

(Indeed: $|\mathcal{G}_n| = |S_n| < \infty$ & $\pi_n : \mathcal{G}_n \longrightarrow S_n$ surjective $\Rightarrow \pi_n$ is also injective)

We prove by induction on n that $|\mathcal{G}_n| \leq n!$ $\forall n \geq 2$.

Base Case: $n=2$. $\mathcal{G}_2 := \langle \sigma \mid \sigma_1^2 = e \rangle \simeq \mathbb{Z}/2\mathbb{Z}$ has size $2 \leq 2!$

Inductive Step: We assume $|\mathcal{G}_k| \leq k!$ $\forall k = 2,\dots,n$, and show $|\mathcal{G}_{n+1}| \leq (n+1)!$

Since $\{\sigma_1,\dots,\sigma_{n-1}\} \subseteq \mathcal{G}_{n+1}$ satisfy the relations defining $\mathcal{G}_n$, we have a group homomorphism $i_n : \mathcal{G}_n \longrightarrow \mathcal{G}_{n+1}$

(Note: We don't know yet if i_n is injective or not)

Set $G_n = \operatorname{Im}(i_n) \leq \mathcal{G}_{n+1}$. More precisely G_n = subgroup of $\mathcal{G}_{n+1}$ generated by $\sigma_1,\dots,\sigma_{n-1}$

As $\mathcal{G}_n/\ker i_n \simeq G_n$ by the First Isomorphism Theorem, and $\mathcal{G}_n$ is finite, we know that $$|G_n| = \frac{|\mathcal{G}_n|}{|\ker i_n|} \leq |\mathcal{G}_n| \underset{\text{by the Inductive Hypotheses}}{\leq} n!$$

Note: $\pi_{n+1} \circ i_n = \pi_n$ since

$$\begin{tikzcd} \mathcal{G}_n \arrow[r, "\pi_n"] \arrow[d, "i_n"'] \arrow[dr, phantom, "\circlearrowleft"] & S_n \arrow[d, phantom, "\rotatebox{90}{$\leq$}"] \\ G_n \leq \mathcal{G}_{n+1} \arrow[r, "\pi_{n+1}"] & S_{n+1} \end{tikzcd}$$

<u>Claim</u>: $[\mathcal{G}_{n+1} : G_n] = |\mathcal{G}_{n+1}/G_n| \leq n+1$. (This would imply $|\mathcal{G}_{n+1}| = |G_n|\,[\mathcal{G}_{n+1} : G_n] \leq (n+1)\, n! = (n+1)!$, as we wanted)

<u>Proof of the Claim</u>: We identify $(n+1)$ left cosets from $\mathcal{G}_{n+1}/G_n$.

$H_{n+1} = e\,G_n \in \mathcal{G}_{n+1}/G_n$, $H_n = \sigma_n G_n$, $H_{n-1} = \sigma_{n-1}\sigma_n G_n$, ...

..., $H_1 = \sigma_1 \cdots \sigma_n G_n$ $\quad$ ($H_k = \sigma_k \sigma_{k+1} \cdots \sigma_n G_n$ for all $k = 1, \ldots, n$)

<u>Claim 1</u>: $H_\ell \subseteq$ inverse image under π_{n+1} of the subset $\{w \in S_{n+1} \mid w_{(n+1)} = \ell\}$)

(In fact $=$ holds)

Pf/ We check each H_k separately ($k = n+1$ & $k = 1, \ldots, n$)

- $x \in H_{n+1} \Rightarrow \alpha = \pi_{n+1}(x)$ verifies $\alpha_{(n+1)} = n+1$ since $\pi_{n+1} \circ i_n = \pi_n$.
- $x \in H_\ell$ ($\ell = 1, \ldots, n$) $\Rightarrow x = \sigma_\ell \cdots \sigma_n\, g$ for some $g \in G_n$ so $g = i_n(w)$, $w \in \mathcal{G}_n$.

$\Rightarrow \pi_{n+1}(x) = \pi_{n+1}(\sigma_\ell \cdots \sigma_n\, i_n(w)) = \pi_{n+1}(\sigma_\ell \cdots \sigma_n)\, \underbrace{\pi_{n+1} \circ i_n(w)}_{= \pi_n(w)}$

$\underset{\langle s_1, \ldots s_{n-1}\rangle}{\pi_n(w) \in}$ fixes $n+1$ & $\pi_{n+1}(\sigma_\ell \cdots \sigma_n)_{(n+1)} = (s_\ell \cdots s_n)_{(n+1)} = \ell$.

<u>Claim 2</u>: $H_1, \ldots, H_{n+1}$ are all distinct.

Pf/ If $x \in H_k \cap H_\ell$ with $k \neq \ell$, then

$$\pi_{n+1}(x) \in \{w \in S_{n+1} \mid w_{(n+1)} = \ell\} \cap \{w \in S_{n+1} \mid w(n+1) = k\} = \emptyset$$

Contradiction!

<u>Claim 3</u>: $\mathcal{G}_{n+1}/G_n = \{H_1, \ldots, H_{n+1}\}$ (so $|\mathcal{G}_{n+1}/G_n| \leq n+1$, as we wanted)

Pf/ We will show $\forall w \in \mathcal{G}_{n+1}$ and $1 \leq \ell \leq n+1$ $w \cdot H_\ell \in \{H_1, \ldots, H_{n+1}\}$

It is enough to check it for the generators of $\mathcal{G}_{n+1}$, ie when $w = \sigma_k$ for $k = 1, \ldots, n$.

(This will be enough to check $\{H_1, \ldots, H_{n+1}\} = \mathcal{G}_{n+1}/G_n$ by Lemma below)

Concretely, what is $\sigma_k H_\ell$?

- If $\ell = n+1$: $\sigma_k H_{n+1} = \sigma_k G_n = \begin{cases} G_n = H_{n+1} & \text{if } 1 \leq k \leq n-1 \\ \sigma_n G_n = H_n & \text{if } k = n+1 \end{cases}$ (*)

- If $\ell \neq n+1$: $\sigma_k H_\ell = \sigma_k(\sigma_\ell \sigma_{\ell+1} \cdots \sigma_n) G_n$

We treat several cases, by comparing k and ℓ.

CASE 1: $k < \ell - 1$, then $\sigma_k \sigma_i = \sigma_i \sigma_k \quad \forall i \geq \ell$ by the relations in $\mathcal{G}_n$

so $\sigma_k H_\ell = \sigma_k \sigma_\ell \sigma_{\ell+1} \cdots \sigma_n G_n = \sigma_\ell \sigma_k \sigma_{\ell+1} \cdots \sigma_n G_n = \sigma_\ell \cdots \sigma_n \sigma_k G_n$

$$= \sigma_\ell \cdots \sigma_n \underbrace{\sigma_k H_{n+1}}_{= G_n \text{ by } (*)} = \sigma_\ell \cdots \sigma_n G_n = H_\ell$$

CASE 2: $k = \ell - 1$, then $\sigma_{\ell-1} H_\ell = H_{\ell-1}$ by definition of $H_{\ell-1}$.

CASE 3: $k = \ell$, then $\sigma_\ell H_\ell = \underbrace{\sigma_\ell \sigma_\ell}_{= \mathrm{id} \text{ by relations in } \mathcal{G}_{n+1}} \sigma_{\ell+1} \cdots \sigma_n G_n = H_{\ell+1}$.

CASE 4: $k \geq \ell + 1$, then σ_k commutes with $\sigma_\ell \cdots \sigma_{k-2}$

So $\sigma_k H_\ell = \sigma_k \sigma_\ell \cdots \sigma_{k-2} \sigma_{k-1} \sigma_k \sigma_{k+1} \cdots \sigma_n G_n$

$$= \sigma_\ell \sigma_k \sigma_{\ell+1} \cdots \sigma_{k-2} \sigma_{k-1} \sigma_k \sigma_{k+1} \cdots \sigma_n G_n$$

$$= \sigma_\ell \sigma_{\ell+1} \cdots \sigma_{k-2} \underbrace{\sigma_k \sigma_{k-1} \sigma_k}_{\substack{\| \\ \sigma_{k-1} \sigma_k \sigma_{k-1} \text{ by relations in } \mathcal{G}_{n+1}}} \sigma_{k+1} \cdots \sigma_n G_n$$

Now σ_{k-1} commutes with $\sigma_{k+1} \sigma_{k+2} \cdots \sigma_n$, so

$$\sigma_k H_\ell = \sigma_\ell \sigma_{\ell+1} \cdots \sigma_{k-2} \sigma_{k-1} \sigma_k \sigma_{k-1} \sigma_{k+1} \cdots \sigma_n G_n$$

$$= \sigma_\ell \cdots\cdots \sigma_n \underbrace{\sigma_{k-1} G_n}_{= G_n \text{ by } (*)} = H_\ell$$

$\square$

Lemma: Given G group & $H \leq G$ subgroup, fix $X \subseteq G/H$, $X \neq \emptyset$.
If $gX = X \quad \forall g \in G$, then $X = G/H$.

Proof: Pick any $aH \in X$. Then, any $yH \in G/H$ can be expressed as $\underbrace{(ya^{-1})}_{=g}\underbrace{(aH)}_{\in X}$
So $yH = g(aH) \in gX = X$.

§34.5 Application:

The given presentation of S_n allows us to define the sign function on permutations in a different what than we did in §34.2

Definition: $\text{sign}: S_n \longrightarrow \{\pm 1\}$ $\text{sign}(ij) = -1$ determines a (unique) group homomorphism called the sign function

Given a permutation $w \in S_n$, we will write it as a product of transpositions $w = \tau_{i_1} \cdots \tau_{i_r}$. Then $\text{sign}(w) = (-1)^r$.

By construction, this assignment is multiplicative.

Issue: Why is $\text{sign}(w)$ well-defined?

Q: How do we know that for different expressions of w, the parity of the number of transpositions we used hasn't changed?

A: Use the presentation of S_n!

$\text{sign}(s_i) = -1 \quad \forall i$

Relations say
$$\text{sign}(s_i^2) = (-1)^2 = 1 \checkmark$$
$$\text{sign}(s_i s_j) = 1 = \text{sign}(s_j s_i) \quad \text{if } |i-j|>1$$
$$\text{sign}(s_i s_{i+1} s_i) = (-1)^3 = \text{sign}(s_{i+1} s_i s_{i+1})$$

So $\text{sign}: S_n \longrightarrow \{\pm 1\}$ is well-defined.

In particular if $w = s_{i_1} \cdots s_{i_k}$ for $i_1 \cdots i_k, j_1 \cdots j_\ell \in \{1, \ldots, n-1\}$
$= s_{j_1} \cdots s_{j_\ell}$

then $k \equiv \ell \mod (2)$, ie, the parity when using simple transpositions won't change.

In particular $(ij) = s_{j-1} s_{j-2} \cdots s_{i+1} s_i s_{i+1} \cdots s_{j-2} s_{j-1}$.

uses $(j-1-i)2+1$ simple transpositions. This is an even number,

so $\text{sign}(ij) = -1$. as we wanted

$\square$