Lecture 23

(23.0) Recall: last time we proved that

$$\left.\begin{array}{l} \alpha, \beta : H \longrightarrow \underset{gp}{Aut}(N) \\ \alpha(h) = T \circ \beta(h) \circ T^{-1} \quad \forall\, h \in H \end{array}\right\} \Rightarrow N \underset{\alpha}{\rtimes} H \cong N \underset{\beta}{\rtimes} H$$
$$(T(n), h) \longleftarrow\!\shortmid (n, h)$$

Here is another such circumstance:

Assume we are given a group hom $j : H \longrightarrow N$, out of which we build an α_j:

$$\begin{array}{rcl} H & \longrightarrow & Aut_{gp}(N) \\ h & \longmapsto & \alpha_j(h)(n) = j(h)\, n\, j(h)^{-1}. \end{array}$$

Lemma
$$\begin{array}{ccc} N \underset{\alpha_j}{\rtimes} H & \xrightarrow[f]{\cong} & N \times H \\ \downarrow & & \downarrow \\ (n, h) & \longrightarrow & (n \cdot j(h), h) \end{array}$$

Proof. f is a group hom because $\forall\ n_1, n_2 \in N$, $h_1, h_2 \in H$:

[if true, an iso., with inverse $(n, h) \mapsto (n, j(h^{-1}), h)$]

$$f(n_1, h_1) \overset{\text{in } N \times H}{\cdot} f(n_2, h_2) = (n_1 j(h_1) n_2 j(h_2), h_1 h_2)$$

&
$$f\left((n_1, h_1) \overset{\text{in } N \underset{\alpha_j}{\rtimes} H}{\cdot} (n_2, h_2)\right) = f\left((n_1 \cdot \alpha(h_1)(n_2), h_1 h_2)\right)$$
$$= f(n_1 j(h_1) n_2 j(h_1)^{-1}, h_1 h_2)$$
$$= (n_1 j(h_1) n_2 j(h_1)^{-1} \cdot j(h_1 h_2), h_1 h_2)$$

□

(23.1) Recall the definition: A group G is called <u>simple</u> if it has no <u>proper</u> (i.e. $\neq G$), <u>non-trivial</u> (i.e. $\neq \{e\}$), <u>normal</u> subgroups.

Convention: $\{e\}$ is <u>NOT</u> simple.

e.g. $\{\mathbb{Z}/p\mathbb{Z}\}_{p:\text{prime}}$: the set of simple abelian groups (cyclic)

Plan to study all (finite) groups: identify all finite simple groups! see how to build any group from simple ones

(Thus the word "simple" is used in the sense "everything complicated is made out of simple things"; not in the sense "easy to understand".)

(23.2) A Schur-type Lemma.

Let G_1 and G_2 be two groups (assume G_1 is simple) and let $f: G_1 \longrightarrow G_2$ be a group hom. Then either $f(x) = e_2$ (e_2 = unit of G_2) $\forall\, x \in G_1$; or f is injective.

Proof. $\mathrm{Ker}(f) \trianglelefteq G_1$ & G_1 being simple implies

either $\mathrm{Ker}(f) = G_1$ (i.e. $f(x) = e_2\ \forall\, x \in G_1$)

or $\mathrm{Ker}(f) = \{e_1\}$ (i.e., f is injective) □

(23.3) Alternating group. Let $n \geq 2$ and S_n be the permutation group on n letters.

Recall : (i) cyclic notation $\sigma = (x_1\ x_2\ \dots\ x_\ell) \in S_n$; where $\{x_1, x_2, \dots, x_\ell\} \subset \{1, 2, \dots, n\}$; means

$$\sigma(x_1) = x_2\ ;\ \sigma(x_2) = x_3\ ;\ \dots\ ;\ \sigma(x_{\ell-1}) = x_\ell\ ;$$
$$\sigma(x_\ell) = x_1\ ;\ \sigma(y) = y \quad \forall\ y \notin \{x_1, \dots, x_\ell\}.$$

(ii) Important identity (easy to prove):

$\forall\ \pi \in S_n$ and $\sigma = (x_1\ x_2\ \dots\ x_\ell) \in S_n$

(*) — $$\boxed{\pi\ (x_1\ x_2\ \dots\ x_\ell)\ \pi^{-1} = (\pi(x_1)\ \pi(x_2)\ \dots\ \pi(x_\ell))}$$

(iii) Other reminders -

- disjoint cycles commute (Proof: take π = a cycle disjoint from σ in (*).)
- $\pi = \pi_1\ \pi_2\ \dots\ \pi_\ell$ - disjoint cycles $\pi_1, \dots, \pi_\ell$
  each π_j = a cycle of length r_j
  $(r_1 + r_2 + \dots + r_\ell = n)$
  $\Rightarrow$ order(π) = l.c.m. $(r_1, r_2, \dots, r_\ell)$
- Cycles of length 2 are called <u>transpositions</u> $\{(i\ j) \mid 1 \leq i < j \leq n\}$. Every permutation can be written as product of transpositions:

Proof. $(x_1\ x_2 \cdots x_k) = (x_1\ x_2)(x_2\ x_3) \cdots (x_{k-1}\ x_k)$ □

(iv) In Lecture 8, we proved the existence of sign homomorphism

$$S_n \xrightarrow{\text{sign or } \varepsilon} \{\pm 1\}$$

so that $\varepsilon((ij)) = -1 \quad \forall \ 1 \le i < j \le n.$

For this we used, in Lecture 8, the following presentation of S_n:

$$\left\langle s_1, \dots, s_{n-1} \;\middle|\; \begin{array}{l} s_i^2 = e \ (1 \le i \le n-1) \ ; \ s_i s_j = s_j s_i \ (|i-j| \ge 2) \ ; \\ s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1} \ (1 \le i \le n-2) \end{array} \right\rangle$$

In (23.4) we give a more direct proof of the existence of sign hom

(23.4) Let $\pi \in S_n$ and let us write $\pi = \pi_1 \pi_2 \cdots \pi_\ell$; product of disjoint cycles of lengths $r_1, r_2, \dots, r_\ell$ respectively.

Define $N(\pi) = (r_1 - 1) + (r_2 - 1) + \dots + (r_\ell - 1)$

Lemma.- If $\pi = \tau_1 \tau_2 \tau_3 \cdots \tau_q$ where each τ_q is a transposition, then $q \equiv N(\pi) \pmod 2$.

Proof.- The following identity is easy to verify:

$$(a\ c_1\ c_2 \cdots c_k\ b\ d_1 \cdots d_\ell) = (a\,b)(b\,d_1 \cdots d_\ell)(a\,c_1 \cdots c_k)$$

Using this identity, we get the formula:

$$(**)\quad N((a\,b)\cdot\pi) = \begin{cases} N(\pi)+1 & \text{if } a,b \text{ lie in same cycle} \\ N(\pi)-1 & \text{o/w} \end{cases}$$

Now we can prove the lemma by induction on q.

$q = 0$ means $\pi = id$, hence $N(\pi) = 0 = q$ ✓.

$q > 0$. $\quad \pi = \tau_1 \underbrace{\boxed{\tau_2 \cdots \tau_q}}_{\pi'} = \tau_1\,\pi'$.

$$(**) \Rightarrow N(\pi) = N(\pi') \pm 1 \overset{\text{by induction on } \pi' = \tau_2 \cdots \tau_q}{\equiv} (q-1) \pm 1 \pmod 2$$

$$\equiv q \pmod 2$$

□

Cor. – $\quad \pi \longmapsto (-1)^{\#\text{ transpositions needed to write } \pi}$

is a well-defined group hom. $\varepsilon : S_n \longrightarrow \{\pm 1\}$

$A_n \overset{\text{defn.}}{=} \operatorname{Ker}(\varepsilon) \trianglelefteq S_n$ of index 2.

(A_n (alternating group on n letters))

(23.5) $A_2 = \{e\} \trianglelefteq S_2$.

$\mathbb{Z}/3\mathbb{Z} \cong A_3 = \langle (123) \rangle \trianglelefteq S_3$.

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

$(12)(34) =: x$
$(13)(24) =: y$
$(14)(23) =: z$
} 3 (ord 2 elements)

(Total = $12 = \frac{4!}{2}$ ✓)

$\{e, x, y, z\} \trianglelefteq A_4$ (Exercise!)

Lemma. (i) For $n \geq 3$; A_n is generated by 3-cycles.

(ii) For $n \geq 5$; all 3-cycles (in A_n) are conjugate to each other <u>in A_n</u>.

Proof. (i) $(a\ b\ c) = (a\ b)(b\ c)$ ⇒ every 3-cycle is in $A_n = \text{Kernel}(\varepsilon)$.

Conversely, if $\sigma \in A_n$, then σ = a product of <u>even number</u> of transpositions, hence a product of 3-cycles because:

$(a\ c)(a\ c) = e$

$(a\ c)(a\ b) = (a\ b\ c)$

$(a\ b)(c\ d) = (a\ b\ c)(b\ c\ d)$

[Fig: product of 2 transpositions can be written in terms of 3-cycles]

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

i.e. $\gamma\,(a_1\ b_1\ c_1)\,\gamma^{-1} = (a_2\ b_2\ c_2)$.

If $\varepsilon(\gamma) = +1$, we have $\gamma \in A_n$ and there is nothing to prove.

If $\varepsilon(\gamma) = -1$, choose $x, y \notin \{a_2, b_2, c_2\}$; $x \neq y$.

[Need $n \geq 5$ here.]

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

$\gamma' = (x\ y)\cdot\gamma \xrightarrow{\ \varepsilon\ } (-1)\cdot\varepsilon(\gamma) = (-1)(-1) = +1$

So $(a_1\ b_1\ c_1)$ can be conjugated (by $\gamma' \in A_n$) to $(a_2\ b_2\ c_2)$ □

(23.6) Theorem: A_n is simple $\forall\ n \geq 5$.

Proof. Assume $K \trianglelefteq A_n$ is a non-trivial normal subgroup ($K \neq \{e\}$).

Let us write $X = \{1, 2, \ldots, n\}$.

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

Recall: $X^\sigma = \{x \in X \text{ such that } \sigma(x) = x\}$.

Claim. – σ is a 3-cycle. Assuming this, and using the fact that K is normal, we conclude that K contains all (in A_n) 3-cycles (see Lemma (ii) on page 6). But then $K = A_n$, by the same Lemma (i).

Proof of the claim: • First assume that σ has a 3-cycle in it.

$\sigma = (a_1\ a_2\ a_3\ \cdots)\cdots$. If $\sigma = (a_1\ a_2\ a_3)$ we are done. Otherwise there must exist $a_4 \neq a_5$ $(\notin \{a_1, a_2, a_3\})$ such that $\sigma(a_4) \neq a_4$ and $\sigma(a_5) \neq a_5$ (Why? – Ex.)

(more cycles perhaps)

Let $\tau = (a_3\ a_4\ a_5)$ and consider

$$\sigma' = \tau\sigma\tau^{-1}\sigma^{-1} \in K \quad (\text{as } K \text{ is normal})$$

Ex. – $X^\sigma \subset X^{\sigma'}$. $a_2 \in X^{\sigma'} \setminus X^\sigma$

contradicting maximality of $|X^\sigma|$.

Now, we are able to restrict ourselves to the case when

σ = a product of even number of transpositions.

$= (a\ b)(c\ d) \cdots$ perhaps more transpositions.

Choose $k \notin \{a, b, c, d\}$ [$n \geq 5$]

take $\tau = (c\ d\ k)$ and $\sigma' = \tau \sigma \tau^{-1} \sigma^{-1} \in K$.

Ex. - $X^\sigma \setminus \{k\} \subset X^{\sigma'}$. $a, b \in X^{\sigma'} \setminus X^\sigma$

again contradicting maximality of $|X^\sigma|$. □