Lecture 27

We are going to start with the conjugacy classes in S_n.

Recall that conjugacy classes are just orbits for the conjugate action of a group onto itself. In a previous lecture we saw the conjugates and conjugacy classes in S_3. Here, we want to see conjugates and conjugacy classes in S_n. So let's start with some examples and try to analyze the situation there.

Recall that any $\sigma \in S_n$ can be written as a product of disjoint cycles. So we'll only work w/ disjoint cycles.

Examples :-

Consider S_7 and let $\tau = (125)(43)$.

Let's find what the conjugate action of τ on some $\sigma \in S_7$ is.

Note that $\tau^{-1} = \big((125)(43)\big)^{-1} = (43)^{-1}(125)^{-1}$

$$= (43)(152)$$

i) Let $\sigma = (375)$. Then $\tau \cdot \sigma = \tau\sigma\tau^{-1}$

$$\tau\sigma\tau^{-1} = (125)(43)(375)(43)(152)$$

$$= (147) = (471)$$

Note that $\tau\sigma\tau^{-1}$ is again a 3-cycle. Moreover, the entries of $\tau\sigma\tau^{-1}$ are just the images of the entries of σ under τ as $\tau(3) = 4$

$\tau(7) = 7$

$\tau(5) = 1$

(ii) $\sigma = (1754)(23)$

Then $\tau\sigma\tau^{-1} = (125)(43)(1754)(23)(43)(125)$

$$= (2713)(54)$$

Again, $\tau\sigma\tau^{-1}$ has the same cycle type decomp-
-osition as σ and the entries in $\tau\sigma\tau^{-1}$ are just the images of the entries in σ under τ.

Let's change τ and see if the same things happens or not. Suppose $\tau = (1543)$

i') $\sigma = (375)$. Note that $\tau^{-1} = (1345)$

Then $\tau\sigma\tau^{-1} = (1543)(375)(1345)$

$$= (741) = (174)$$

Again $\tau\sigma\tau^{-1}$ has the same cycle type as σ and the entries in $\tau\sigma\tau^{-1}$ are just the images of entries in σ under τ.

ii') $\sigma = (1754)(23)$

$\tau\sigma\tau^{-1} = (1543)(1754)(23)(1345)$

$= (5743)(21)$

Again $\tau\sigma\tau^{-1}$ has the same cycle type as σ and the entries in $\tau\sigma\tau^{-1}$ are just the images of entries in σ under τ.

All this examples basically tell us that given $\sigma \in S_n$, any conjugate to σ has the same cycle decomposition type as σ and we can explicitly find the entries too. More precisely,

<u>Theorem 1</u> Let $\sigma \in S_n$. Then $\forall\ \tau \in S_n$, $\tau\sigma\tau^{-1}$ has the same cycle decomposition type as σ. More-over the entries of $\tau\sigma\tau^{-1}$ are obtained by just writing the images of corresponding entries

of σ under τ.

<u>Proof</u> :- Suppose

$$\sigma = (a_1 a_2 \cdots a_n)(b_1 b_2 \cdots b_m) \cdots$$

In order to prove the theorem, we just need to show that if for $i, j \in \{1, 2, \ldots, n\}$

$$\sigma(i) = j \quad \text{then}$$

$\tau\sigma\tau^{-1}$ sends $\tau(i)$ to $\tau(j)$, as then we just replace the entries in σ by their images under τ which will also keep the same cycle decomposition type.

Now $\quad \tau\sigma\tau^{-1}(\tau(i)) = \tau\sigma(i) = \tau(j)$

$\Rightarrow$ $\tau\sigma\tau^{-1}$ sends $\tau(i)$ to $\tau(j)$ and hence the theorem is proved.

$\boxed{}$

So now we know that any conjugate of σ

has the same cycle decomposition type as σ.
Is the converse true?, i.e., any $\alpha \in S_n$ which has the same cycle decomposition type as σ is conjugate to σ which is to say that must there be a $\tau \in S_n$ s.t. $\alpha = \tau\sigma\tau^{-1}$?

It's enough to give an algorithm for finding τ, once we are given α and σ.

Again let $\alpha, \sigma \in S_7$, $\alpha = (1235)$ and $\sigma = (1374)$. We want to find a $\tau \in S_7$ s.t. $\tau\sigma\tau^{-1} = \alpha$. We follow the following algorithm:-

1) Write both α and σ as a product of disjoint cycles and write the cycles in increasing order of their lengths. We must include the 1-cycles too.

2) From Theorem 1, we know that if σ and α were conjugates then the entries of α are just the images of the corresponding entries of σ under τ. So, for finding τ we reverse-engineer! i.e., look at the corresponding entries in σ and α and write τ as that permutation which will make Theorem 1 work. Let's see an example to understand this fact.

Following 1), we write α and σ as follows

σ	α
$(2)(5)(6)(1374)$	$(4)(6)(7)(1235)$

i.e., we write σ and σ in increasing order of the lengths of the cycle, including the 1-cycles. Since there are more than one 1-cycle, it doesn't matter in which order you write them.

Now if $\alpha = \tau\sigma\tau^{-1}$ then from Theorem 1,

τ should send
$$2 \mapsto 4$$
$$5 \mapsto 6$$
$$6 \mapsto 7$$
$$1 \mapsto 1$$
$$3 \mapsto 2$$
$$7 \longrightarrow 3$$
$$4 \mapsto 5$$

Writing that as cycles $\tau = (2\,4\,5\,6\,7\,3)$

and one can check that indeed $\tau\sigma\tau^{-1} = \alpha$.

Let's see another example.

Let $\sigma, \alpha \in S_9$. $\sigma = (1\,5)(3\,4\,9)(6\,8\,2)$

and $\alpha = (2\,3)(8\,9\,6)(5\,1\,7)$

We want to find $\tau \in S_9$ s.t. $\tau\sigma\tau^{-1} = \alpha$.

We follow 1) and 2) of the algorithm:-

σ $\qquad\qquad\qquad\qquad$ α

$(7)(15)(349)(682)$ $\qquad\qquad$ $(4)(23)(896)(517)$

Note, again that we have written the 1-cycle too and it doesn't matter in which order you write the two 3-cycles. They might give different τ's but all them will satisfy $\tau\sigma\tau^{-1} = \alpha$. So we get that

There can be many τ in S_n s.t. $\tau\sigma\tau^{-1} = \alpha$ for a given σ and α in S_n.

Now we do 2).

τ must send $7 \to 4,\ 1 \to 2,\ 5 \to 3,\ 3 \to 8,\ 4 \to 9,$
$9 \to 6,\ 6 \to 5,\ 8 \to 1,\ 2 \mapsto 7$, so

$\tau = (749653812)$ and one can check that $\tau\sigma\tau^{-1} = \alpha$.

In fact, there is nothing special with these examples and the same procedure will work for any S_n, giving

<u>Theorem 2</u> If $\sigma, \alpha \in S_n$ have the same cycle decomposition type, then they are conjugate to each other, i.e., $\exists\, \tau \in S_n$ s.t. $\tau\sigma\tau^{-1} = \alpha$. Moreover, τ can be explicitly found by following the proce--dures in the algorithm.

So combining Theorem 1 and 2, we get the following important result:-

Let $\sigma \in S_n$. Then $\alpha \in S_n$ is conjugate to σ, i.e, $\alpha \in O_\alpha$ if and only if σ and α have the same cycle decomposition type.

So for example if $G = S_5$ and $\sigma = (1234)$

then all other 4-cycles are conjugate to σ and only 4-cycles are conjugate to σ. Thus

$|O_\sigma| = \#$ of 4-cycles.

But the number of 4 cycles are $\dfrac{{}^5C_4 \times 4!}{4}$

$$= \frac{\frac{5!}{4!} \times 4!}{4} = \frac{5!}{4} = 5 \times 3 \times 2 \times 1$$

$$= 30$$

So, $|O_\sigma| = 30$. But from the O-S Theorem, $|S_5| = |O_\sigma||Stab(\sigma)|$ and for the conjugation action, $Stab(\sigma) = C(\sigma) \rightarrow$ centralizer of σ, thus we get, $|C(\sigma)| = \dfrac{|S_5|}{|O_\sigma|} = \dfrac{5!}{30}$

$$= \frac{5!}{\frac{{}^5C_4 \times 4!}{4}}$$

$$= \frac{5! \times 4}{{}^5C_4 \times 4!} = 4$$

But if you follow the argument above, then there was nothing special about S_5 or a 4-cycle.

Let $\sigma \in S_n$ be an m-cycle. Then from Theorem 1 and 2, all m-cycles in S_n are the only conjugates to σ

$$\Rightarrow |O_\sigma| = \frac{{}^nC_m \times m!}{m} = \frac{\frac{n!}{m! \times (n-m)!} \times m!}{m}$$

$$= \frac{n \cdot (n-1) \cdots (n-m+1)}{m}$$

So $$\boxed{|O_\sigma| = \frac{n \cdot (n-1) \cdots (n-m+1)}{m}}$$

and hence from the O-S Theorem, we get that

$$|C(\sigma)| = \frac{|S_n|}{|O_\sigma|} = \frac{n!}{\frac{n\cdot(n-1)\cdots(n-m+1)}{m}}$$

$$= m\cdot(n-m)!$$

Thus for any m-cycle σ in S_n

$$\boxed{|C(\sigma)| = m\cdot(n-m)!}$$

—————x—————x—————

Finally, we want to prove Cauchy's Theorem for any group, using group action. Earlier, we proved Cauchy's Theorem for abelian groups only.

<u>Theorem [Cauchy]</u> Let G be a finite group and let p be a prime s.t. $p \mid |G|$. Then G has an element of order p.

Proof :→ Consider the set X

$$X = \{ (g_1, g_2, \dots, g_p) \in \underbrace{G \times G \times \cdots \times G}_{p\text{-times}} \mid g_1 g_2 \cdots g_p = e \}$$

i.e., we are considering those p-tuples in $\underbrace{G \times G \times \cdots \times G}_{p\text{-times}}$ s.t. their ordered product $= e$.

Note that p is the same prime as in the hypothesis of the theorem. Also, ∵ each $g_i \in G$ $1 \le i \le p$, we are just multiplying them toge- -ther and getting e.

Now $\underbrace{(e, e, \dots, e)}_{p\text{-times}} \in X \Rightarrow X \neq \phi$.

Also, if $(g_1, \dots, g_p) \in X$ then there are $|G|$ choices for g_1, $|G|$ choices for $g_2, \dots,$ $|G|$ choices for g_{p-1}. However, since $g_1 g_2 \cdots g_p = e$

$$\Rightarrow \quad g_p = (g_1 g_2 \cdots g_{p-1})^{-1} \Rightarrow g_p \text{ has}$$

only one choice, once we have chosen $g_1, \dots, g_{p-1}$.

Thus, $|X| = |G|^{p-1}$. Since $p \mid |G| \Rightarrow$

$$p \mid |X| \quad \text{——— (1)}$$

Consider an action of $\mathbb{Z}_p$ on X by

$$1 \cdot (g_1, g_2, \dots, g_p) = (g_2, g_3, \dots, g_p, g_1)$$

i.e., if 1 acts on $(g_1, g_2, \dots, g_p)$ then we shift the elements towards the left by 1 place.

Similarly $2 \cdot (g_1, g_2, g_3, \dots, g_p) = (g_3, \dots, g_p, g_1, g_2)$

so we shift every element towards left by 2 places.

Check :→ The above is a group action.

By the Orbit-Stabilizer Theorem, if $x \in X$

$\Rightarrow |O_x| \,\big|\, |\mathbb{Z}_p|$ as $\mathbb{Z}_p$ is acting on X.

$\Rightarrow \forall x \in X, \; |O_x| = 1$ or p.

Also, the orbits partitions $X \Rightarrow$

$$\sum_{x \in X} |O_x| = |X|$$

$\therefore$ from ①, $p \,\big|\, |X| \Rightarrow p \,\big|\, \sum |O_x|$ — ②

now since $|O_x|$ can have size either 1 or p

$\Rightarrow$ either all orbits have size p or

if atleast one orbit has size 1 $\Rightarrow$ there must be atleast p orbits w/ size 1 as only then ② will be satisfied.

Now w/ the above action of $\mathbb{Z}_p$ on X

$$|O_{(e,e,\ldots,e)}| = 1$$

Thus there must be atleast $(p-1)$ elements in X, not equal to $(e, \dots, e)$ with their orbit size as 1.

If $(g_1, g_2, \dots, g_p) \in X$ w/ $|O_{(g_1, \dots, g_p)}| = 1$

then $\quad 1 \cdot (g_1, \dots, g_p) = (g_1, \dots, g_p)$

$$\Rightarrow \quad (g_2, g_3, \dots, g_p, g_1) = (g_1, \dots, g_p)$$

$$\Rightarrow \quad \begin{aligned} g_2 &= g_1 \\ g_3 &= g_2 \\ &\vdots \\ g_1 &= g_p \end{aligned} \quad \Rightarrow \quad g_1 = g_2 = \cdots = g_p = g \text{ (say)}$$

Now $(g_1, g_2, \dots, g_p) \in X \Rightarrow g_1 g_2 \cdots g_p = e$

$$\Rightarrow \quad \underbrace{g \cdot g \cdots g}_{p\text{-times}} = e \quad \Rightarrow \quad g^p = e$$

$$\Rightarrow \quad \operatorname{ord}(g) \mid p \Rightarrow \operatorname{ord}(g) = 1 \text{ or } \operatorname{ord}(g) = p$$

If $\operatorname{ord}(g) = 1 \Rightarrow g = e \Rightarrow (g_1, \dots, g_p) = (e, \dots, e)$ which is not possible.

Thus $\operatorname{ord}(g) = p$ and hence G has an element of order p.

$\boxed{\text{QED}}$