Section 4.3 Groups Acting on Themselves by Conjugation

Recall
A <u>partition</u> of $n \in \mathbb{Z}^+$ is a non-decreasing sequence of positive integers that sum to n.

Example Partitions of $n=5$

1, 1, 1, 1, 1	1, 2, 2
1, 1, 1, 2	2, 3
1, 1, 3	
1, 4	
5	

Key Idea Any group acts on the set $a = G$ by conjugation:
$g \cdot a = gag^{-1}$ (Check that this is a group action)

Elements, $a, b \in G$ are <u>conjugate</u> if $\exists\, g \in G$ with $b = gag^{-1}$
Orbits of this action are called <u>conjugacy classes</u>.
Conjugacy class containing $a \in G$ is $\{gag^{-1} \mid g \in G\}$

conjugacy class containing a
conjugacy class containing b
If $d \in Z(G)$, its conjugacy class is $\{gdg^{-1} \mid g \in G\} = \{d\}$

$Z(G)$ in gray

Different conjugacy classes may have different orders. Proposition 2 gives their orders. It involves stabilizers.

Stabilizer of $a \in G$ is $G_a = \{g \in G \mid g \cdot a = a\} = \{g \in G \mid gag^{-1} = a\}$
$= \{g \in G \mid ga = ag\} = C_G(a)$

Proposition 2

$$\begin{pmatrix}\text{\# of elements}\\ \text{in conjugacy class}\\ \text{containing } a\end{pmatrix} = \begin{pmatrix}\text{\# of elements}\\ \text{of orbit of } a\\ \text{under action}\end{pmatrix} = |G : G_a| = |G : C_G(a)|$$

Consequence
Theorem 7 (The Class Equation)

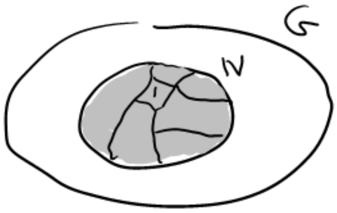
If G is finite and $g_1\ g_2\ g_3 \cdots g_k$ are representives distinct conjugacy classes not in $Z(G)$, then

$$|G| = |Z(G)| + \sum_{i=1}^{k} |G : C_G(a)|.$$

Corollary
Theorem 8 If G has order p^α, for a prime p, then $Z(G) \neq \{1\}$

Proof By class equation $1 \leq |Z(G)| = |G| - \underbrace{\sum_{i=1}^{k} |G : C_G(a)|}_{\text{Each term is a multiple of } p \text{ by Lagrange's Theorem}}$ is a multiple of p, so $p \leq |Z(G)|$

Significant Observation



Every normal subgroup $N \trianglelefteq G$ is a union of conjugacy classes.
(Because taking conjugates of $a \in N$ does not take a outside of N)

Converse is not true: Union of conjugacy classes may not even be a subgroup!

Conjugacy in S_n

Proposition 10 If $\sigma = (a_1\, a_2\, a_3 \cdots a_k)(b_1 b_2 \cdots b_\ell)\cdots \in S_n$ and $\tau \in S_n$ then $\tau\sigma\tau^{-1} = (\tau(a_1)\, \tau(a_2)\, \tau(a_3) \cdots \tau(a_k))(\tau(b_1)\, \tau(b_2) \cdots \tau(b_\ell))\cdots$

Proof:

$$\begin{array}{rccccccccl}
\sigma = & (a_1 & \xrightarrow{\sigma} & a_2 & \xrightarrow{\sigma} & a_3 & \xrightarrow{\sigma} \cdots \xrightarrow{\sigma} & a_k) & \cdots \\
& \tau^{-1}\uparrow & & \tau\downarrow\uparrow\tau^{-1} & & \tau\downarrow\uparrow\tau^{-1} & & \tau\uparrow\downarrow\tau^{-1} & \\
\tau\sigma\tau^{-1} = & (\tau(a_1) & & \tau(a_2) & & \tau(a_3) & \cdots & \tau(a_k)) & \cdots
\end{array}$$

Consequence (Two cycles are conjugate) $\iff$ (they have the same length)

Proof $(\Rightarrow)$ Proposition 10

$(\Leftarrow)$ Given equal length cycles $\sigma = (a_1\, a_2 \cdots a_k)$ and $\pi = (b_1\, b_2 \cdots b_k)$

Take $\tau \in S_n$ with
$$\begin{array}{cccc}
(a_1 & a_2 & \cdots & a_k) \\
\tau\downarrow & \tau\downarrow & & \tau\downarrow \\
(b_1 & b_2 & & b_k)
\end{array}$$
Then $\pi = \tau\sigma\tau^{-1}$ by Proposition 10.

Example Conjugacy class of $(1,2,3) \in S_4$ is all 3-cycles in S_4, i.e.
$\{(1,2,3), (1\,3\,2), (1\,2\,4), (1\,4\,2), (1\,3\,4), (1\,4\,3), (2\,3\,4), (2\,4\,3)\}$

How does this play out with arbitrary permutations (that are not cycles)?

Definition If $\pi \in S_n$ is a product of disjoint cycles of lengths $n_1 \le n_2 \le n_3 \le \cdots \le n_k$ (including cycles of length 1), then we say π has <u>cycle type</u> $n_1\, n_2\, n_3 \cdots n_k$.

Example $\pi \in S_n$ $\pi = (1\,3\,2)(4)(5\,6\,7)(8\,9)$ has cycle type $1, 2, 3, 3$.

Proposition 11 $\sigma, \pi \in S_n$ are conjugate in S_n if and only if they have the same cycle type. Thus number of conjugacy classes in S_n equals the number of partitions of n.

Reason:
$$\left.\begin{array}{l}
\sigma = (1\,3\,2)(4)(5\,6\,7)(8\,9) \\
\qquad\ \downarrow\downarrow\downarrow\ \ \downarrow\ \ \downarrow\downarrow\downarrow\ \ \downarrow\downarrow\tau \\
\pi = (4\,5\,9)(3)(1\,2\,6)(7\,8)
\end{array}\right\}\ \pi = \tau\sigma\tau^{-1}, \text{ etc.}$$

Example: S_5 $\quad (|S_5| = 5! = 120)$

Partitions of 5	Representative of conjugacy class with that cycle type
1 1 1 1 1	$()$ ⟵ even
1 1 1 2	$(1\,2)$
1 1 3	$(1\,2\,3)$ ⟵ even
1 4	$(1\,2\,3\,4)$
5	$(1\,2\,3\,4\,5)$ ⟵ even
1 2 2	$(1\,2)(3\,4)$ ⟵ even
2 3	$(1\,2)(3\,4\,5)$

even ones are in A_5

Computing centralizers in S_n (Useful because conjugacy class of $\pi \in S_n$ has $|S_n : C_{S_n}(\pi)|$ elements, so sometimes you need to find this number.)

Consider $\pi = (1\,2\,3 \cdots m) \in S_n$. What is $C_{S_n}(\pi)$ exactly?
First we will find its order. Conjugacy class of π consists of all m-cycles.
Total number of m-cycles is:

$$\binom{n}{m} m! \frac{1}{m} = \frac{n!}{m!(n-m)!}(m-1)! = \boxed{\frac{n!}{m(n-m)!}} = \underbrace{|S_n : C_{S_n}(\pi)|}_{\text{Using Proposition 2}} = \boxed{\frac{n!}{|C_{S_n}(\pi)|}}$$

Therefore $\boxed{|C_{S_n}(\pi)| = m(n-m)!}$

Now let's find the set $C_{S_n}(\pi)$ explicitly.
Let τ be a permutation of $\{m+1, m+2, m+3 \dots n\}$. ⟵ $(n-m)!$ such $\pi \in S_n$

Note: $\tau\pi\tau^{-1} = \pi$

Also $\pi = \pi^{\ell}\underbrace{(\tau\pi\tau^{-1})}_{\pi}\pi^{-\ell} = (\pi^{\ell}\tau)\pi(\pi^{\ell}\tau)^{-1}$

Conclusion: If $\pi = (1\,2\,3\,4 \cdots m) \in S_n$ then:

$$C_{S_n}(\pi) = \{\pi^{\ell}\tau \mid 1 \le \ell \le m,\ \tau \in S_{\{m+1, m+2, \dots n\}}\}$$

Recall $|A_5| = \frac{|S_5|}{2} = 60$

Theorem A_5 is simple. (i.e. has no proper nontrivial normal subgroup)

Proof Consider conjugacy classes of cycles in A_5.

A_5:
- 1
- $(1\,2\,3)$ ⟵ $\frac{5!}{3(5-3)!} = \frac{120}{6} = 20$ of these
- $(1\,2)(3\,4)$ ⟵ $\frac{1}{2}\binom{5}{2}\binom{3}{2} = 15$ of these
- $(1\,2\,3\,4\,5)$ ⟵ $\frac{1}{2}\frac{5!}{5(5-5)!} = 12$ of these
- $(1\,3\,5\,2\,4)$ ⟵ $\frac{1}{2}\frac{5!}{5(5-6)} = 12$ of these

Note: $(1\,2\,3\,4\,5)$
↓↓↓↓↓ $\tau = (2\,3\,5\,4)$ is odd.
$(1\,3\,5\,2\,4)$

Thus $(1\,2\,3\,4\,5)$ and $(1\,3\,5\,2\,4)$ are conjugate in S_5 but not in A_5.

A normal subgroup $N \trianglelefteq A_5$ would be a union of conjugacy classes, including $\{1\}$.
Thus $|N| = 1 + (\text{sum of some of } 20, 15, 12)$ and $|N|$ divides $|A_5| = 60$.
Only possibility is $N = \{1\}$. Thus A_5 is simple. ∎