# Sections 10



Last time: A finite set, $\sigma \in S_A$ is a cycle if it is of form $\sigma = (a_1\ a_2 \cdots a_n)$, meaning

$$\sigma(a_1) = a_2,\ \sigma(a_2) = a_3,\ \dots,\ \sigma(a_{n-1}) = a_n,\ \sigma(a_n) = a_1,$$
$$\sigma(b) = b \quad \text{if} \quad b \in \{a_1, \dots, a_n\}.$$

Transposition $\tau = (i\ j)$, cycle of length 2.

Thm Every $\sigma \in S_n$ can be written as

$$\sigma = \tau_1 \cdots \tau_m,$$

where $\tau_i$ are transpositions.

Note: Can always find $\tau_i$ s.t $m \leq n-1$.

Thm If $\sigma = \tau_1 \cdots \tau_m = \tau_1' \cdots \tau_{m'}'$, $\tau_i, \tau_j'$ are transpositions, then $m$ even/odd $\iff$ $m'$ even/odd.

Def If $\sigma = \tau_1 \cdots \tau_m$, with $m$ even/odd, say $\sigma$ is even/odd.

Example In $S_3$,

| even | odd |
|---|---|
| $e = (12)(12)$ | $\mu_1 = (2\ 3)$ |
| $\rho_1 = (1\ 2\ 3)$ | $\mu_2 = (1\ 3)$ |
| $= (1\ 3)(1\ 2)$ | $\mu_3 = (1\ 2)$. |
| $\rho_2 = (1\ 3\ 2)$ | |
| $= (1\ 2)(1\ 3)$ | |

Thm/def: The set $A_n = \{\sigma \in S_n \mid \sigma \text{ is even}\} \subseteq S_n$ is a subgroup, the "alternating group on $n$ letters" (Alternerende gruppa)

"Pf" $\sigma = \tau_1 \cdots \tau_m$, $\sigma' = \tau_1' \cdots \tau_{m'}'$, $m$, $m'$ even

$\Rightarrow \sigma\sigma' = \tau_1 \cdots \tau_m \tau_1' \cdots \tau_{m'}'$, $m + m'$ even $\Rightarrow \sigma\sigma' \in A_n$.

Example $A_3 = \{e, \rho_1, \rho_2\}$, $A_3 \simeq (\mathbb{Z}_3, +)$.

## Cosets

Let $G$ be a group $H \leq G$.

Def A left coset of $H$ is a set of the form

$$aH = \{ah \mid h \in H\}$$

for some $a \in G$. A right coset is a set of the form

$$Ha = \{ha \mid h \in H\}$$

for some $a \in G$. In additive notation $a + H = H + a$

Example Let $G = \mathbb{Z}$, $H = 3\mathbb{Z} < G$.

$$0 + 3\mathbb{Z} = \{0 + n \mid n \in 3\mathbb{Z}\} = 3\mathbb{Z}$$

$$1 + 3\mathbb{Z} = \{1 + n \mid n \in 3\mathbb{Z}\} = \{\ldots -2, 1, 4, \ldots\}$$

$$2 + 3\mathbb{Z} = \{2 + n \mid n \in 3\mathbb{Z}\} = \{\ldots -1, 2, 5, \ldots\}$$

Every $k \in \mathbb{Z}$ lies in one of these three.

Thm If $b \in aH$, $\iff bH = aH$.

Proof $b \in aH \Rightarrow b = ah$ for some $h \in H$.

$$\Rightarrow a = bh^{-1} \in bH$$

$c \in bH \iff cb^{-1} \in H \iff c(ah)^{-1} \in H \iff h^{-1}a^{-1}c \in H \iff a^{-1}c \in H$

$\iff ac \in aH$.

Corollary Every element of $G$ lies in a unique left coset of $H$.

$G = S_3$, $H = \langle \mu_1 \rangle = \{e, \mu_1\}$ $(\mu_1^2 = 2)$ $\mu_1 = (2\,3)$.

Left cosets of $\langle \mu_1 \rangle$ are

$$e\langle \mu_1 \rangle = \langle \mu_1 \rangle = \mu_1 \langle \mu_1 \rangle = \{\mu_1, \mu_1^2\}$$

$$\mu_2\langle \mu_1 \rangle = \{\mu_2 e, \mu_2 \mu_1\} = \{\mu_2, (1\,3\,2)\} \qquad \mu_2\mu_1 = (1\,3)(2\,3)$$

$$= \{\mu_2, \rho_2\} = \rho_2 \langle \mu_1 \rangle$$

$$\mu_3\langle \mu_1 \rangle = \{\mu_3 e, \mu_3 \mu_1\} = \{\mu_3, \rho_1\} = \rho_1 \langle \mu_1 \rangle.$$

Thm All cosets of $H$ have the same size.

Proof Let $aH$, $bH$ be cosets. Define

$$\phi : aH \longrightarrow bH$$

$$\phi(g) = ba^{-1}g,$$

valid since if $g \in aH \Longrightarrow g = ah$, $h \in H \Longrightarrow ba^{-1}ah = bh \in bH$.

Inverse $\phi^{-1} : bH \longrightarrow aH$ is $\phi^{-1}(g) = ab^{-1}g$, $\Longrightarrow \phi$ is one-to-one & onto $\Longleftrightarrow |aH| = |bH|$.

Thm If $G$ is a finite group, $H \leq G$, then $|H|$ divides $|G|$.

Proof $G$ is partitioned into cosets of size $|H|$,

$$\frac{|G|}{|H|} = \text{no. of cosets of } H \text{ in } G, \text{ an integer.}$$

Example Subgroups of $S_3$, $|S_3| = 6$, $|\langle e \rangle| = 1$, $|\langle \rho_1 \rangle| = |\langle \rho_2 \rangle| = 3$

$|\langle \mu_i \rangle| = 2$ $i = 1, 2, 3$.

Subgroups of $(\mathbb{Z}_n, +)$, $|\mathbb{Z}_n| = \varphi n$ are $\langle d \rangle$, where $d$ divides $n$,

$|\langle d \rangle| = \frac{n}{d}$, which divides $n$.

**Def** If $g \in G$, the order of $g$ is $|\langle g \rangle|$, equivalently

order of $g = \infty$ if $g^n \neq e \quad \forall n > 0$

— " — $= n$ if $n$ is minimal s.t. $g^n = e$

$$\langle g \rangle = \{e, g, g^2, \dots, g^{n-1}\}.$$

**Corollary** If $G$ is finite, $|g|$ divides $|G|$.

**Corollary** If $G$ is finite group, $g^{|G|} = e$ for all $g \in G$.

**Proof** $|g|$ divides $|G| \Leftrightarrow \frac{|G|}{|g|} = k$ for some $k \in \mathbb{N}$

$$g^{|G|} = \left(g^{|g|}\right)^k = e^k = e.$$

**Example** Every $\sigma \in S_n$ satisfies $\sigma^{n!} = e$.

**Def** If $G$ is a group $H < G$, the index of $H$ in $G$, is denoted $[G:H]$ is the size of the set of (left) cosets of $H$ in $G$.

**Example** $[\mathbb{Z} : 3\mathbb{Z}] = 3$

$[\mathbb{Z} : \langle 0 \rangle] = \infty$

$[G:H] = \frac{|G|}{|H|}$, if $G$, $H$ finite.

**Thm** If $K \leq H \leq G$, then $[G:H][H:K] = [G:K]$.

* Cor: Prime order groups are cyclic!

## Direct products

**Def** If $S_1, \dots, S_n$ are sets, then

$$S_1 \times \cdots \times S_n = \{(s_1, \dots, s_n) \mid s_i \in S_i\}.$$