MTH 339

Cyclic Groups:

Recall: If $G = \{a^n \mid n \in \mathbb{Z}\}$ for an $a \in G$ we call G cyclic and a the generator of G. We write $G = \langle a \rangle$.

Example: $(\mathbb{Z}, +)$ is cyclic, $G = \langle 1 \rangle = \langle -1 \rangle$.

$$\mathbb{Z}_8 = \langle 1 \rangle = \langle 3 \rangle = \langle 5 \rangle = \langle 7 \rangle$$

(To see this, compute for example

$$\langle 3 \rangle = \{3, 3+3 \bmod 8, 3+3+3 \bmod 8 \ldots\}$$
$$= \{3, 6, 1, 4, 7, 2, 5, 0\}.$$

$\langle 2 \rangle$ is not generating $\mathbb{Z}_8$ as $\langle 2 \rangle = \{0, 2, 4, 6\}$.

Thm Criterion for $a^i = a^j$

Let G be a group, $a \in G$.
If a has infinite order, all distinct powers of a are distinct group elements.

If a has finite order, say $|a| = n$, then $\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$ and $a^i = a^j$ if and only if n divides $i-j$.

Proof: If a has infinite order, there is no nonzero n such that $a^n = e$. Since $a^i = a^j \Rightarrow a^{i-j} = e$, we have $i = j$ or $i - j = 0$.

Assume $|a| = n$. We first show that

(*) $\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$.

Certainly, the elements $\{e, a, a^2, \dots, a^{n-1}\}$ are distinct (otherwise $|a| < n$).

Suppose a^k is an arbitrary member of $\langle a \rangle$.

We can write $k = qn + r$, $0 \leq r < n$.

$a^k = a^{qn+r} = a^r$, so $a^k \in \{e, a, \dots, a^{n-1}\}$

This proves (*).

Now assume $a^i = a^j \Rightarrow a^{i-j} = e$

$i - j = qn + r$, $0 \leq r < n$.

$\Rightarrow a^{i-j} = a^r = e \Rightarrow r = 0$, so

$i - j = qn$, hence $n \mid (i-j)$

Conversely, if $n \mid i-j$, so $i-j = qn$, we have

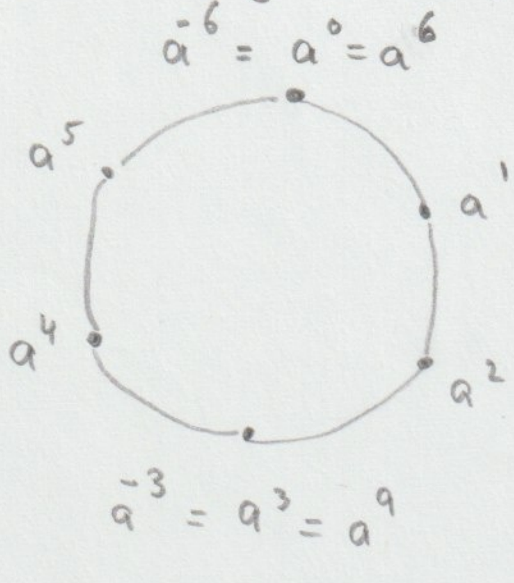
$a^{i-j} = a^{qn} = (a^n)^q = e$, so $a^i = a^j$

$\square$

<u>Corollary:</u> $a^k = e$ implies that $|a|$ divides k.

Proof: Set $n = |a|$ and $j = 0$.

So, in summary, a cyclic group is simple:



Therefore, essentially, $\mathbb{Z}_n$ and $\mathbb{Z}$ serve as prototypes for all cyclic group.

Permutation Groups

Def Permutation of A, Permutation Group of A.

A permutation of a set A is a function from A to A that is both one-to-one and onto. A permutation group of a set A is a set of permutations of A that forms a group under function composition.

Typically, we consider $A = \{1, 2, 3, \dots, n\}$.
For example α could be defined as

$$\alpha(1) = 2, \quad \alpha(2) = 3, \alpha(3) = 1, \quad \alpha(4 = 4$$

$$\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{bmatrix}$$

Composition of permutations expressed in array notation:

$$\sigma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{bmatrix} \qquad \gamma = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix}$$

$$\gamma\delta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 1 & 2 & 3 \end{bmatrix} \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 1 & 3 & 5 \end{bmatrix}$$

Example: S_3: Set of all one-to-one functions from $\{1,2,3\}$ to itself. The six elements are:

$$\epsilon = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{bmatrix}, \quad \alpha = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{bmatrix} \quad \alpha^2 = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{bmatrix}$$

$$\beta = \begin{bmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{bmatrix}, \quad \alpha\beta = \begin{bmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{bmatrix} \quad \alpha^2\beta = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix}$$

Note that $\beta\alpha = \begin{bmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{bmatrix} = \alpha^2\beta \neq \alpha\beta$,

so S_3 is non-Abelian.

Example: Generalize the above example to S_n.

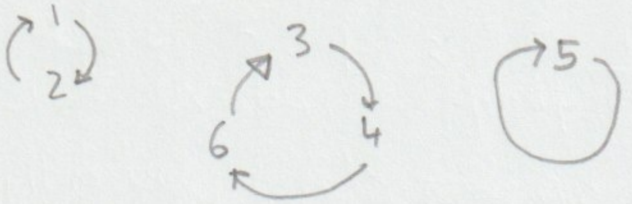
$$|S_n| = n!$$

The S_n are rich in subgroups. S_5 has more than 100 subgroups.

Cycle Notation

Consider $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 4 & 6 & 5 & 3 \end{bmatrix}$

$\alpha = (1,2)(3,4,6)(5)$



1 and 2 interchange	$3 \to 4$ $4 \to 6$ $6 \to 3$	5 invariant

An expression $(a_1, a_2, \dots, a_m)$ is called an m-cycle.

Note that some cycles leave some elements unchanged (e.g $(3,4,6)$ does not affect 1, 2, or 5.

Thm Every permutation of a finite set can be written as a cycle or a product of disjoint cycles.

Proof: Choose $a_1 \in A = \{1, 2, \dots, n\}$. Then "start to cycle" $a_2 = \alpha(a_1)$, $a_3 = \alpha^2(a_1)$ and so on. At some m, we need to be back at a_1.

(Since A is finite, for sure, there will be a repetition $\alpha^i(a_1) = \alpha^j(a_1)$, $i < j$, so $a_1 = \alpha^{j-i}(a_1)$)

Now we can write our first cycle

$\tilde{\alpha} = (a_1, a_2, \dots, a_m)$

For the next cycle $\tilde{\beta}$, we start with b_1 that is not in the set $\{a_1, \dots, a_m\}$. Continuing this, we will eventually run out and obtain

$$\alpha = \tilde{\alpha}\,\tilde{\beta}\,\tilde{\gamma} \dots$$

$\square$

MTH 339 - Do now

1./ Show $U(10) = \{1, 3, 7, 9\} = \langle 3 \rangle$

2./ Show that for $U(8) = \{1, 3, 5, 7\}$ we have $\langle 1 \rangle = \{1\}$, $\langle 3 \rangle = \{3, 1\}$, $\langle 5 \rangle = \{5, 1\}$, and $\langle 7 \rangle = \{7, 1\}$, so $U(8)$ is not a cyclic group.

3./ For $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{bmatrix}$ and $\beta = \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{bmatrix}$

compute $\alpha\beta$ and $\beta\alpha$.

4./ Write $\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 3 & 1 & 6 & 2 & 4 \end{bmatrix}$ in cycle notation.

($\beta = (2, 3, 1, 5)(6, 4) = (4, 6)(3, 1, 5, 2)$)

MTH 339 - HW

1./ Find all generators of $\mathbb{Z}_6$, $\mathbb{Z}_8$, and $\mathbb{Z}_{20}$.

2./ List the elements of the subgroups $\langle 3 \rangle$ and $\langle 7 \rangle$ in $U(20)$

3./ Let G be a group, $a \in G$.
Prove $\langle a^{-1} \rangle = \langle a \rangle$.

4./ If a cyclic group has an element of infinite order, how many elements of finite order does it have?

5./ Prove that a group of order 3 must be cyclic.

6./ Let $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 3 & 5 & 4 & 6 \end{bmatrix}$

$$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 4 & 3 & 5 \end{bmatrix}$$

Compute α^{-1}, $\beta\alpha$, $\alpha\beta$.

MTH 339 - HW

7./ Let $\alpha = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 3 & 4 & 5 & 1 & 7 & 8 & 6 \end{bmatrix}$

$\beta = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 3 & 8 & 7 & 6 & 5 & 2 & 4 \end{bmatrix}$

Write $\alpha, \beta, \alpha\beta$ as products of disjoint cycles.

8./ Let G be a group of permutations on a set X, let $a \in X$, and define $\text{stab}(a) = \{\alpha \in G \mid \alpha(a) = a\}$ (stabilizer of a in G). Prove that $\text{stab}(a)$ is a subgroup of G,

9./ For $n \geq 3$, let $H = \{\beta \in S_n \mid \beta(1) = 1 \text{ or } 2$ and $\beta(2) = 1 \text{ or } 2\}$

Prove that H is a subgroup of S_n and determine $|H|$.