A <u>group</u> is a set G with a function

$$G \times G \longrightarrow G$$
$$(a,b) \longmapsto a \heartsuit b \quad \text{such that}$$

(a) If $g_1, g_2, g_3 \in G$ then

$$(g_1 \heartsuit g_2) \heartsuit g_3 = g_1 \heartsuit (g_2 \heartsuit g_3).$$

(b) There exists $\☺ \in G$ such that

if $g \in G$ then $\☺ \heartsuit g = g$ and $g \heartsuit \☺ = g$.

(c) If $g \in G$ then there exists $b \in G$

such that $g \heartsuit b = \☺$ and $b \heartsuit g = \☺$

A <u>subgroup</u> of G is a subset H of G

such that

(a) If $h_1, h_2 \in H$ then $h_1 \heartsuit h_2 \in H$.

(b) $\☺ \in H$.

(c) If $h \in H$ then $y \in H$

(remember $h \heartsuit y = \☺$ and $y \heartsuit h = \☺$).

A group G is <u>commutative</u>, or <u>abelian</u>, if

G satisfies

if $g_1, g_2 \in G$ then $g_1 \heartsuit g_2 = g_2 \heartsuit g_1$.

Let H and K be groups.

A homomorphism from H to K is a function $f: H \to K$ such that

(a) If $h_1, h_2 \in H$ then $f(h_1 \cdot h_2) = f(h_1) f(h_2)$,

(b) $f(1) = 1$,

(c) If $h \in H$ then $f(h^{-1}) = f(h)^{-1}$.

An isomorphism is a homomorphism $f: H \to K$ which is bijective.

The symmetric groups

$$S_1 = \{(1)\}, \quad S_2 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$$

$$S_3 = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \right.$$
$$\left. \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \right\}$$

The cyclic groups

$$C_1 = \{(1)\}, \quad C_2 = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \right\}$$

$$C_3 = \left\{ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \right\}$$

$$C_4 = \left\{ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{pmatrix} \right\}$$

The dihedral groups

$$D_3 = \left\{ \begin{pmatrix} 1&0&0\\0&1&0\\0&0&1 \end{pmatrix}, \begin{pmatrix} 0&0&1\\1&0&0\\0&1&0 \end{pmatrix}, \begin{pmatrix} 0&1&0\\0&0&1\\1&0&0 \end{pmatrix}, \begin{pmatrix} 0&0&1\\0&1&0\\1&0&0 \end{pmatrix}, \begin{pmatrix} 0&1&0\\1&0&0\\0&0&1 \end{pmatrix}, \begin{pmatrix} 1&0&0\\0&0&1\\0&1&0 \end{pmatrix} \right\}$$

$$D_4 = \left\{ \begin{pmatrix} 1&0&0&0\\0&1&0&0\\0&0&1&0\\0&0&0&1 \end{pmatrix}, \begin{pmatrix} 0&0&0&1\\1&0&0&0\\0&1&0&0\\0&0&1&0 \end{pmatrix}, \begin{pmatrix} 0&0&1&0\\0&0&0&1\\1&0&0&0\\0&1&0&0 \end{pmatrix}, \begin{pmatrix} 0&1&0&0\\0&0&1&0\\0&0&0&1\\1&0&0&0 \end{pmatrix}, \begin{pmatrix} 0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0 \end{pmatrix}, \begin{pmatrix} 0&0&1&0\\0&1&0&0\\1&0&0&0\\0&0&0&1 \end{pmatrix}, \begin{pmatrix} 0&1&0&0\\1&0&0&0\\0&0&0&1\\0&0&1&0 \end{pmatrix}, \begin{pmatrix} 1&0&0&0\\0&0&0&1\\0&0&1&0\\0&1&0&0 \end{pmatrix} \right\}$$

$C_k = \{c_0, c_1, \dots, c_{k-1}\}$ with $\{(1+j, 1), (2+j, 2), \dots, (k+j, k)\}$ being the positions of the 1's in c_j.

The group $\mathbb{C}^\times$

$\mathbb{C}^\times = \{\text{invertible elements in } \mathbb{C}\}$

$= \mathbb{C} - \{0\} = GL_1(\mathbb{C}) = \{(c) \mid c \neq 0\}$.

The group of n^{th} roots of unity

$\mu_n = \{ e^{2\pi i k/n} \mid k \in \{0, \dots, n-1\} \}$

$= \{ e^{0}, e^{2\pi i/n}, e^{2\pi i 2/n}, \dots, e^{2\pi i (n-1)/n} \}$

$= \{1, \zeta, \zeta^2, \dots, \zeta^{n-1}\}$ if $\zeta = e^{2\pi i/n}$

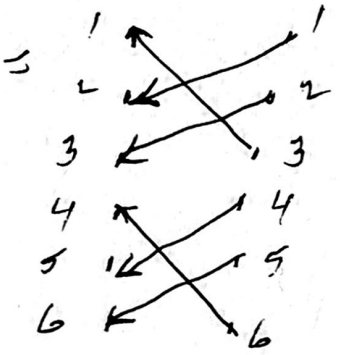
μ_n is a subgroup of $\mathbb{C}^\times$.

Let G be a group. Let $g \in G$

The <u>order</u> of the element is the smallest $k \in \mathbb{Z}_{>0}$ such that $g^k = 1$.

<u>Different notations for elements of S_n</u>

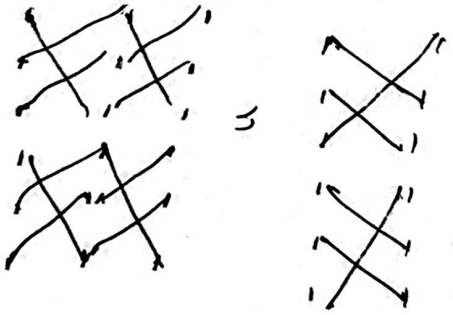
$$\begin{pmatrix} 0&0&1&0&0&0 \\ 1&0&0&0&0&0 \\ 0&1&0&0&0&0 \\ 0&0&0&0&0&1 \\ 0&0&0&1&0&0 \\ 0&0&0&0&1&0 \end{pmatrix} = \begin{pmatrix} 1&2&3&4&5&6 \\ 2&3&1&5&6&4 \end{pmatrix}$$ two line notation

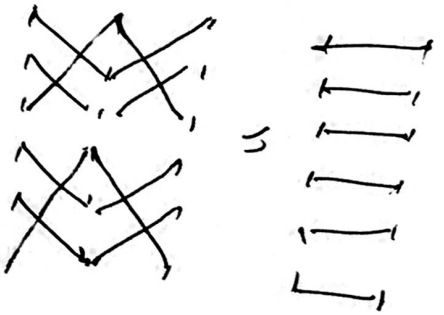
$=$ 

function notation

$= (123)(456)$ cycle notation

$= [231564]$ one line notation

$x^2 = xx =$  $=$

$x^3 = x^2 \cdot x =$ 

So $\text{order}(x) = 3$.