Generating Sets and Cayley Graphs

Def: Let G be a group and $S \subseteq G$ a subset.
The subgroup $\langle S \rangle$ generated by S is
$$\langle S \rangle = \{ s_1 s_2 \cdots s_r \mid r \geq 1 \text{ and } s_1, \ldots, s_r \in S \} \cup \{e\}$$
We say S is a generating set for G or S generates G if $G = \langle S \rangle$.

Notation: $\langle s_1, \ldots, s_r \rangle = \langle \{ s_1, \ldots, s_r \} \rangle$

Ex: S_3 is generated by $\{(12), (23)\}$ because

$(12)(23) = (123)$ Combined with e,
$(23)(12) = (132)$ this is all the elements!
$(12)(23)(12) = (13)$

Ex: S_n is generated by $S = \{ (jk) \mid j, k \in \{1, 2, \ldots, n\} \}$

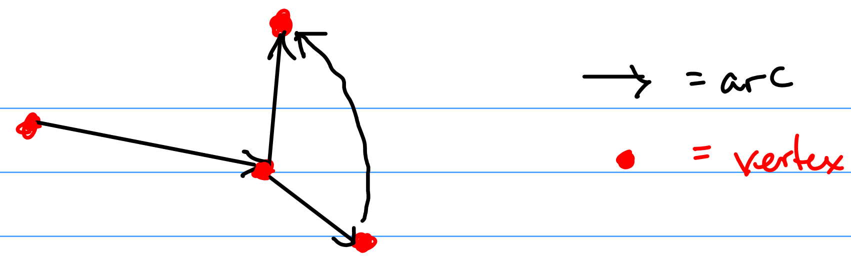
Def: Elements of the form (jk) are called transpositions.

Ex: The group of symmetries of a square is generated by the matrices $R = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ and $S = \begin{bmatrix} -1 & 0 \\ 0 & 0 \end{bmatrix}$.

We can draw a picture of a group G with a generating set S using a Cayley digraph.

Def: A directed graph or digraph is a collection of vertices connected together with directed edges called arcs.

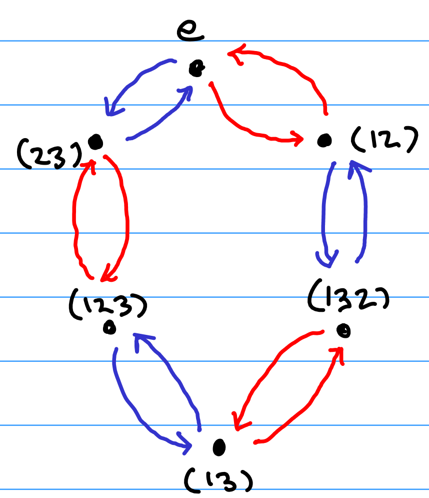
Ex:



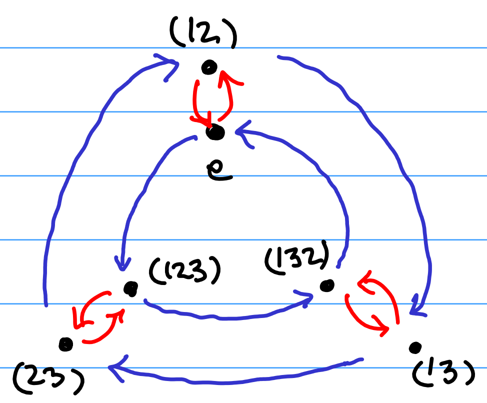
In general these can be decorated with various colors, symbols, line styles, etc. to improve understanding.

Def: The <u>Cayley digraph</u> $X(G,S)$ associated to a group G with generating set S has vertices given by the elements of G. There is an arc from vertex a to vertex b if and only if $ba^{-1} \in S$.

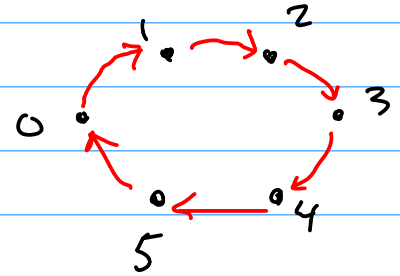
Ex: $G = S_3$, $S = \{(12), (23)\}$



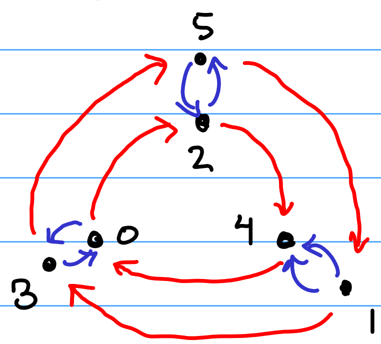
Ex: $G = S_3$, $S = \{(12), (123)\}$



Ex: $G = \mathbb{Z}_6$, $S = \{1\}$



Ex: $G = \mathbb{Z}_6$, $S = \{2, 3\}$



Compare with S_3 above!

Q: How can we tell if a group is Abelian from its Cayley graph?

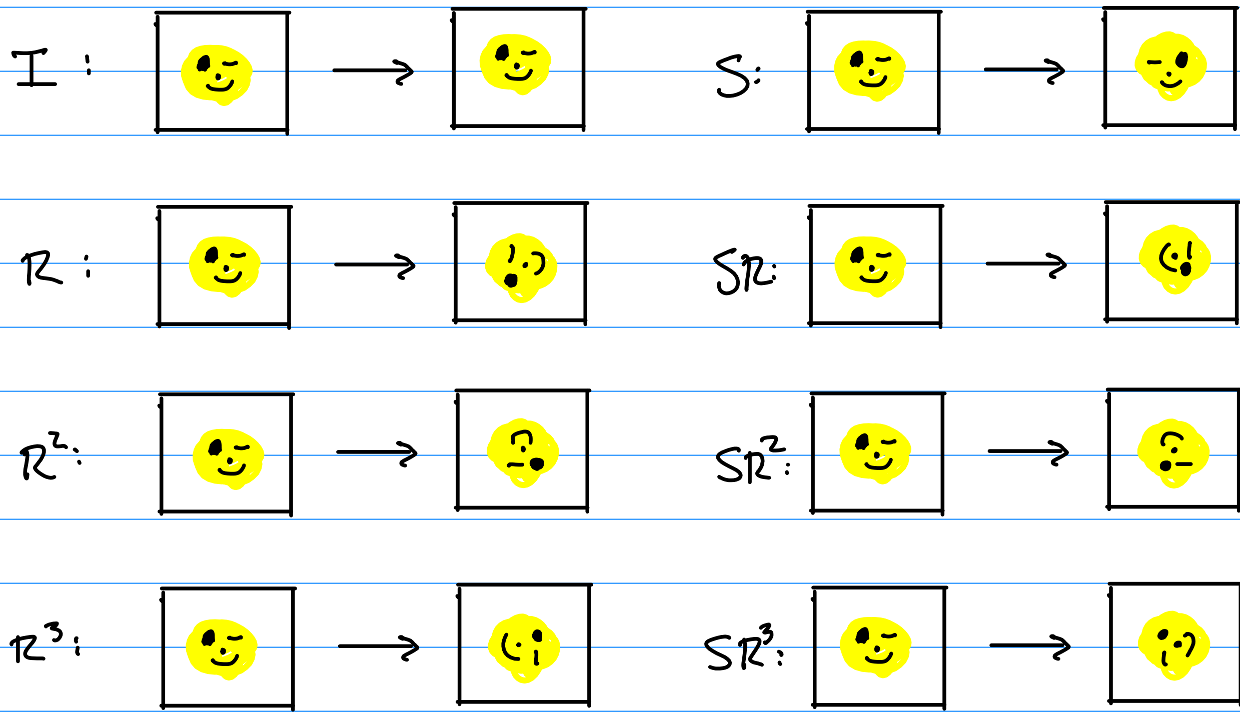
Structure of Groups

Goal: Try to view (finite) groups in some uniform way.

Cayley's Theorem: Every finite group is isomorphic to a subgroup of S_n for some n.

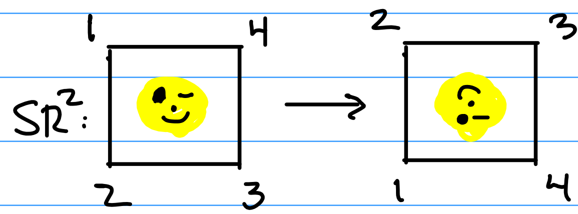
Def: A subgroup of S_n is called a permutation group.

Ex: The group of symmetries of the square has the following 8 elements.



If we label the corners, we can see that each map defines a permutation of $\{1,2,3,4\}$

<u>Ex:</u>



$\longleftrightarrow \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$

$= (12)(34)$

In this way, we identify

$I \longleftrightarrow e$	$S \longleftrightarrow (14)(23)$
$R \longleftrightarrow (1234)$	$SR \longleftrightarrow (13)$
$R^2 \longleftrightarrow (13)(24)$	$SR^2 \longleftrightarrow (12)(34)$
$R^3 \longleftrightarrow (1432)$	$SR^3 \longleftrightarrow (24)$

<u>Def</u>: A function $f: G \to \tilde{G}$ satisfying $f(a * b) = f(a) \,\tilde{*}\, f(b)$ is called a <u>group homomorphism</u>.

More specifically:

injective group homomorphism = <u>monomorphism</u>
surjective group homomorphism = <u>epimorphism</u>
bijective group homomorphism = <u>isomorphism</u>.

Anatomy of a homomorphism:

$$f : G \to \tilde{G}$$

codomain $\geq$ image

kernel $\leq$ domain

<u>Def</u>: The <u>kernel</u> and <u>image</u> of f are (respectively)

$$\ker f = \{ g \in G \mid f(g) = \tilde{e} \} = f^{-1}(\tilde{e}).$$
$$\operatorname{img} f = \{ f(g) \mid g \in G \} = f(G)$$

<u>Theorem</u>: These are both subgroups

> <u>Cayley's Theorem</u>: If G is a finite group, then there exists an integer $n > 0$ and a monomorphism $f : G \to S_n$. In particular, G is isomorphic to the permutation group $\operatorname{img}(f) \leq S_n$.

Now it makes a <u>lot</u> of sense to study permutations!

<u>Proof of Cayley's Theorem</u>: Let $G = \{ g_1, \ldots, g_n \}$. Then for each j, k there exists a unique integer $\sigma(j,k) \in \{1, 2, \ldots, n\}$ with $g_j g_k = g_{\sigma(j,k)}$.

Note $\sigma_j : k \mapsto \sigma(j,k)$ is a permutation of $\{1, 2, \ldots, n\}$

because if $g_\ell = g_j^{-1}$, then $g_{\sigma(\ell, \sigma(j,k))} = g_\ell g_{\sigma(j,k)} = g_\ell g_j g_k = g_k$

and therefore σ_ℓ is the inverse of σ_j.

Can easily check $g_i \mapsto \sigma_i$ is a monomorphism $\square$

Properties of Permutations

(1) Each $\sigma \in S_n$ may be written as a product of disjoint cycles uniquely, up to the order of the product

(2) Each $\sigma \in S_n$ can be written as a product of transpositions (not uniquely!)

(3) If $\sigma = (a_0 a_1)(a_2 a_3) \dots (a_{2j} a_{2j+1})$
and $\sigma = (b_0 b_1)(b_2 b_3) \dots (b_{2k} b_{2k+1})$
then $j = k \mod 2$.

Def: The *parity* of a permutation is *even* if it can be written as a product of an even # of transpositions. Otherwise it is *odd*. The *sign* is

$$\operatorname{sgn}(\sigma) = \begin{cases} 1, & \sigma \text{ even} \\ -1, & \sigma \text{ odd} \end{cases}$$

Theorem: The map $\operatorname{sgn}: S_n \longrightarrow U_2 = \{\pm 1\}$ is a group homomorphism.

Def: The kernel of sgn is the *alternating group* A_n