Week 4

Example. $V = \{e, a, b, c\}$

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

$$\begin{aligned} &< a >= \{e, a\} \\ &< b >= \{e, b\} \\ &< c >= \{e, c\} \\ &< a, b >= \{\text{finite products of powers of } a \text{ and } b\} \\ &\qquad\quad = \{e, a, b, c\} \end{aligned}$$

Defn. (Generators)

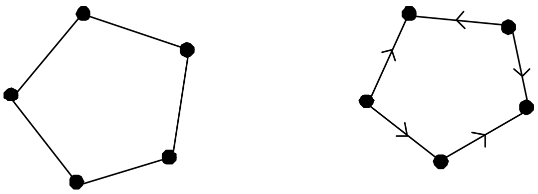
Let G be a group and let $a_i \in G$ for $i \in I$. The smallest subgroup of G containing $\{a_i | i \in I\}$ is the subgroup generated by $\{a_i | i \in I\}$, i.e., the subgroup which contains all the finite products of powers of a_i where $i \in I$. The subgroup H of G generated by $\{a_i | i \in I\}$ is denoted by $< \{a_i | i \in I\} >$ and $\{a_i | i \in I\}$ is the set of generators of H. If $|I| < +\infty$, then H is finitely generated and $H =< a_1, a_2, \cdots, a_t >$ for some t.

e.g. $H =< \{a_1, a_2\} >$

$$[(a_1)^3 (a_2)^2 (a_1)^{-7}]^{-1} = {a_1}^7 {a_2}^{-2} {a_1}^{-3}$$

Note: $(ab)^{-1} = b^{-1} a^{-1}$.

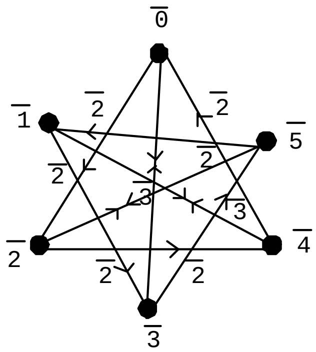
Defn. A graph consists of a set of "vertices" and some "edges" joining vertices. A diagraph (directed graph) consists of a set of "vertices" and some "arcs" (directed edge) joining vertices.



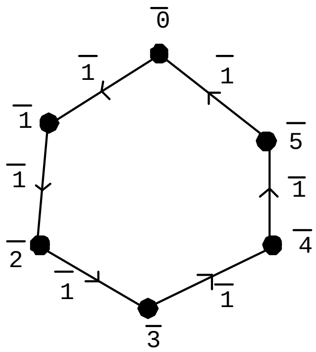
Graph Digraph

Defn. Let G be a group with generating set $A = \{a_1, a_2, \cdots, a_t\}$. A Cayley "color" graph of G with respect to A is denoted by $D_A(G)$ where the vertex set of $D_A(G)$ is G and (g_1, g_2) is an *arc* of $D_A(G)$ if and only if $g_2 = g_1 a_i$ for some $a_i \in A$. Moreover, the *arc* (g_1, g_2) is colored by a_i.

$\mathbb{Z}_6 =< \bar{2}, \bar{3} >$



$\mathbb{Z}_6 =< \bar{1} >$



Note: The diagraph is connected, i.e., we can get from any vertex

g_i to any vertex g_j by travelling along consecutive *arcs*, starting at g_i and ending at g_j.

Defn. (Permutation)

A permutation of a set A is a bijection from A onto itself. Denote a permutation of A by S_A. If A is a finite set which has n elements, then S_A is also denoted by S_n.

Theorem S_n is a group with operation "function composition $\circ$".

Proof. Verify yourself.

Notation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}$ is a permutation of S_5.

Let $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}$.

Then $\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}$

$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix} = (1\ 5\ 4\ 2)(3) \leftarrow$ Cycle representation.

Fact: $|S_n| = n!$

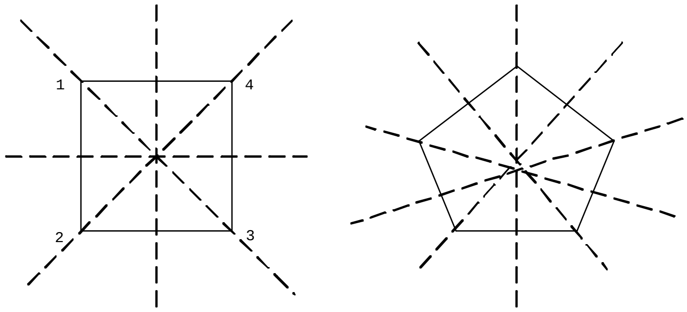
Fact: S_3 is not an abelian group.

$$S_3 = \{\rho_0, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\}$$
$$= \{e, (123), (132), (23)(1), (13)(2), (12)(3)\}$$
$$\rho_1\mu_1 = \mu_3,\ \mu_1\rho_1 = \mu_2.\ (?)$$

Example. $D_n = \{\rho_0, \rho_1, \rho_2, \cdots, \rho_{n-1}, \mu_1, \mu_2, \cdots, \mu_n\}$

ρ_i: Rotating $\dfrac{360i}{n}$ degree counterclockwise.

μ_j: Symmetric reflection.



Example. $D_4 = \{\rho_0, \rho_1, \rho_2, \rho_3, \mu_1, \mu_2, \delta_1, \delta_2\}$

$$= \{e, (1234), (13)(24), (1432), (12)(34), (14)(23), (13), (24)\}.$$

Example. $\{\rho_0, \rho_1, \rho_2, \rho_3\} \leq D_4,\ \{\rho_0, \mu_1\} \leq D_4,\ \{\rho_0, \delta_1\} \leq D_4.$

Theorem (Cayley's Theorem)

Every group is isomorphic to a group of permutations.

Proof. Let G be a group. We claim that G is isomorphic to a subgroup of S_G.

Claim: If φ is a monomorphism from a group G_1 into a group G_2, then $\varphi[G_1] \leq G_2$ where $\varphi[G_1] = \{\varphi(g) | g \in G_1\}$.

Consider $\varphi' : G_1 \to \varphi[G_1]$ where $\varphi'(g) = \varphi(g)\ \forall\ g \in G_1$. Then φ' is an isomorphism. Thus $\varphi[G_1] \leq G_2$.

Therefore, the proof follows by defining a monomorphism from G into S_G.

For each $x \in G$, let λ_x be the mapping from G into G such that $\lambda_x(g) = xg\ \forall\ g \in G$. Then λ_x is a permutation of G.(Check) Now, define $\psi : G \to S_G$ by $\psi(x) = \lambda_x$.

Claim: ψ is a monomorphism from G into S_G.

(1) ψ is 1-1. $\forall\ x, y \in G$, let $\psi(x) = \psi(y)$, then $\lambda_x = \lambda_y$, hence $\forall g \in G,\ \lambda_x(g) = \lambda_y(g)$, hence $xg = yg$ which implies that $x = y$.

(2) ψ is a homomorphism. $\forall\ x, y \in G,\ \psi(xy) = \lambda_{xy}$. Since $\forall\ g \in G,\ \lambda_{xy}(g) = xy(g) = x(yg) = x(\lambda_y(g)) = \lambda_x(\lambda_y(g)) = \lambda_x\lambda_y(g),\ \lambda_{xy} = \lambda_x\lambda_y$. This concludes the proof (2) and the claim.

We have the proof.

Note $\lambda_x(g) = xg$ is called a left regular representation. The proof can also be done by using the right regular representation $\rho_x(g) = gx$. In that case, "$\psi(x) = \rho_{x^{-1}}$" is used.