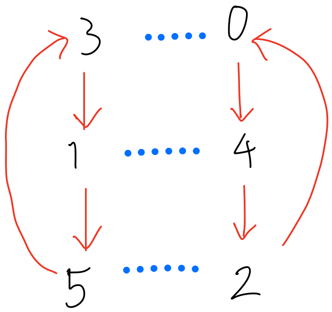
Generators & Cayley diagrams Part II

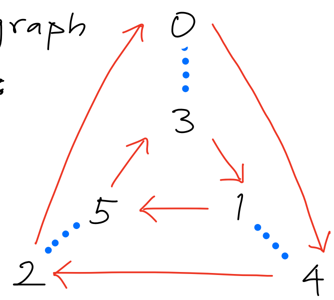
(Part I is in Day 2 notes)

Ex (Copied from Day 2 notes)

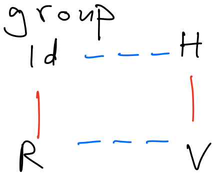
The Cayley diagram for $\mathbb{Z}_6$ w/ generating set $S = \{\underset{f}{3}, \underset{R}{4}\}$



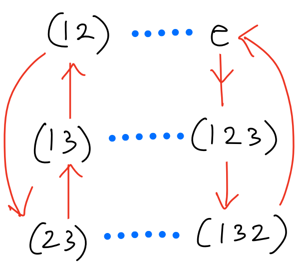
The same graph rearranged:



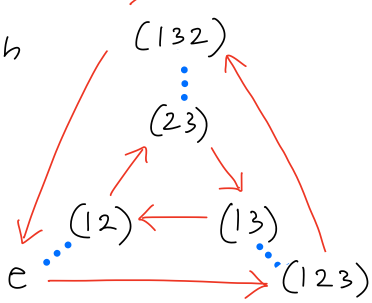
Ex Cayley diagram for rectangle mattress group w/ generating set $S = \{H, R\}$:



Ex Cayley diagram for generating set $\{\underset{f}{(12)}, \underset{R}{(123)}\}$ of S_3

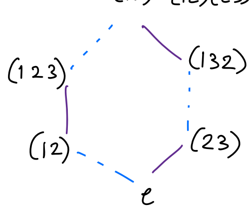


The same graph rearranged:



Ex Cayley diagram for generating set $\{(12), (23)\}$ of S_3

$(13) = (12)(23)(12) = (23)(12)(23)$

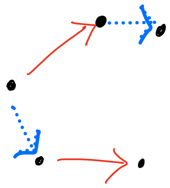


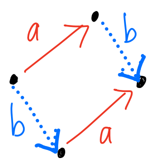
$(23)(12)$

Note A Cayley diagram can be used as a "group calculator".
Start at e, then chase the sequence through the Cayley graph.

Ex What is $RRfRRRRf$ equal to? Ans: (123)
What is $RRfRRRRfR^{-1}$ equal to? Ans: e

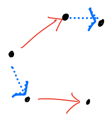
Fact To check that a group G is abelian, it suffices to check that $ab=ba$ for all generators of G. (Why?)

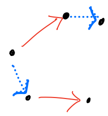
① The pattern  never appears in the Cayley graph of an abelian group

② The pattern 

tells us $ab=ba$

Ex • $\mathbb{Z}_6$ and the rectangle mattress group are abelian,

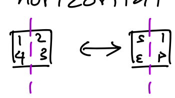
and pattern  doesn't appear

• S_3 is not abelian, and pattern  does appear

in both Cayley diagrams w/ $S=\{(12),(123)\}$
and w/ $S=\{(12),(23)\}$

• Exercise: Draw the Cayley diagram for

∗ D_4 using $S=\{R,f\}$ where $R=Rot(90°)$, f: horizontal flip



∗ $\mathbb{Z}_8$ using $S=\{3\}$

Note We can use a Cayley diagram to "see" the cyclic subgroup $\langle x \rangle$ generated by an elt x.

Draw the path from e to x, then repeat the same path until we return to e.

Notation For this visual reason, we will refer to $\langle x \rangle$ as the <u>orbit of x</u>.

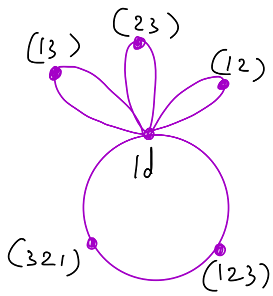
Ex The orbit of (132) is $\langle (132) \rangle = \langle R^2 \rangle = \{e, R^2, R\} = \{e, (132), (123)\}$

The orbit of (13) is $\langle (13) \rangle = \langle \underset{\overset{\|}{fR^2}}{Rf} \rangle = \{e, Rf\} = \{e, (13)\}$

We can visualize these orbits in an "orbit graph":

* Every elt will be part of at least one orbit
* Each cycle represents an orbit

Ex The orbit graph of S_3:



S_3 has five distinct orbits (including $\{Id\}$)

Dihedral groups, again

See Day 1 & Day 2 notes for earlier intro to D_n

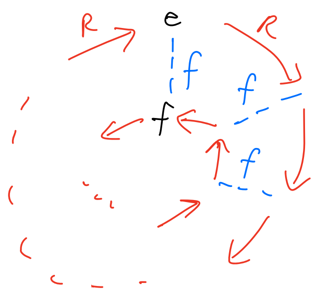
Let $n \geq 3$.

D_n = group of symmetries of a regular n-gon ($n \geq 3$)

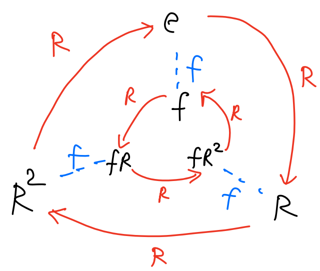
Prop Let R denote the counterclockwise rotation by $\frac{2\pi}{n}$,

and f any reflection across a line of symmetry.

① The Cayley diagram of D_n w/ $S = \{f, R\}$ is



Ex for D_3:



② From part (1), we see that

$$D_n = \{ Id, R, R^2, \ldots, R^{n-1},$$ — rotations (including Id)

reflections/flips — $$f, fR, fR^2, \ldots, fR^{n-1} \}$$

where the items on the list are distinct.

③ The powers of R are rotations, and fR^i are reflections.

④ The order of R is n, so $R^{-1} = R^{n-1}$ & $R^{-i} = R^{n-i}$

The order of each reflection is 2,

so $$Rf = (Rf)^{-1} = f^{-1}R^{-1} = fR^{-1}$$

These are often called "relations"

So $\boxed{Rf = fR^{-1}}$ (equivalently $fRf = R^{-1}$)

Similarly, $\boxed{R^i f = fR^{-i}}$ (equivalently, $fR^i f = R^{-i}$)

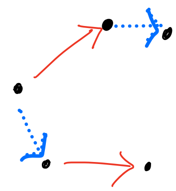
<u>Remark</u> Part ② of Prop above tells us that every element of D_n is a product of R and f.

We say D_n is generated by R and f.

<u>Prop</u> D_n is not abelian

<u>Proof</u> (using Cayley diagram)

It has a Cayley diagram w/ pattern



<u>Proof</u> (using remark)

$$f(fR) = (ff)R = R \quad \text{but} \quad (fR)f = (R^{n-1}f)f = R^{n-1}$$

Since $n \geq 3$, R and R^{n-1} are distinct.

$\square$

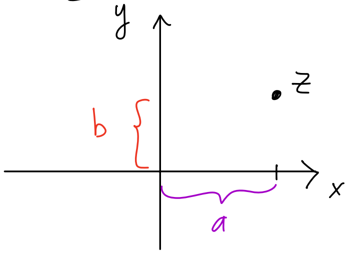
<u>Corollary</u> D_n is not cyclic.

Group of complex numbers

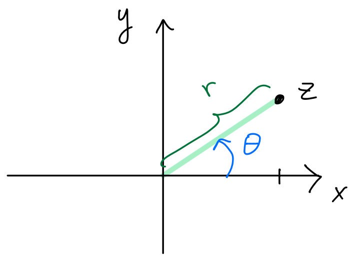
(Ch 2 Example 15, pg 47)

$\mathbb{C} = \{\text{complex numbers}\} = \{\underbrace{a}_{\text{real part}} + \underbrace{b}_{\text{imaginary part}} i : a, b \in \mathbb{R}\}$ where $i^2 = -1$

Cartesian / rectangular coordinates



polar coordinates



$$z = a + bi = r(\cos\theta + i\sin\theta) = re^{i\theta}$$

$r = |z| = \sqrt{a^2 + b^2}$,

called absolute value or modulus or magnitude of z

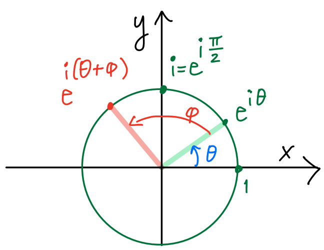
$a = r\cos\theta$

$b = r\sin\theta$

Thm ① $e^{i\theta} e^{i\varphi} = e^{i(\theta+\varphi)}$

② If $z = re^{i\theta}$ then $z^n = r^n e^{in\theta}$

③ $(Ae^{i\theta})(Be^{i\varphi}) = AB\, e^{i(\theta+\varphi)}$



Def $\mathbb{C}^* \overset{\text{def}}{=} \mathbb{C} \setminus \{0\}$ is a group w/ multiplication as group operation.

Identity: 1

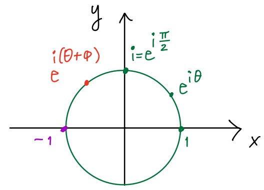
The inverse of $z = a + bi = Re^{i\theta}$ is $z^{-1} = \dfrac{a - bi}{a^2 + b^2} = \dfrac{1}{R} e^{-i\theta}$

Some subgroups of $\mathbb{C}^*$:

① $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$

② $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$

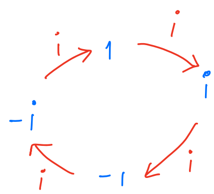
③ The circle group $\mathbb{T} \overset{\text{def}}{=} \{ z \in \mathbb{C} : |z| = 1 \}$

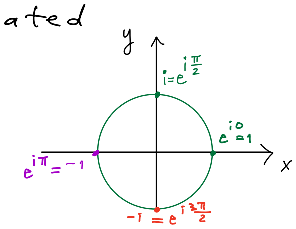


$\mathbb{T}$ contains $1, -1, i, -i, \frac{\sqrt{3}}{2} + \frac{1}{2} i = \cos(\frac{\pi}{6}) + i \sin(\frac{\pi}{6}) = e^{i\frac{\pi}{6}}$

All of these subgroups above have infinite order

④ The subset $H = \{1, -1, i, -i\}$ of the circle group is a subgroup. It's a cyclic group generated by i or $-i$.





Note that each elt of H satisfies the equation $z^4 = 1$

<u>Def / Thm</u> If $n \geq 2$, the <u>n-th roots of unity</u> are the complex numbers satisfying the equation $z^n = 1$.

$$\{ n\text{-th roots of unity} \} = \{ e^{i\frac{2\pi k}{n}} : k = 0, 1, 2, \dots, n-1 \}$$

The n-th roots of unity form a cyclic group of $\mathbb{T}$ of order n. A generator for this group is called a <u>primitive n-th root of unity</u>.

<u>Ex:</u> $\{ 5\text{th roots of unity} \} = \{ 1, e^{i\frac{2\pi}{5}}, e^{i\frac{4\pi}{5}}, e^{i\frac{6\pi}{5}}, e^{i\frac{8\pi}{5}} \}$

All 5-th roots of unity (except 1) is primitive.

<u>Ex:</u> i and $-i$ are primitive 4 th roots of unity.

Terminology for functions

Def Let $f : \overset{\text{domain}}{A} \to \overset{\text{codomain}}{B}$ be a function.

* The *image* of f, denoted $\operatorname{Im} f$ or $f(A)$ is the subset $\{f(a) : a \in A\}$ of B

(Some textbooks refer to $f(A)$ as the *range* of f)

* f is *injective* (or one-to-one) if : $f(a_1) = f(a_2)$ implies $a_1 = a_2$

* f is *surjective* (or onto) if :

for each $b \in B$, there is at least one $a \in A$ s.t $f(a) = b$.

* Let $C \subset B$.

— The *preimage* of C under f, denoted $f^{-1}(C)$ is the subset $\{a \in A : f(a) \in C\}$ of A.

— When C is a singleton set $C = \{b\}$, the preimage $f^{-1}(\{b\}) = \{a \in A : f(a) = b\}$ is called the *fiber* of b under f.

Homomorphisms Part I

Ch 10, pg 194-195
only for now

Def Let $(G, *)$ and $(H, \square)$ be groups.

A (group) homomorphism is a function

\phi $\quad$ domain $\quad$ codomain

$\varphi : G \longrightarrow H$ such that

$$\varphi(\underbrace{g_1 * g_2}_{\text{operation in } G}) = \varphi(g_1) \underbrace{\square}_{\text{operation in } H} \varphi(g_2) \quad \text{for all } g_1, g_2 \in G.$$

* If the homomorphism is also a bijection, then φ is called an isomorphism and we write $G \cong H$ and say G is isomorphic to H.

* An isomorphism from G to itself is called an automorphism of G.

* The kernel of φ is $\varphi^{-1}(\{e_H\}) = \{g \in G : \varphi(g) = e_H\}$
  - Notation: $\operatorname{Ker} \varphi$

Thm Let $\varphi : G \to H$ be a homomorphism of groups. Then φ sends e_G to e_H

Proof $e_H \, \varphi(e_G) = \varphi(e_G)$ since e_H is the identity elt in H and $\varphi(e_G) \in H$

$= \varphi(e_G e_G)$ since e_G is the identity elt in G

$= \varphi(e_G)\, \varphi(e_G)$ since φ is a homomorphism

So $e_H \, \varphi(e_G) = \varphi(e_G)\, \varphi(e_G)$

By the right cancellation property of groups (Ch 2) we have $e_H = \varphi(e_G)$. $\square$

Ex: Consider the map $\phi : \mathbb{C}^* \to \mathbb{C}^*$

defined by $\phi(z) = z^4$

a) Prove that ϕ is a homomorphism

Proof: For all complex numbers $a, b \in \mathbb{C}^*$,

$\phi(ab) = (ab)^4$

$= a^4 b^4$ since the multiplication of complex numbers is commutative

$= \phi(a)\,\phi(b)$

b) $\ker \phi \overset{\text{def}}{=} \{ z \in \mathbb{C}^* : \phi(z) = 1 \}$

$= \{ z \in \mathbb{C}^* : z^4 = 1 \}$

$= \{ 4\text{th roots of unity} \}$

$= \{ 1, e^{i\frac{\pi}{2}}, e^{i2\frac{\pi}{2}}, e^{i3\frac{\pi}{2}} \}$

$= \{ 1, i, -1, -i \}$

Ex $\varphi : \mathbb{Z} \longrightarrow D_4$ defined by

$k \longmapsto R^k$ where R is a rotation by $\frac{2\pi}{4}$ in D_4

is a homomorphism which is not injective and not surjective.

Proof

* φ is a homomorphism: For all $k, l \in \mathbb{Z}$, we have

$$\varphi(k+l) = R^{k+l} = R^k R^l = \varphi(k)\varphi(l).$$

* It's not injective, e.g. $\varphi(2) = R^2 = R^4 R^2 = R^6 = \varphi(6)$ but $2 \neq 6$ in $\mathbb{Z}$.
* It's also not surjective: $\varphi(\mathbb{Z})$ doesn't contain any reflection. $\square$

Note $\ker \varphi = 4\mathbb{Z} = \{\ldots, -4, 0, 4, 8, \ldots\}$

$\operatorname{Im} \varphi = \{$ Rotations by $0, \frac{\pi}{2}, \pi, \frac{3\pi}{2} \}$

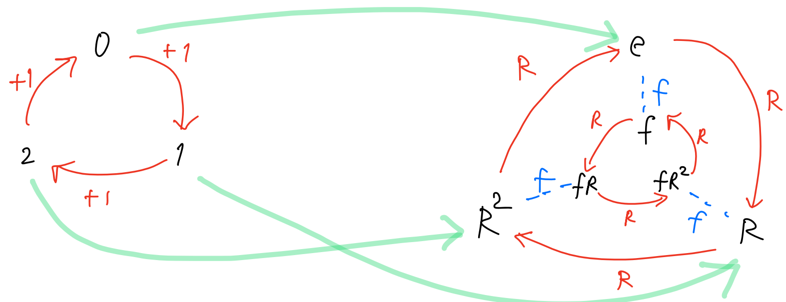
Ex $\varphi : \mathbb{Z}_3 \longrightarrow D_3$ defined by

$$k \longmapsto R^k \quad \text{where } R \text{ is a rotation by } \frac{2\pi}{3} \text{ in } D_3$$

is an injective homomorphism which is not surjective.

Visualization

$\mathbb{Z}_3 = \langle 1 \rangle$ $\qquad\qquad$ $D_3 = \langle R, f \rangle$ — one of the flips



$0 \mapsto e$

$1 \mapsto R$

$2 \mapsto R^2$

Remark D_3 contains a subgroup $\langle R \rangle = \{e, R, R^2\}$ which is "identical in structure" to $\mathbb{Z}_3$.

We say "the structure of $\mathbb{Z}_3$ shows up in D_3".

We say "$\mathbb{Z}_3$ embeds into D_3 as a subgroup".

Def An injective homomorphism is also called an embedding

Ch 6 isomorphisms

In Ch 5, we said that ..

- every cyclic group of infinite order behaves like $\mathbb{Z}$
- every cyclic group of order n behaves like $\mathbb{Z}_n$

Now we say every cyclic group is isomorphic to $\mathbb{Z}$ or $\mathbb{Z}_n$

Thm Suppose $G = \langle a \rangle$ is a cyclic group.

(Ex 2) If $|a| = \infty$ then $\varphi: \mathbb{Z} \to G$, $k \mapsto a^k$

is an isomorphism.

Proof $\varphi(k+l) = a^{k+l} \overset{\text{exponent laws}}{=} a^k a^l = \varphi(k)\varphi(l)$

So φ is a homomorphism.

To show φ is injective: Let $\varphi(k) = \varphi(l)$

Then $a^k = a^l$

$a^k a^{-l} = e$

$a^{k-l} = e$

Since a is of infinite order, $k-l$ must be 0, so $k=l$. $\square$

To show φ is surjective: Every elt of G is of the form a^k for some $k \in \mathbb{Z}$,

so $\varphi(k) = a^k$.

Ex $U(9) = \{1, 2, 4, 5, 7, 8\} = \langle 2 \rangle$

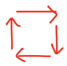
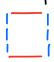
Since the order of 2 in $U(9)$ is 6,

$U(9) \cong \mathbb{Z}_6$.

Def $V_4 = \{e, a, b, c\}$ is the group w/ multiplication (Cayley) table

	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Thm Up to isomorphism, there are two groups of order 4, $\mathbb{Z}_4$ and V_4.

Ex Other groups isomorphic to $\mathbb{Z}_4$:

* $\{Id, R, R^2, R^3\} \leq D_4$
  Rot(90°)
* $\{Id, (1263), (16)(23), (3621)\} = \langle (1263) \rangle = \langle (3621) \rangle$ from Quiz 03
* $U(5) = \{1, 2, 3, 4\} = \langle 2 \rangle = \langle 3 \rangle$ from Quiz 02

Other groups isomorphic to V_4:

* the rectangle mattress group from Day 1
* $U(8)$
* $U(12)$
* $\{Id, R, f, fR^2\} \leq D_4$
  Rot(90°) any flip
* $\{Id, (12)(34), (13)(24), (14)(23)\} \leq S_4$

Thm $\mathbb{Z}_4$ is not isomorphic to V_4

Pf Suppose $\mathbb{Z}_4 \to V_4$ is an isomorphism.

Case $\varphi(1) = e$: Then $\varphi(2) = \varphi(1+1) = \varphi(1)\varphi(1) = ee = e = \varphi(1)$.

Having $\varphi(2) = \varphi(1)$ means φ is not injective.

So $\varphi(1) \neq e$.

Case $\varphi(1) \neq e$: Then $\varphi(1) = x$ where $x = a, b,$ or c.

Then
$$\begin{aligned} \varphi(3) &= \varphi(1+1+1) \\ &= \varphi(1)\varphi(1)\varphi(1) \\ &= x^3 = x^2 x \\ &= x \quad \text{since } |x| = 2 \\ &= \varphi(1) \end{aligned}$$

Having $\varphi(3) = \varphi(1)$ means φ is not injective.

In both cases, φ is not a bijection.

So there is no isomorphism from $\mathbb{Z}_4$ to V_4

— end of PDF —