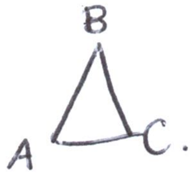
MATH 2020 Lecture 6

Symmetries

A symmetry of a geometric figure is a rearrangement of the figure preserving the arrangement of its sides and vertices, as well as distances and angles.

A rigid motion is a map from $\mathbb{R}^2$ to itself preserving the symmetry of some object.

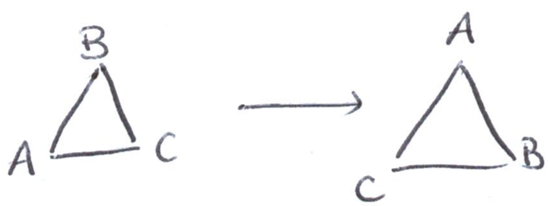
For example, consider the equilateral triangle



We can transform it in a number of ways using symmetry / rigid motions.

$\boxed{\text{permutation of vertices}}$

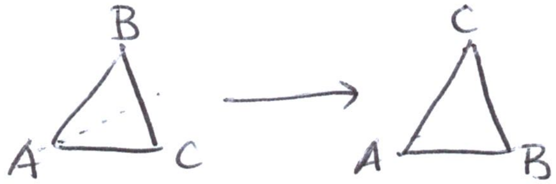
identity, $id = \begin{pmatrix} A & B & C \\ A & B & C \end{pmatrix}$



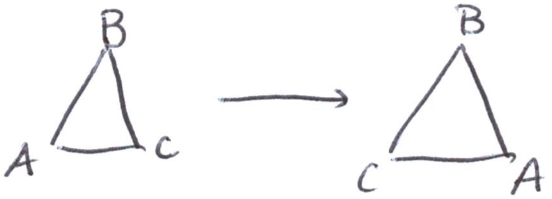
rotation $\rho_1 = \begin{pmatrix} A & B & C \\ B & C & A \end{pmatrix}$

rotation $\rho_2 = \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix}$

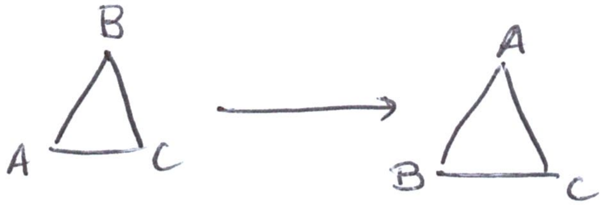
Also three reflections:



reflection $\mu_1 = \begin{pmatrix} A & B & C \\ A & C & B \end{pmatrix}$



reflection $\mu_2 = \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}$



reflection $\mu_3 = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$.

We can make a "multiplication" on the set $\{id, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\}$ of symmetries. Since each symmetry is also a <u>permutation</u> of the vertices, we can compose symmetries as functions. Define multiplication of symmetries π_1, π_2 by:

$$\pi_1 \cdot \pi_2 = \pi_1 \circ \pi_2$$

composition of functions.

So, for example,

$\mu_1 \cdot \rho_1 = \mu_1 \circ \rho_1$, and so

$\mu_1 \circ \rho_1 (A) = \mu_1 (B) = C$, $\quad \mu_1 \circ \rho_1 (C) = \mu_1 (A) = A$.

$\mu_1 \circ \rho_1 (B) = \mu_1 (C) = B$, So $\mu_1 \cdot \rho_1$ "is" the permutation $\begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}$,

which is μ_3. So $\mu_1 \cdot \rho_1 = \mu_3$ in our "multiplication" on the set $\{id, \rho_1, \rho_2, \mu_1, \mu_2, \mu_3\}$. In general, we can make a whole multiplication table for this set:

	id	ρ_1	ρ_2	μ_1	μ_2	μ_3
id						
ρ_1				μ_3		
ρ_2						
μ_1		μ_2				
μ_2						
μ_3						

to see the rest go to page ~~#~~ 43.

So $\mu_1 \rho_1 \neq \rho_1 \mu_1$, a new kind of multiplication since it is not commutative.

Integers modulo n (with addition!) and symmetries of a shape are instances of a general structure called a group.

Definition: A binary operation on a set G is a function $G \times G \longrightarrow G$ that assigns an element $a \circ b$ to each pair $(a, b) \in G \times G$.

Definition: A group is a set G and a binary operation $(a,b) \longmapsto a \cdot b$ satisfying

(i) The binary operation is associative, so
$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

(ii) There exists an element $e \in G$, called the identity, satisfying
$$e \cdot a = a \cdot e = a \quad \text{for all } a \in G.$$

(iii) For each element $a \in G$, there exists an inverse element of G, denoted a^{-1}, which satisfies
$$a \cdot a^{-1} = a^{-1} \cdot a = e.$$

A group with the property that $a \cdot b = b \cdot a$ for all $a, b \in G$ is called abelian, a group without this property is nonabelian (alternatively, commutative / non-commutative).

Example: $\mathbb{Z}_n$ with addition as the binary operation is a group. However, $\mathbb{Z}_n$ with multiplication is not a group. An element $a \in \mathbb{Z}_n$ has a multiplicative inverse iff $\gcd(a,n) = 1$. So if n is not prime, then ~~and~~ any divisor d

of n will not have an inverse. What if
n is prime?

A "multiplication table" for a group is called
a Cayley table.

Start here.

Example: If we take $\mathbb{Z}_n$ with multiplication, then:
the operation is associative; however it is not a group.
There is an identity:

$$1 \cdot k = k \cdot 1 = k \mod n \text{ for all } 0 \leq k \leq n-1,$$

but some elements have no inverses. For example
0 has no inverse since

$0 \cdot k = k \cdot 0 = 0$, so we can't multiply anything by 0 to get 1.

Also divisors, like $2 \in \mathbb{Z}_6$. Then:

$$\begin{array}{ll} 2 \cdot 0 = 0 & 2 \cdot 5 = 4 \\ 2 \cdot 1 = 2 & 2 \cdot 4 = 2 \\ 2 \cdot 2 = 4 & 2 \cdot 3 = 0 \end{array}$$

so 2 has no inverse. But since $k \in \mathbb{Z}_n$ will
have an inverse iff $\gcd(k,n) = 1$, we know
which "problem elements" we must discard in

order to obtain a group. Set

$$U(n) = \{[k] \in \mathbb{Z}_n \mid \gcd(k,n) = 1\}.$$

Then $U(n)$ is a group, called the <u>group of units</u> of $\mathbb{Z}_n$.

For example, here is $U(8)$:

$$U(8) = \{\cancel{0}, 1, \cancel{2}, 3, \cancel{4}, 5, \cancel{6}, 7, \cancel{8}\}$$
$$= \{1, 3, 5, 7\}.$$

With Cayley table:

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

MATH 2030 Lecture 7

Examples of groups.

<u>Example</u>: Let $M_n(\mathbb{R})$ be the set of $n \times n$ matrices with real entries, and $GL_n(\mathbb{R})$ the subset of invertible $n \times n$ matrices.

Since the product of two invertible matrices is invertible, matrix multiplication provides a binary operation

$$GL_n(\mathbb{R}) \times GL_n(\mathbb{R}) \longrightarrow GL_n(\mathbb{R})$$
$$(A, B) \longmapsto AB.$$

Then we check:

(i) Matrix multiplication is associative (presumably you saw this in linear algebra)

(ii) There is an identity, namely

$$I = \begin{bmatrix} 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & 0 & & 0 \\ 0 & 0 & 1 & 0 & \ddots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \end{bmatrix} \in GL_n(\mathbb{R})$$

satisfies $AI = IA = A$.

(iii) Every $A \in GL_n(\mathbb{R})$ has an inverse, since $GL_n(\mathbb{R})$ is the set of <u>invertible</u> matrices, by definition.

Thus $GL_n(\mathbb{R})$ is a group (note it's <u>nonabelian</u>), since matrix mult. is <u>not</u> commutative.

Example: Set $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$. Then multiplication of complex numbers:

$$(a+ib)(c+id) = ac - bd + i(ad+bc)$$

makes $\mathbb{C}^*$ into a group. The identity is 1, and inverses are given by

$$(a+ib)^{-1} = \frac{a-ib}{a^2+b^2}.$$

A group is finite if it has a finite number of elements, sometimes it is said to be "of finite order", and "the order of G" is taken to mean the number of elements in G. E.g $|\mathbb{Z}_n| = n$.

Properties of groups:

Proposition: Every group has exactly one identity element.

Proof: Suppose e and e' are both identities, that is

$$ge = eg = g \quad \text{and} \quad ge' = e'g = g \quad \text{for all } g \in G.$$

If we take $g = e'$ and e the identity, then

$$ee' = e'$$

while reversing their roles gives $ee' = e$. So

$$e = ee' = e'.$$

Proposition: Every $g \in G$, G a group, has exactly one inverse.

Proof: Same as above: If g has two inverses, say h and h', then

$$h = he = h(gh') = (hg)h' = eh' = h'.$$

Proposition: If $g, h \in G$, G a group, then

$$(gh)^{-1} = h^{-1}g^{-1}.$$

Proof: Note that

$$(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1} = gg^{-1} = e$$

and $(h^{-1}g^{-1})(gh) = h^{-1}(g^{-1}g)h = h^{-1}h = e$,

meaning $h^{-1}g^{-1}$ is the inverse of gh.

Proposition: If G is a group and $g \in G$, then

$$(g^{-1})^{-1} = g.$$

Proof: Observe $(g^{-1})(g^{-1})^{-1} = e$. So

$$(g^{-1})^{-1} = e(g^{-1})^{-1} = gg^{-1}(g^{-1})^{-1} = ge = g.$$

Proposition: If G is a group and $a, b, c \in G$, then $ba = ca$ implies $b = c$, and $ab = ac \Rightarrow b = c$.

Proof:
$$ba = ca \Rightarrow ba(a^{-1}) = ca(a^{-1})$$
$$\Rightarrow be = ce$$
$$\Rightarrow b = c.$$

Similar for other cases.

As in the case of numbers, we define exponents

$$g^n = \underbrace{g \cdot g \cdot \cdots \cdot g}_{n \text{ times}}, \quad g^{-n} = \underbrace{g^{-1} \cdot g^{-1} \cdots g^{-1}}_{n \text{ times}}$$

The usual laws hold:

(i) $g^m \cdot g^n = g^{m+n}$

(ii) $(g^m)^n = g^{mn}$

But also

(iii) $(gh)^n = (g^{-1}h^{-1})^{-n}$, and $(gh)^n = g^n h^n$ if G is abelian

MATH 2020 Lecture 8

§ 3.3 Subgroups.

Sometimes a smaller group can sit inside a larger group. For example, $(\mathbb{Z}, +)$ is a group, but so is $(2\mathbb{Z}, +)$, where $2\mathbb{Z}$ = set of even integers.

Then $2\mathbb{Z} \subset \mathbb{Z}$ is an example of a <u>subgroup</u>.

<u>Definition</u>: If $(G, \circ)$ is a group, and H is a subset of G, then H is a subgroup of G if $(H, \circ)$ is a group.

(Here, we think of restricting the binary operation $G \times G \longrightarrow G$ to the subset $H \times H$, to get a map $H \times H \longrightarrow H$).

<u>Remark</u>: Every group G has at least two subgroups, namely $H = G$ (the whole group is a subset of itself)

$H = \{e\}$ (the group containing only the identity)

If we want to rule out these possibilities, we ask that H be a <u>nontrivial</u> $(H \neq \{e\})$ and <u>proper</u> $(H \neq G)$ subgroup.

<u>Example</u>: Consider $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$. Then $\mathbb{R}$, together with multiplication from the reals, is a group.

We saw last day that $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ with operation

$$(a+ib)(c+id) = ac - bd + i(ad+bc)$$

is also a group.

Then $\mathbb{R}^* \subset \mathbb{C}^*$ is a subgroup, since the restriction of complex multiplication to the subset $\mathbb{R}^*$ yields real multiplication, which makes $\mathbb{R}^*$ into a group.

I.e. If $a+ib,\ c+id \in \mathbb{R}^\times$ then $b = d = 0$

and $(a+ib)(c+id) = ac - bd + i(ad+bc)$

becomes $(a)(c) = ac$.

<u>Example</u>: We saw that $GL_n(\mathbb{R})$ with matrix multiplication is a group. Let $SL_n(\mathbb{R}) \subset GL_n(\mathbb{R})$ denote

$$SL_n(\mathbb{R}) = \{ A \in GL_n(\mathbb{R}) \mid \det(A) = 1 \}.$$

Then $SL_n(\mathbb{R})$, with matrix multiplication, is a subgroup of $GL_n(\mathbb{R})$. In particular note that

$\det(A) = 1$ and $\det(B) = 1 \Rightarrow \det(AB) = 1$

so $A, B \in SL_n(\mathbb{R}) \Rightarrow AB \in SL_n(\mathbb{R})$

and $\det(A) = 1 \Rightarrow \det(A^{-1}) = 1$, so

$A^{-1} \in SL_n(\mathbb{R})$.

So the binary operation

$$GL_n(\mathbb{R}) \times GL_n(\mathbb{R}) \longrightarrow GL_n(\mathbb{R})$$

restricts to

$$SL_n(\mathbb{R}) \times SL_n(\mathbb{R}) \longrightarrow SL_n(\mathbb{R})$$

and $SL_n(\mathbb{R})$ contains all of its inverses.

<u>Example</u>: Something we did not yet check is that $M_n(\mathbb{R})$, the set of $n \times n$ matrices with real entries, is a group with the operation of <u>matrix addition</u>.

Then observe that $GL_n(\mathbb{R}) \subset M_n(\mathbb{R})$ is <u>not</u> a subgroup. Restricting the binary operation

$$M_n(\mathbb{R}) \times M_n(\mathbb{R}) \longrightarrow M_n(\mathbb{R})$$

to $GL_n(\mathbb{R}) \times GL_n(\mathbb{R})$ does <u>not</u> give a map whose image is in $GL_n(\mathbb{R})$. For example, $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \in GL_n(\mathbb{R})$, but

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \notin GL_n(\mathbb{R}).$$

Thus $GL_n(\mathbb{R})$ is <u>not</u> a subgroup of $(M_n(\mathbb{R}), +)$.

<u>Example</u>: Suppose we take the set $\mathbb{Z}_2 \times \mathbb{Z}_2$, and define addition coordinate-wise:

$$(a,b) + (c,d) = (a+c, b+d).$$

Then $\mathbb{Z}_2 \times \mathbb{Z}_2$ becomes a group, the addition table is:

	(0,0)	(0,1)	(1,0)	(1,1)
(0,0)	(0,0)	(0,1)		
(0,1)	(0,1)	(0,0)	(1,1)	(1,0)
(1,0)		(1,1)		
(1,1)		(1,0)		

etc.

only fill out a few of these, refer to page 38 in text.

Then, for example,

$H_1 = \{(0,0), (0,1)\}$ is a subgroup and so is

$H_2 = \{(0,0), (1,0)\}$.

So a group can potentially have <u>many</u> <u>subgroups</u>

<u>Proposition</u>: A subset H of a group G is a subgroup if and only if it satisfies:

(i) The identity e of G is in H

(ii) If $h_1, h_2 \in H$ then $h_1 h_2 \in H$

(iii) If $h \in H$ then $h^{-1} \in H$.

<u>Proof</u>:

If H is a subgroup, then we first show these 3 things hold. Since H is a group in its own right, it has an identity e_H.

Then to show $e = e_H$, note two facts:

① $e_H e_H = e_H$, and

② $e e_H = e_H e = e_H$, since $e \in G$ is identity.

So in fact $e_H e_H = e e_H$, so $e = e_H$ by right cancellation. So $e \in H$.

The second condition holds since H is a group.

The third is a consequence of uniqueness of inverses, namely: If $h' \in H$ is the inverse of $h \in H$, then $hh' = h'h = e$. But this means h' is also the inverse of $\underline{h \text{ in } G}$, so by uniqueness of inverses $h' = h^{-1}$, so $h^{-1} \in H$.

Conversely, if (i) – (iii) hold then H is a group, since these properties (together with associativity) define a group.

<u>Proposition</u>: Let $H \subset G$ be a subset of a group. Then H is a subgroup if and only if $H \neq \emptyset$, and whenever $g, h \in H$ then $gh^{-1} \in H$.

Proof: First, if H is a subgroup then $g, h \in H$ implies $gh^{-1} \in H$ since H is a group.

On the other hand, suppose $g, h \in H$ implies $gh^{-1} \in H$, for some subset $H \subset G$, $H \neq \emptyset$. Then taking $h = g$, we see $gg^{-1} = e \in H$, so (i) holds.

Now taking elements $e, g \in H$ then $eg^{-1} = g^{-1} \in H$, so H is closed under taking inverses and (iii) holds.

Last, given $h_1, h_2 \in H$ then $h_1, h_2^{-1} \in H$ and so $h_1(h_2^{-1})^{-1} = h_1 h_2 \in H$, so (ii) holds.

Suggested questions: 1-10, 12, 14, 15, 16, 20-24, 31, 32, 33, 37, 39, 41, 46, 45, 47, 53.