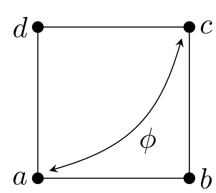
NOTES ON GROUPS, MATH 369.101

Intro to groups

Groups is a fairly applicable part of abstract algebra. Groups have less structure than rings or fields, which makes it so that there are many more situations in which they come up, but they have enough structure to be able to say interesting things about them.

Introduction. To give you a sneak-peek into the wide variety of groups that exist:

(1) Take any ring R (possibly but not necessarily a field), but use only $+$, the addition operation. Then $(R, +)$ is a group. (For example, $(\mathbb{Z}_n, +)$)
(2) The first example includes the set of $n \times n$ matrices with entries in a field $\mathbb{F}$ (since $M_n(\mathbb{F})$ is a ring). But if we just take those matrices which have an inverse (multiplicative), call it $\mathrm{GL}_n(\mathbb{F})$, and use $\cdot$ for matrix multiplication, then $(\mathrm{GL}_n(\mathbb{F}), \cdot)$ is a group.
(3) Any vector space with vector addition $(V, +)$ is a group.
(4) The set $\mathbb{S} = \{e^{i\theta} \mid \theta \in [0, 2\pi)\} \subset \mathbb{C}$ can be identified with the set of points on the unit circle in the plane. If we multiply two of them (as complex numbers), we get a new number in $\mathbb{S}$. with this multiplication $*$, $(\mathbb{S}, *)$ is a group.
(5) Take a *shape* P in the plane (for us, let's just think of a regular polygon). A **symmetry** ϕ is a 1-1 and onto map from the P to P. For a regular polygon, think of any 1-1, onto function which permutes the set of vertices, then complete the definition of the symmetry in the following way: if a, b are vertices and the permutation takes these vertices to c, d, then send the edge ab to the edge cd (if you always get an edge that way, then this gives a symmetry).



For example, if P is a square with vertices a, b, c, d. Taking $\phi(a) = c$, $\phi(b) = b$, $\phi(c) = a$, and $\phi(d) = d$, we take edges $ab \mapsto cb$, $bc \mapsto ba$, $cd \mapsto ad$, and $da \mapsto dc$. This gives us one symmetry of the square P.

Date: Oct. 26.

Another symmetry of the square is given by $\psi(a) = b$, $\psi(b) = c$, $\psi(c) = d$, and $\psi(d) = a$. Think about where the edges go.

We can multiply ϕ, ψ, two symmetries on P, by first applying ψ, then applying ϕ (take the composition). In other words do $\phi \circ \psi$, which is another symmetry. With the operation of $\circ$, the set of symmetries of P make a group.

A binary operation is something (like addition, or like multiplication) which takes two things in a set (with order mattering) and returns something new in the same set.

Definition 1. Let G be a set with a binary operation $*$. So $\forall g, h \in G$ there is a defined $g * h \in G$ (G is closed under $*$).

Then G is a **group** if the following axioms are met.

(1) (Associativity): $\forall f, g, h \in G$, we have $(f * g) * h = f * (g * h)$.
(2) (Identity): $\exists\ e \in G$ so that $e * g = g * e = g$, $\forall\ g \in G$.
(3) (Inverses): For each $g \in G$, $\exists\ g^{-1} \in G$ so that $g * g^{-1} = g^{-1} * g = e$.

Back to our examples, let's check they are groups.

(1) A ring R, but use only $+$. (So here $G = R$ and our $*$ is $+$.)

For any $r, s \in R$ we certainly have $r + s \in R$ since R is a ring. Also, $+$ is associative since that is one of the axioms of a ring, that is, $r + (s + t) = (r + s) + t$ for $r, s, t \in R$.

The identity is the additive identity 0, and for each $r \in R$ the inverse is the additive inverse $-r$. Since $*$ is $+$:

$$r * (-r) = r + -r = 0 = e.$$

So, in particular, $(\mathbb{Z}, +)$ is a group, $(\mathbb{Z}_n, +)$ is a group, $(R[x], +)$ is a group, etc.

(2) $(\mathrm{GL}_n(\mathbb{F}), \cdot)$

Matrix multiplication is associative. The identity I is the matrix with 1 on diagonal and 0 off the diagonal. We specifically said that $\mathrm{GL}_n(\mathbb{F})$ is the set of matrices that have an inverse (that is $AA^{-1} = A^{-1}A = I$). So if $A \in \mathrm{GL}_n(\mathbb{F})$ then A^{-1} exists. Furthermore, since $(A^{-1})^{-1} = A$, A^{-1} also has an inverse and so $A^{-1} \in \mathrm{GL}_n(\mathbb{F})$ also. This shows that $(\mathrm{GL}_n(\mathbb{F}), \cdot)$ satisfies the "Inverses" axiom for groups.

(3) Vector space $(V, +)$.

(Check).

(4) $(\mathbb{S}, *)$.

Note:

$$\begin{aligned} e^{i\alpha} * e^{i\beta} &= (\cos(\alpha) + i\sin(\alpha))(\cos(\beta) + i\sin(\beta)) \\ &= (\cos(\alpha)\cos(\beta) - \sin(\alpha)\sin(\beta)) + (\cos(\alpha)\sin(\beta) + \sin(\alpha)\cos(\beta))i \\ &= \cos(\alpha + \beta) + i\sin(\alpha + \beta) \\ &= e^{i(\alpha+\beta)}. \end{aligned}$$

So $\mathbb{S}$ is closed under $*$. Now for associativity (using the calculation we just did):

$$(e^{i\alpha} * e^{i\beta}) * e^{i\gamma} = e^{i(\alpha+\beta)} * e^{i\gamma} = e^{i(\alpha+\beta+\gamma)}$$

and

$$e^{i\alpha} * (e^{i\beta} * e^{i\gamma}) = e^{i\alpha} * e^{i(\beta+\gamma)} = e^{i(\alpha+\beta+\gamma)}.$$

So $*$ is associative.

Identity: $e^{i0} * e^{i\alpha} = e^{i\alpha} = e^{i\alpha} * e^{i0}$ for any α.

Inverses: $e^{i\alpha} * e^{i(2\pi-\alpha)} = e^{2\pi i} = e^{i0}$.

So $(\mathbb{S}, *)$ is a group!

(5) Symmetries with composition. Let's call our n-sided regular polygon P_n and use D_n for the set of symmetries of P_n.

Composition of functions is always associative.

Identity: Keep each point fixed: $e(x) = x$. This is definitely a bijection, and for any symmetry ψ, if $y = \psi(x)$, then:

$$e(\psi(x)) = e(y) = y = \psi(x) \qquad \text{and} \qquad \psi(e(x)) = \psi(x).$$

Since ψ can be any function symmetry, these two equations show that $e * \psi = e \circ \psi = \psi$ and $\psi * e = \psi \circ e = \psi$.

So $e(x) = x$ defines the identity element in the set of symmetries.

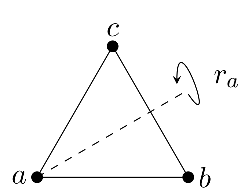
Inverses: A symmetry is determined by a bijective function on the set P, and for any bijective function we define: if $y = \phi(x)$ then $x = \phi^{-1}(y)$.

This makes ϕ^{-1} a function on P since every $y \in P$ is $\phi(x)$ for some $x \in P$ (ϕ is onto), and $\phi^{-1}(y)$ is well-defined since there was only one such x (ϕ is 1-1).

We then get that $\phi^{-1} \circ \phi(x) = \phi^{-1}(\phi(x)) = \phi^{-1}(y) = x$ (and something similar for $\phi \circ \phi^{-1}$), so $\phi^{-1} \circ \phi = e$ is the identity function.

We can conclude that $(D_n, \circ)$ is a group.

Let's more fully explore symmetries on a regular polygon, starting with an equilateral triangle P_3.

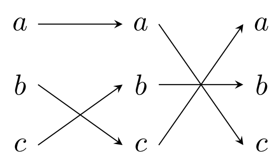


Since ϕ has to take vertices to vertices (and the edges are determined by that), we only have 6 choices. Let r_x flip the triangle about the angle bisector going through x, and t_1, t_2 are rotations about the center by $\pi/3$ and $2\pi/3$ respectively.

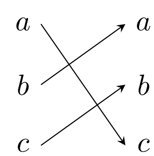
x	$e(x)$	$r_a(x)$	$r_b(x)$	$r_c(x)$	$t_1(x)$	$t_2(x)$
a	a	a	c	b	b	c
b	b	c	b	a	c	a
c	c	b	a	c	a	b

Now let's explore how the operation of composition relates these to each other.

(1) Checking $r_b \circ r_a$:

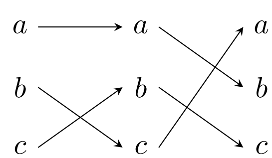


The composition is what you get by following from far left to far right:



which is an arrow diagram for t_2. This means that (writing $*$ for the operation $\circ$), we have $r_b * r_a = t_2$ in the group $(D_3, \circ)$.

(2) Let's check $t_1 \circ r_a$:



The composition gives us a map that sends $a \mapsto b$, $b \mapsto a$ and $c \mapsto c$. Checking our table above, we see that $t_1 * r_a = r_c$.

Check also that $t_2 * r_a = r_b$.

(3) Check that $r_a * r_b = t_1 \neq t_2$, so this tells us that $*$ is not commutative in D_3.

(4) Also check that $t_1 * t_1 = t_2$ and that $t_1 * t_2 = t_2 * t_1 = e$.

(5) Also check that $r_a * r_a = e$ (and that the same is true for r_b and r_c).

For items (4) and (5), think about the meaning of these equations for symmetries of the triangle. Why do the equations make sense?