Lecture 4: Groups – basic properties and related ideas

We will look at some basic properties of groups which can be derived just from the group axioms.

Recall

A group is a pair $(G, *)$ where G is a set and $*$ is a binary operation on G such that:

(1) There exists an element 1_G such that $f * 1_G = 1_G * f = f$ for all f in G.

(2) For all f in G, there exists an element f^{-1} such that

$$f * f^{-1} = f^{-1} * f = 1_G.$$

(3) (Associativity) For any f, g, h in G,

$$(f * g) * h = f * (g * h).$$

Cancellation property

Let a, b and c be elements of a group G.

If either $ab = ac$ or $ba = ca$, then $b = c$.

(In other words, we can cancel c either on the left or the right.)

Proof: Suppose $ab = ac$.

Then, $a^{-1}(ab) = a^{-1}(ac)$.

So, by associativity,

$$(a^{-1}a)b = (a^{-1}a)c.$$

So $1_G \cdot b = 1_G \cdot c$, i.e.

$b = c$.

If $ba = ca$, the proof is similar. //

Remark

It is not true, in general that

$ab = ca \implies b = c.$

For example in the dihedral group D_3, $\rho^2\tau = \tau\rho.$

However, we cannot cancel τ to get $\rho^2 = \rho$ (which is false)

<u>About the identity element</u>

The axioms say that there exists <u>some</u> element 1_G such that $f * 1_G = 1_G * f = f$ for all f. They do not explicitly say that there is <u>only one</u> such element. However, we can deduce this.

Uniqueness of identity.

Theorem Let G be a group and let f be an element of G such that $fx = x$ for *some* x in G. Then $f = 1_G$.

Proof $fx = x \implies f = 1_G$

(by "cancelling" x on the right.) //

Remark

Notice that we only needed to assume that $fx = x$ for <u>some</u> x, not necessarily all x.
Also, we did not need to assume $xf = x$.

About inverses

Similarly, in the case of inverses, the axioms only state that for any f in G, there exists <u>some</u> f^{-1} such that $f * f^{-1} = f^{-1} * f = 1_G$. However, we can <u>deduce</u> a stronger statement.

Uniqueness of inverses

Theorem Let G be a group and let f be an element of G. If h is an element such that $fh = 1_G$, then $h = f^{-1}$. Similarly, if h satisfies $hf = 1_G$, then $h = f^{-1}$.

Proof: $h = 1_G \cdot h$

$$= (f^{-1} f) \cdot h$$

$$= f^{-1}(fh)$$

$$= f^{-1} \cdot 1_G = f^{-1}.$$

The proof in the case $hf = 1_G$ is similar. (Ex. – Write it out.)

//

Inverses of a product:

Note that if a, b are in a group G, $(ab)^{-1}$ is not the same as $a^{-1} \cdot b^{-1}$!

In fact, we claim that $(ab)^{-1} = b^{-1} \cdot a^{-1}$. (Note the order!)

Indeed,

$$ab \cdot (b^{-1}a^{-1}) = a(bb^{-1})a^{-1}$$
$$= a \cdot 1_G \cdot a^{-1}$$
$$= aa^{-1} = 1_G.$$

So $(ab)^{-1} = b^{-1}a^{-1}$!

In general, $a^{-1}b^{-1}$ and $b^{-1}a^{-1}$ are not the same.

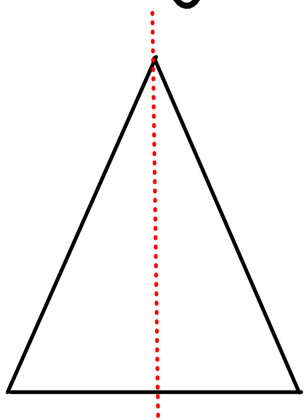
Notation

If the binary operation in a group is being written like multiplication, we write f^n for $\underbrace{f \cdot f \cdot \, \cdots \, f}_{n \text{ times}}$ where n is a positive number.

We will write f^{-n} for $(f^{-1})^n$. One can check that this behaves as expected, i.e. $f^m \cdot f^n = f^{m+n}$ for <u>any</u> integers m and n.

Similar-looking groups.

What is the group of isometries of a non-equilateral isosceles triangle?



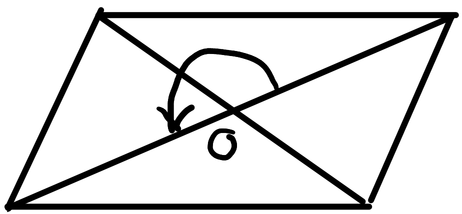
There are only two isometries

- id (identity)
- τ (a reflection)

The multiplication table fo this group is very simple.

	id	τ
id	id	τ
τ	τ	id.

Now, consider the isometries of a parallelogram which has unequal sides and is not a rectangle.



There are only two isometries

(1) id (identity)

(2) ρ (rotation around O through π)

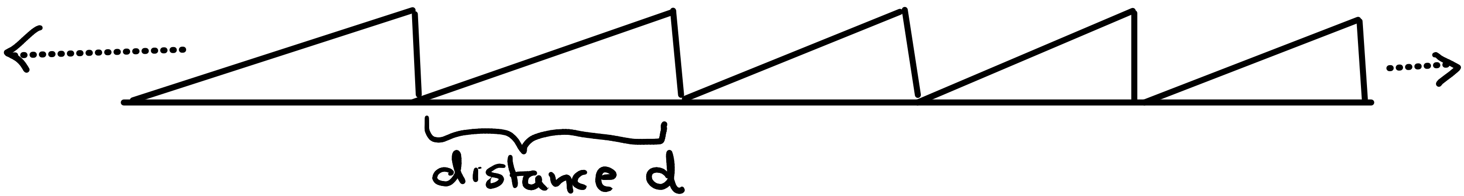
The multiplication table is

	id	ρ
id	id	ρ
ρ	ρ	id.

We notice that these groups are "essentially the same".

Let us look at another example....

Let A be the following set



The pattern repeats infinitely in both directions.

The group of isometries is the set $\{ id, \sigma, \sigma^{-1}, \sigma^{2}, \sigma^{-2}, \ldots \}$

where σ = translation to the right through distance d.

Composition is simple: $\sigma^{i} \cdot \sigma^{j} = \sigma^{i+j}$

for any integers j.

So, this group is "like" $(\mathbb{Z}, +)$.

When should two groups be treated essentially the same?

We should say they are the same if we can match up the elements in a way that "respects" the binary operations.

Definition

Let $(G, *)$ and $(H, \odot)$ be two groups. A <u>group isomorphism</u> from $(G,*)$ to $(H,\odot)$ is a 1-1 correspondence $\varphi : G \longrightarrow H$ such that $\varphi(x * y) = \varphi(x) \odot \varphi(y)$ for all x, y in G.

We say that two groups are isomorphic if there exists a group isomorphism from one to the other.

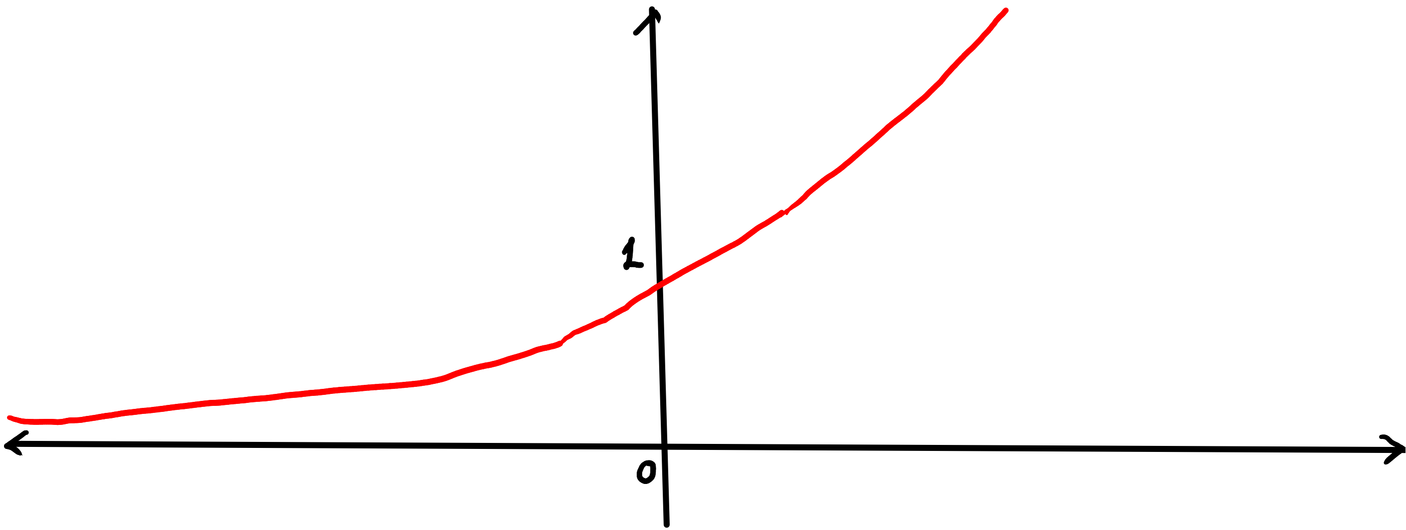
Example

Let $\mathbb{R}_+$ denote the set of positive real numbers. $\mathbb{R}_+$ is a group under the binary operation of multiplication.

We denote this group by $(\mathbb{R}_+, \cdot)$.

Fix some real number $a > 1$.

Consider the function $\varphi : \mathbb{R} \longrightarrow \mathbb{R}_+$ given by $\varphi(x) = a^x$.



It can be shown that φ is a 1-1 correspondence.

$$\varphi(x+y) = a^{x+y} = a^x \cdot a^y$$

$$= \varphi(x) \cdot \varphi(y).$$

Thus, φ is a group isomorphism. So $(\mathbb{R}_+, \cdot)$ is isomorphic to $(\mathbb{R}, +)$.

Isomorphisms "preserve" identity and inverses

Theorem Let G and H be groups. Let $\varphi : G \to H$ be an isomorphism. Then

(1) $\varphi(1_G) = 1_H$

(2) For any $x \in G$, $\varphi(x^{-1}) = \varphi(x)^{-1}$.

Proof: $\varphi(1_G) = \varphi(1_G \cdot 1_G)$

$$= \varphi(1_G) \cdot \varphi(1_G)$$

So, by cancelling $\varphi(1_G)$ from both sides, we get $\varphi(1_G) = 1_H$.

This proves (1).

Now, let x be any element of G.

Then $\varphi(x \cdot x^{-1}) = \varphi(x) \cdot \varphi(x^{-1})$.

But $\varphi(x \cdot x^{-1}) = \varphi(1_G) = 1_H$.

So $\varphi(x) \cdot \varphi(x^{-1}) = 1_H$

So, $\varphi(x^{-1}) = \varphi(x)^{-1}$.

//

Example

G = group of rotational symmetries of a regular hexagon

H = group of isometries of an equilateral triangle.

Are they isomorphic?

Answer No.

Two ways to see this.

(1) G contains the rotation ρ through $2\pi/6$ radians.

Then $\rho^6 = 1_G$. Also, ρ^2 and ρ^3 are not equal to 1_G

There is no such element in H!

Indeed if x is any element of H, either $x^2 = 1_H$ or $x^3 = 1_H$. (Check this!)

If $\varphi : G \longrightarrow H$ were any isomorphism, $\varphi(P)^2 = \varphi(P^2)$ and $\varphi(P)^3 = \varphi(P^3)$ must both be distinct from 1_H — contradiction.