Groups: Basic Definitions

Def: Let G be a set. A <u>binary operation</u> on G is a function:

$$*: G \times G \longrightarrow G$$

For psychological reasons, notationally we write $*(a,b)$ as $a*b$, for all $a,b \in G$.
The pair $(G,*)$ is called a <u>binary structure</u>.

Def: A <u>group</u> is a set G, together with a binary operation $*$ on G, such that the following hold:

1. (Associativity): $(a*b)*c = a*(b*c)$ $\forall a,b,c \in G$.
2. (Existence of identity): $\exists e \in G$ s.t. $a*e = e*a = a$ $\forall a \in G$.
3. (Existence of inverses): ~~Given~~ For all $a \in G$, $\exists b \in G$ s.t. $a*b = b*a = e$.

Def: A binary operation $*$ on a set G is called <u>commutative</u>, ~~ie (Abelian)~~ if $\forall a,b \in G$, $a*b = b*a$. A group $(G,*)$ is likewise called <u>commutative</u>, (or <u>Abelian</u>) if $\forall a,b \in G$, $a*b = b*a$.

<u>Examples</u>: Binary operations

$$+: \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$
$$+(a,b) = a+b$$

$$\cdot : GL_2(\mathbb{R}) \times GL_2(\mathbb{R}) \longrightarrow GL_2(\mathbb{R})$$
$$\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} e & f \\ g & h \end{pmatrix} \right) \longmapsto \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} =$$
$$= \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix}$$

Notes / Remarks: 1. In Boltje's notes there is a more complete treatment of binary structures. Due to time we are focusing/skipping strait to groups.

2. ⚠ Warning: In Boltje's notes $(\mathbb{Z}_n, +_n)$ is used to denote the gp we are calling $(\mathbb{Z}/n\mathbb{Z}, +)$. $(\mathbb{Z}_n, +_n)$ is slightly different in that Boltje defines $\mathbb{Z}_n$ as the set of standard representatives of the equivalence classes $\mathbb{Z}/n\mathbb{Z}$, and defines

$$a +_n b = \text{remainder of } a+b \text{ when divided by } n$$

This way he avoids having to talk about equivalence classes.

3. Notation / Example: Let X be a set.

$$F(X, X) = \text{functions from } X \text{ to } X$$

$$Sym(X) = \text{bijective functions from } X \text{ to } X$$

$Sym(X) \subseteq F(X, X)$

If $X = \{1, 2, 3, \ldots, n\}$, $Sym(X)$ is denoted by $Sym(n)$ or Sym_n and called the symmetric group. Composition of functions, $\circ$, is the binary operation we will usually consider on the sets $F(X, X)$ and $Sym(X)$.

Table of Examples and Non-examples (all binary operations in table are associative.)

Set	Binary Operation	Identity?	Inverses?	Group? Why Not?
$\mathbb{N}$	$+$	No	No	No, no id or inv.
$\mathbb{N}$	$\cdot$	1	No	No, no inv.
$\mathbb{Z}$	$+$	0	~~Yes~~ $a + -a = 0$	Yes
$\mathbb{Z}$	$\cdot$	1	No	No, no inv.
$\mathbb{Q}$	$+$	0	~~Yes~~ $a + -a = 0$	Yes
$\mathbb{Q}$	$\cdot$	1	$a \cdot 1/a = 1$ works for all a except $a \neq 0$	No, 0 does not have an inverse.
$\mathbb{Q} - \{0\}$	$\cdot$	1	$a \cdot 1/a = 1$	Yes
$\mathbb{Z}/n\mathbb{Z}$	$+$	$0 + n\mathbb{Z}$	$a + n\mathbb{Z} + -a + n\mathbb{Z} = 0 + n\mathbb{Z}$	Yes
$\mathbb{Z}/n\mathbb{Z}$	$\cdot$	$1 + n\mathbb{Z}$	$0 + n\mathbb{Z}$ does not have an inverse	No, no inv.
$\mathbb{R}^n$	$+$ addition of vectors	$(0, 0, \dots, 0, 0)$	$(a_1, a_2, \dots, a_n) + (-a_1, -a_2, \dots, -a_n) = (0, 0, \dots, 0)$	Yes
$\mathbb{R}_{>0}$ pos. real #s	$\cdot$	1	$a \cdot 1/a = 1$	Yes
$M_{n \times n}(\mathbb{R})$ $n \times n$ matrices	matrix mult.	$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$	Not every matrix has an inverse.	No, no inv.
$GL_n(\mathbb{R})$ $n \times n$ invertible matrices	matrix mult.	$\begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$	Yes	Yes

/3

$F(X,X)$	$\circ$	id_X	Not every function has an inverse	No
$Sym(X)$	$\circ$	id_X	Yes, bijective functions have inverses	Yes

Group - new mathematical object, set with extra structure. We define the functions between groups that we will consider. Previous examples

Object/Subject	Functions
Sets/Set theory	Any functions
Vector Spaces/Lin. Alg.	Linear functions/operators/transformations
$\mathbb{R}$/Calculus	Cont. functions, diff. functions, int. functions

For gp theory, we consider functions that preserve the gp structure.

Def: Let $(G, *)$ and $(H, \circ)$ be two groups. A <u>homomorphism</u>, f, from G to H, is a function $f: G \to H$, such that for all $x, y \in G$,

$$f(x * y) = f(x) \circ f(y)$$

A bijective homomorphism is called an <u>isomorphism.</u> $(G, *)$ and $(H, \circ)$ are called <u>isomorphic</u> if there exists an isomorphism between them. This is denoted $(G, *) \cong (H, \circ)$ or $G \cong H$ if the binary operations are clear.

<u>Remarks</u>: 1. For all gps $(G, *)$, the identity function id_G is a gp hom. from G to G.

2. Two gps being isom. means intuitively that they are the "same" gp but just viewed from different perspectives.

<u>Examples</u>: 1. The exponential function $f: (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$, defined by $f(x) = e^x$ is a gp hom because $\forall x, y \in \mathbb{R}$,

$$f(x+y) = e^{x+y} = e^x \cdot e^y = f(x) \cdot f(y)$$

f is an isomorphism because f has an inverse given by $g(x) = \log x$

2. The function $T: (\mathbb{R}^2, +) \to (\mathbb{R}, +)$ given by $T(x,y) = x$ is a gp hom because for all $(x,y), (z,w) \in \mathbb{R}^2$,

$$T((x,y) + (z,w)) = T((x+z, y+w))$$
$$= x+z$$
$$= T(x,y) + T(z,w)$$

T is not an isom. because T is not injective.

3. If $A \in M_{n\times m}(\mathbb{R})$, $\phi_A: (\mathbb{R}^m, +) \to (\mathbb{R}^n, +)$, $\phi_A(v) = Av$ is gp hom.

Prop: Let $(G, *)$, $(H, \circ)$, and $(M, \square)$ be three groups. Let $f: G \to H$ and $g: H \to M$ be homomorphisms. Then the composition, $g \circ f: G \to M$ is a homomorphism.

proof: Let $x, y \in G$. Then need to show $g\circ f(x * y) = (g\circ f)(x) \square (g \circ f)(y)$.

Have
$$g\circ f(x * y) = g(f(x*y))$$
$$= g(f(x) \circ f(y)) \quad \text{because } f \text{ is a hom.}$$
$$= g(f(x)) \square g(f(y)) \quad \text{because } g \text{ is a hom.}$$
$$= (g\circ f)(x) \square (g \circ f)(y) \quad \square$$

Prop: Let $(G, *)$ be a gp. Then the identity element of G is unique.

proof: Let $e, e' \in G$ be two identity elements of G. Then

$e = e * e'$ and $e' = e * e'$ by the identity property.

So $e = e'$. $\square$

Prop (inverses are unique): Let $(G,*)$ be a gp. For all $a \in G$, the inverse of a is ~~only~~ unique.

proof: Let b, c be two inverses of a, so

$$a*b = b*a = e$$
and
$$a*c = c*a = e$$

Then we need to show $b=c$. We have:

$$\begin{aligned} b &= e*b && \text{by id. prop.} \\ &= (c*a)*b && \text{by above} \\ &= c*(a*b) && \text{by associativity} \\ &= c*e && \text{by above} \\ &= c && \text{by id. prop.} \end{aligned}$$

Remark: By proposition, given a gp $(G,*)$ we can unambiguously write down the identity element. For an abstract gp $(G,*)$, e or 1 is usually used to denote the identity element. For gps you already know, the identity element may already have a symbol. We may also given $a \in G$, unambiguously write a^{-1} for the inverse of a in G.

Prop (cancellation law): Let $a, b, c \in G$, where $(G,*)$ is a gp. If $a*c = a*b$ (resp $c*a = b*a$), then $c=b$.

proof: If $a*c = a*b$, then

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

Similarly for other one.

Prop: Let $(G,*)$ be a group. Then for all $a,b \in G$,

$$(a*b)^{-1} = b^{-1} * a^{-1}$$

Proof: We have

$$\begin{aligned}(a*b)*(b^{-1}*a^{-1}) &= a*(b*b^{-1})*a^{-1} \\ &= a*e*a^{-1} \\ &= a*a^{-1} \\ &= e\end{aligned}$$

and

$$\begin{aligned}(b^{-1}*a^{-1})*(a*b) &= b^{-1}*(a^{-1}*a)*b \\ &= b^{-1}*e*b \\ &= b^{-1}*b \\ &= e\end{aligned}$$

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

Prop: Let $(G,*)$ be a gp. Then $e^{-1}=e$.

Proof: $e*e=e$, so $e^{-1}=e$.

** Save this for later

Remark/Notation: Writing a group additively, means the group operation is written with a $+$. In this case, 0 usually denotes the identity element and $-a$ denotes the invers of a. Otherwise, the group may be written with $\cdot, \circ, *$, etc., and the identity is 1 or e, along with inverse ~~being~~ of a being denoted by a^{-1}.

We have the following notation

Additive group $(G,+)$, $a \in G$, $n \in \mathbb{Z}$

$$na = \begin{cases} a+a+\cdots a & n\text{-times if } n>0 \\ 0 & \text{if } n=0 \\ -a+-a+\cdots+-a & |n|\text{-times if } n<0 \end{cases}$$

Mult. group $(G,\cdot)$, $a \in G$, $n \in \mathbb{Z}$

$$a^n = \begin{cases} a\cdot a\cdot \cdots \cdot a & n\text{-times if } n>0 \\ e & \text{if } n=0 \\ a^{-1}\cdot a^{-1}\cdots a^{-1} & |n|\text{-times if } n<0 \end{cases}$$

** Save this for later **

With this notation, by definition, we have $\boxed{a^m a^n = a^{m+n} \text{ and } (a^m)^n = a^{mn} \ \forall a \in G, m,n \in \mathbb{Z}}$

Let $f: G \to H$ be a hom.

<u>Prop</u>: Let $(G,*)$, $(H,\square)$ be two gps, and let $f: G \to H$ be a hom. Then

(a) Let $e_G \in G$, $e_H \in H$ denote the identity elements. Then

$$f(e_G) = e_H$$

(b) For all $a \in G$, $f(a^{-1}) = f(a)^{-1}$.

<u>proof</u>: (a) Let $h \in H$. Then

$$h \square f(e_G) = h \square f(e_G * e_G) = h \square f(e_G) \square f(e_G)$$

By cancellation law get

$$h = h \square f(e_G)$$

Similarly $h = f(e_G) \square h$. Therefore $f(e_G) = e_H$.

(b) $f(a^{-1}) \square f(a) = f(a^{-1} * a) = f(e_G) = e_H$

$f(a) \square f(a^{-1}) = f(a * a^{-1}) = f(e_G) = e_H$

Therefore $f(a^{-1}) = f(a)^{-1}$. $\square$