§1 - Introduction to Groups

§1.1 - First Examples

Informally, a group is a set of objects in which we can "multiply" and "divide".

That's pretty much it!

With such a simple description, it should come as little surprise that groups show up a lot in math, physics, chemistry, etc... They appear in many different forms as we will soon see.

Before stating the formal definition, let's explore some familiar examples

Ex 1. <u>The integers $(\mathbb{Z}, +)$</u>

$$\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$$

The operation $+$ takes in two integers and spits out another one.

e.g. $3+5 = 8$ $\qquad$ $0+4 = 4$

$5+3 = 8$ $\qquad$ $(-9)+0 = -9$

$7+(-1) = 6$ $\qquad$ $2+(-2) = 0$

<u>Observations?</u>

(i) 0 is special! It has the property that

$$\boxed{a+0=0+a=a \quad \text{for all } a\in\mathbb{Z}.}$$

We say that 0 is the identity of the group (are there any others?)

(ii) Elements like a and $-a$ share a special relationship:

$$\boxed{a+(-a)=0.}$$

We say that $-a$ is the inverse of a. Likewise, a is the inverse of $-a$

(iii) Addition of integers behaves "nicely"

$$\boxed{(a+b)+c = a+(b+c) \quad \text{for all } a,b,c \in \mathbb{Z}}$$

We say that this operation is associative.

(iv) In this case, our operation is particularly nice: order doesn't matter!

$$\boxed{a+b = b+a \quad \text{for all } a,b \in \mathbb{Z}}$$

We say that this operation is commutative. Likewise we call this group commutative or Abelian.

Ex 2. The rationals $(\mathbb{Q}, +)$

Again, $+$ takes two rational numbers

and outputs another rational number:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$$

Again, addition is associative:

$$\left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f} = \frac{ad+bc}{bd} + \frac{e}{f} = \frac{adf+bcf+bde}{bdf}$$

equal!

$$\frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} + \left(\frac{cf+de}{df}\right) = \frac{adf+bcf+bde}{bdf}$$

and commutative: $\frac{a}{b} + \frac{c}{d} = \frac{c}{d} + \frac{a}{b}$

What's this group's identity element? 0.

What is the inverse of a/b? $-a/b$.

Ex 3. The real numbers $(\mathbb{R}, +)$

Ex 4. The complex numbers $(\mathbb{C}, +)$

In each case, what is the identity?

What is the inverse of an element?

Is the operation associative? commutative?

Ex 5. $(\mathbb{Q}^*, \cdot)$

Do the rational numbers form a group under multiplication?

The identity should be 1, as

$$1 \cdot \frac{a}{b} = \frac{a}{b} \cdot 1 = \frac{a}{b} \text{ for all } \frac{a}{b}$$

Then what about inverses? 0 doesn't have one!

Okay... new strategy! Consider $\boxed{\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}}$,

(rationals with multiplicative inverses)

Now the inverse of any $\frac{a}{b} \in \mathbb{Q}^*$ is

$$\boxed{\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}}$$

Again, we can check that multiplication is associative. It is also commutative.

Ex 6. $(\{1, -1\}, \cdot)$

The only integers with multiplicative inverses are ± 1. These integers form a group under multiplication. We can write down their products in a Cayley table.

$$\begin{array}{c|cc} \cdot & 1 & -1 \\ \hline 1 & 1 & \boxed{-1} \\ -1 & -1 & 1 \end{array} \quad = 1\cdot(-1)$$

We list the product (row i)$\cdot$(column j) in the i^{th} row, j^{th} column of the table (ORDER MATTERS!)

What is this group's identity?

What is the inverse of -1?

Ex 7. $(\mathbb{R}^*, \cdot)$, where $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$

Ex 8. $(\mathbb{C}^*, \cdot)$, where $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$

Ex 9. $(\{1, i, -1, -i\}, \cdot)$, where $i \in \mathbb{C}$, $i^2 = -1$

Again, what are the identities? inverses?

Exercise: Write down the Cayley table in Ex. 9.

Ex 10. $(GL_n(\mathbb{R}), \cdot)$

We can make $M_n(\mathbb{R})$ into a group under matrix multiplication by throwing away any non-invertible matrices:

$$\boxed{\begin{aligned} GL_n(\mathbb{R}) &= \{A \in M_n(\mathbb{R}) : A \text{ is invertible}\} \\ &= \{A \in M_n(\mathbb{R}) : \det(A) \neq 0\} \end{aligned}}$$

If $A, B \in GL_n(\mathbb{R})$, does the product $A \cdot B$ again belong to $GL_n(\mathbb{R})$? Yes! Since $\det(A \cdot B) = \det(A) \cdot \det(B) \neq 0$, $AB \in GL_n(\mathbb{R})$

We say that $GL_n(\mathbb{R})$ is closed under the group operation.

The identity of this group is

$$I_n = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix}_{n\times n}.$$

From linear algebra, we know that matrix multiplication is associative, but NOT commutative!

e.g. when $n=2$, let $A = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}$.

Then $A, B \in GL_2(\mathbb{R})$, yet

$AB = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$, $BA = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$ so $AB \neq BA$!

Thus, this is our first example of a non-Abelian group (a group whose operation is not commutative).

SO! What is a group??

Definition: A set G together with a binary operation $\bullet : G \times G \longrightarrow G$ is a group if

(i) For all $a, b, c \in G$, $(a \bullet b) \bullet c = a \bullet (b \bullet c)$

(i.e., $\bullet$ is an associative operation)

(ii) There is an element $e \in G$ which we call the identity such that

$a \bullet e = e \bullet a = a$ for all $a \in G$.

(iii) For every $a \in G$, there is an element $a^{-1} \in G$ such that $a \bullet a^{-1} = a^{-1} \bullet a = e$.

We call a^{-1} the inverse of a.

Remark: Notice that the group operation $\cdot$ must take two elements of G to another element of G. We say that G is closed under the group operation. You must verify this fact when showing that something is a group, just as we did in Ex 10.

Definition: Elements a, b in a group $(G, \cdot)$ are said to commute if $a \cdot b = b \cdot a$. If $a \cdot b = b \cdot a$ for all $a, b \in G$, we say that G is Abelian (or commutative)

Otherwise we say the G is non-Abelian.

Why would we choose these conditions for our definition of a group?

To answer this question, first consider the following equation:

$$\boxed{x + 4 = 7}$$

Obviously the solution is $x = 3$. For fun let's write out the steps in excrutiating detail:

$$x + 4 = 7 \Rightarrow (x + 4) + (-4) = 7 + (-4)$$

$$\Rightarrow \quad x + (4 + (-4)) = 3$$

$$\Rightarrow \quad x + 0 = 3$$

$$\Rightarrow \quad \underline{x = 3}$$

Our first step required the existence of -4, the <u>inverse</u> to 4

Next, we needed <u>associativity</u> of $+$ to write $(x+4)+(-4) = x + (4+(-4))$.

Finally, we used the fact that there is an additive <u>identity</u> 0 to conclude that $x = 3$.

LOOK FAMILIAR ?

§1.2 Properties of Groups

Natural Questions: In the definition of a group, we say things like "the identity" and "the inverse of a". Are these really unique? Yes! In this section we investigate these properties and other basic facts about groups.

In what follows, we will simply write the group operation as $a \cdot b = ab$.

Proposition: The identity element of a group is unique.

Proof: Suppose a group G had two identity elements e and f.

Then $ef = f$ (as e is identity)

and $ef = e$ (as f is identity)

Thus, $e = f$. $\blacksquare$

Proposition: If a is an element of a group G, then a^{-1} is unique.

Proof: Assignment 1. $\blacksquare$

Proposition: Let G be a group and let $a, b, c \in G$.

(i) [Left cancellation] If $ab = ac$ then $b = c$.

(ii) [Right cancellation] If $ba = ca$ then $b = c$.

Proof: $ab = ac \Rightarrow a^{-1}(ab) = a^{-1}(ac)$

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

$$\Rightarrow eb = ec$$

$$\Rightarrow b = c$$

This proves (i), and (ii) is similar. $\blacksquare$

Definition: If a is an element of a group $(G, \cdot)$ and $k \in \mathbb{Z}$, define

$$a^k = \begin{cases} \underbrace{a \cdot a \cdot \cdots \cdot a}_{k \text{ times}} & \text{if } k > 0, \\ e & \text{if } k = 0, \end{cases}$$

$$\underbrace{a^{-1}\cdot a^{-1}\cdot \cdots \cdot a^{-1}}_{K \text{ times}} \quad \text{if } K<0 \; .$$

Exercise: Prove that the exponent laws

$$\boxed{a^{m+n} = a^m a^n} \quad \text{and} \quad \boxed{(a^m)^n = a^{mn}}$$

hold for all $a \in G$ and all $m, n \in \mathbb{Z}$.

Proposition: If a, b are elements of a group G, then $(ab)^{-1} = b^{-1}a^{-1}$

Proof: Exercise. $\blacksquare$

§1.3 – More Examples

Ex 11. Integers modulo n $(\mathbb{Z}_n, +)$

From MATH 135 we know that

$$\mathbb{Z}_n = \{[0],[1], \ldots, [n-1]\}.$$

where $[a]$ is an equivalence class

$$[a] = \{b \in \mathbb{Z} : n \text{ divides } b-a\}$$

(We will not write $[\cdot]$ from here on.)

We can add elements from $\mathbb{Z}_n$, reducing mod n. In this way, $(\mathbb{Z}_n, +)$ forms a group. Identity? 0.

Inverse of a? $n-a$.

e.g. The Cayley table for $(\mathbb{Z}_4, +)$ is

	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Ex 12. Group of units modulo n $(\mathbb{Z}_n^*, \cdot)$

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : ax \equiv 1 \bmod n \text{ for some } x \in \mathbb{Z}_n\}$$

(integers with multiplicative inverses mod n)

Recall from Math 135 that

$$\boxed{a \in \mathbb{Z}_n^* \text{ if and only if } \gcd(a,n) = 1.}$$

[Indeed, first recall the following fact:

Bezout's Lemma: If $a, b \in \mathbb{Z}$ and $\gcd(a,b) = d$, then there exist $x, y \in \mathbb{Z}$ such that $ax + by = d$.

If $\gcd(a,n) = 1$, then $\exists x, y \in \mathbb{Z}$ such that $ax + ny = 1$. Thus $ax \equiv 1 \bmod n$, so $a \in \mathbb{Z}_n^*$.

Conversely, if $ax \equiv 1 \mod n$, then $n \mid 1 - ax$ and hence $1 - ax = ny$ for some $y \in \mathbb{Z}$.

Since $\gcd(a,n)$ divides a and n, it divides $ax + ny = 1$. Thus, $\gcd(a,n) = 1$. $\blacksquare$]

With the non-invertible elements removed, we may verify that $\mathbb{Z}_n^*$ forms a group under multiplication. Identity? $\underline{1}$.

e.g. $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$.

	1	5	7	11
1	1	5	7	11
5	5	1	11	$\boxed{7}$
7	7	11	1	5
11	11	7	5	1

$5 \cdot 11 = 55 \equiv 7 \mod 12$.

Definition: If G is a group, then the order of G, $|G|$, is the number of elements in G.

e.g. $|\mathbb{Z}| = \infty$, $|\mathbb{Z}_n| = n$, $|\{1,-1\}| = 2$

Exercise: If $p \in \mathbb{N}$ is prime, what is $|\mathbb{Z}_p^*|$? Write down the Cayley table for $\mathbb{Z}_5^*$.

Ex 13. Dihedral Groups, D_n

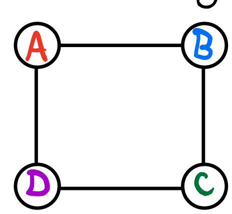
For each integer $n \geq 3$, we define the dihedral group D_n to be the set of all symmetries of a regular n-gon.

What's a symmetry?

It's any movement that can be done to the object while you aren't looking, that you won't know has happened.

For instance, let's look at D_4, the group of all symmetries of a square.

We'll put IMAGINARY labels on the vertices to keep track of the symmetry taking place.



How many symmetries are there?

(i.e., what is the order of D_4?)

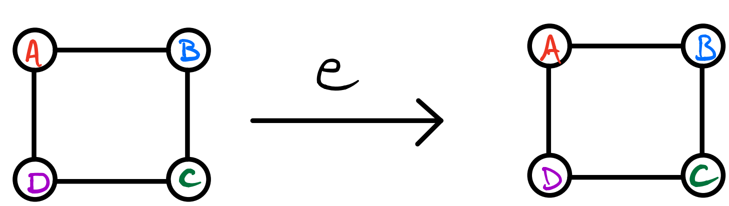
Well... we have 4 choices for where A goes.

Notice, however, that A's neighbours are always B and D. Thus, we have two choices: either B is clockwise from A or D is clockwise from A.

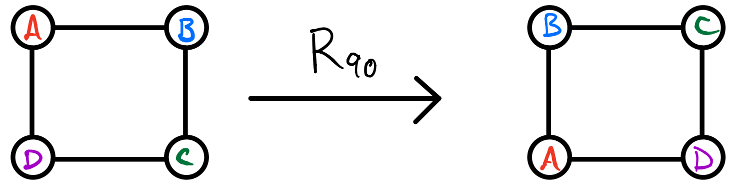
$\therefore$ At most $4 \cdot 2 = \underline{8 \text{ symmetries}}$

Can we actually get all 8? Yes!

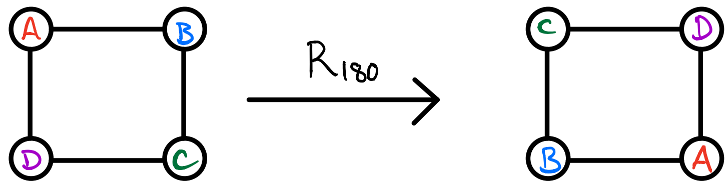
Identity



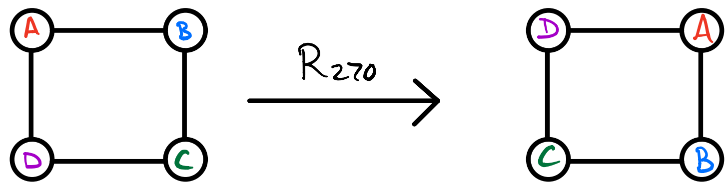
Rotation by 90°
(counterclockwise)



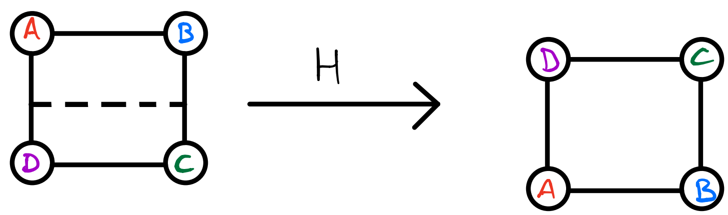
Rotation by 180°



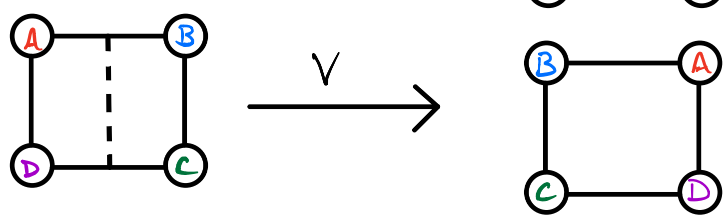
Rotation by 270°



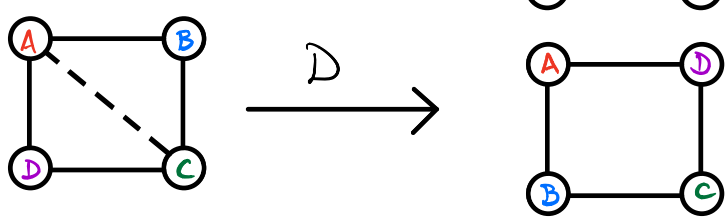
Flip about
horizontal axis



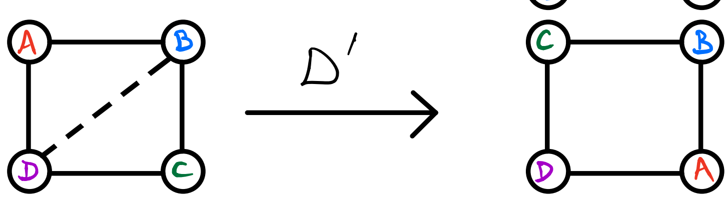
Flip about
vertical axis



Flip about
main diagonal



Flip about
other diagonal



$$\therefore \boxed{D_4 = \{e, R_{90}, R_{180}, R_{270}, H, V, D, D'\}, \quad |D_4| = 8}$$

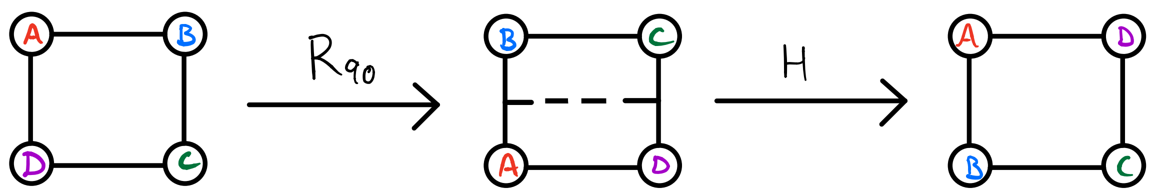
We said that D_n is a group, but

what's the group operation?

It's composition of symmetries!

For instance, suppose we rotate by $90°$

and then flip in the horizontal axis:



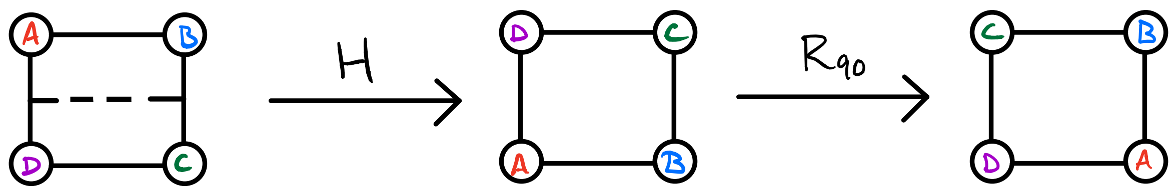
We can express this symmetry as HR_{90},

reading right to left as we would with functions.

Notice that the overall effect is the same

as applying D, hence $\boxed{HR_{90} = D.}$

Note that $R_{90} H = D' \neq D$



Thus, D_n is non-abelian.

Cayley Table:

	e	R_{90}	R_{180}	R_{270}	H	V	D	D'
e	e	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_{90}	R_{90}	R_{180}	R_{270}	e	D'	D	H	V
R_{180}	R_{180}	R_{270}	e	R_{90}	V	H	D'	D
R_{270}	R_{270}	e	R_{90}	R_{180}	D	D'	V	H
H	H	D	V	D'	e	R_{180}	R_{270}	R_{90}
V	V	D'	H	D	R_{180}	e	R_{90}	R_{270}
D	D	V	D'	H	R_{270}	R_{90}	e	R_{180}
D'	D'	H	D	V	R_{90}	R_{270}	R_{180}	e

It's easy to check that, in fact, all of the symmetries in D_4 can be built using a rotation $R = R_{90}$, and flip $F = H$

(we can use $F = H, V, D,$ or D')

Indeed, $R^0 = e$, $R = R_{90}$, $R^2 = R_{180}$, $R^3 = R_{270}$,

$F = H$, $FR = D$, $FR^2 = V$, $FR^3 = D'$

So, $\boxed{D_4 = \{R^k, FR^k : 0 \leq k \leq 3\}}$

This is a much easier way of describing D_n for any $n \geq 3$.

If R = counterclockwise rotation by $\frac{2\pi}{n}$ radians and F = any flip, then

$$\boxed{D_n = \{R^k, FR^k : 0 \leq k \leq n-1\}}$$

Ex 14. Symmetric Groups, S_n

For $n \geq 1$, define S_n to be the set of all permutations of $\{1,2,3,\dots,n\}$. That is,

$$\boxed{S_n = \left\{ \sigma : \{1,2,\dots,n\} \to \{1,2,\dots,n\} \;\middle|\; \sigma \text{ is bijective} \right\}}$$

e.g., S_3 consists of all permutations of $\{1,2,3\}$.

The functions f, g on $\{1,2,3\}$ given by

$$\sigma(1) = 2, \quad \sigma(2) = 3, \quad \sigma(3) = 1$$

$$\tau(1) = 1, \quad \tau(2) = 3, \quad \tau(3) = 2$$

belong to S_3, whereas the function

$$\varphi(1) = 2, \quad \varphi(2) = 3, \quad \varphi(3) = 2$$

does not (why?)

What's the group operation?

Function Composition!

Again, we read right to left:

With $\sigma, \tau \in S_3$ as above, then for $\psi = \sigma \circ \tau$

$$\psi(1) = \sigma(\tau(1)) = \sigma(1) = 2$$

$$\psi(2) = \sigma(\tau(2)) = \sigma(3) = 1$$

$$\psi(3) = \sigma(\tau(3)) = \sigma(2) = 3$$

With this operation, S_n forms a group!

A more compact way of writing a permutation $\pi \in S_n$:

$$\boxed{\pi = \begin{pmatrix} 1 & 2 & \cdots & n \\ \pi(1) & \pi(2) & \cdots & \pi(n) \end{pmatrix}}$$

e.g. With $\sigma, \tau, \psi \in S_3$ as above

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\tau = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\psi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

Exercise: Write down the inverses of σ, τ.

Write $\tau \circ \sigma$ in the compact form above.

Is S_3 abelian?

Arguably, S_n is the most important example of a finite group. We'll see why later in the course. For now, let's determine $|S_n|$.

To build a permutation σ of $\{1, 2, \ldots, n\}$, we have n choices for $\sigma(1)$, then $n-1$ choices for $\sigma(2)$, $n-2$ choices for $\sigma(3)$, etc...

Thus, there are $n(n-1)(n-2)\cdots(2)(1) = n!$ permutations in S_n:

$$\boxed{|S_n| = n!}$$

§1.4 – Building New Groups from Old.

Given groups $(G, *)$ and $(H, *)$, we can form a new group $(G \times H, \cdot)$, the external direct product of G and H.

Here,

$$\boxed{\begin{gathered} G \times H = \{(g,h) : g \in G,\ h \in H\} \\ (g_1, h_1) \cdot (g_2, h_2) = (g_1 * g_2,\ h_1 * h_2) \end{gathered}}$$

Exercise: Prove that $G \times H$ is a group.

e.g. Consider the direct product

$$GL_2(\mathbb{R}) \times \mathbb{Z}$$

$$\left(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, 2 \right) \cdot \left(\begin{bmatrix} 2 & 0 \\ 1 & -1 \end{bmatrix}, 5 \right)$$

$$= \left(\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 2 & 0 \\ 1 & -1 \end{bmatrix}, 2+5 \right) = \left(\begin{bmatrix} 3 & -1 \\ 1 & -1 \end{bmatrix}, 7 \right)$$

Exercise: Write down the Cayley table for

$\mathbb{Z}_2 \times \mathbb{Z}_2$. In general, what is $|G \times H|$ in terms of $|G|, |H|$?

§1.5 – Isomorphisms via Cayley Tables.

At this point we have built a nice library of examples of groups:

Additive: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_n$

Multiplicative: $\{\pm 1\}, \{1, i, -1, i\}, \mathbb{Q}^*, \mathbb{R}^*, \mathbb{C}^*, \mathbb{Z}_n^*$

Matrix Groups: $GL_n(\mathbb{Q}), GL_n(\mathbb{R}), GL_n(\mathbb{C})$

Dihedral Groups: D_n

Symmetric Groups: S_n

Although all of these groups are distinct.

Some operate in much the same way.

Take for example, the groups

$\mathbb{Z}_2$ $\quad\quad$ $\{\pm 1\}$ $\quad\quad$ $\mathbb{Z}_6^*$

+	0	1
0	0	1
1	1	0

·	1	-1
1	1	-1
-1	-1	1

·	1	5
1	1	5
5	5	1

These groups all have order 2, and their Cayley tables look more than a little similar.

Essentially, these groups all consist of an identity e, and one other element a such that $a^2 = e$.

In each case, a has a distinct label but names aside, the groups look identical.

Definition: Two finite groups G, H are said to be isomorphic if, after relabelling and reordering their elements, their Cayley tables look identical. In this case we write $G \cong H$.

We have that $\mathbb{Z}_2 \cong \{\pm 1\} \cong \mathbb{Z}_5^*$

Fact: $\boxed{\text{Any two groups of order 2 are isomorphic!}}$ Why?

Exercise: In the Cayley table of a

finite group G, every element of G must appear exactly once in each row and column.

So if $G = \{e, a\}$ is a group of order 2, then there is only one way to build its Cayley table:

	e	a
e	e	a
a	a	e

Thus, there is only one group of order 2, up to isomorphism!

Exercise: Show that there is exactly one Cayley table for a group of order 3. Conclude that there is only one such group up to isomorphism. What's an example?

Exercise: Write down the Cayley tables for $\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$. Are these groups isomorphic?