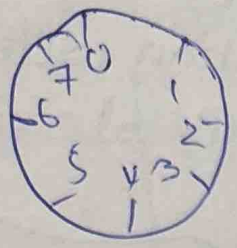
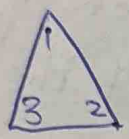
Socratica - Abstract Algebra

Modular Arithmetic

- 

mod 8.

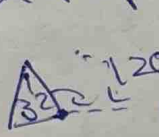
Equilateral Δle Puzzle

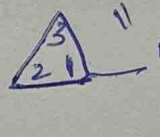
- 

how many ways can you rotate / flip the Δle so that it looks the same before and after?

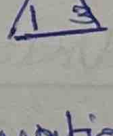
- enumerate all possible distinct (base / fundamental type?) transformations:

① Pick it up, put it back down. "1"

② 

$\Rightarrow$ 

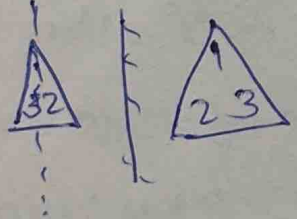
"r"

③ if we do r and then r again we get: 

"r^2"

④ r^3 = 

original Δle $\therefore r^3 = 1$ (transformation 1)

⑤ 

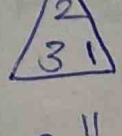
reflect = flip about vertical axis. "f" for flip about the axis (vertical)

⑥ flip and flip = f^2 = 

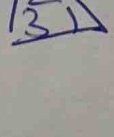
$= 1$

⑦ flip and rotate: 

$\xrightarrow{f}$ 

$\xrightarrow{r}$ 

"$f \cdot r$" = "rf"

⑧ flip, rotate, rotate: 

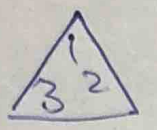
$\xrightarrow{r}$ 

"$f \cdot r^2$" = "$r^2 f$"?

NO??

how ~~to~~ ~~get~~ ~~that~~?

• ∴ there are 6 possible transformations



1

f

r

f.r.

r^2

$f.r^2$

* there were two basic transformations
i) 120° CW rotation called r
ii) flip about vertical axis called f.

↳ called symmetries

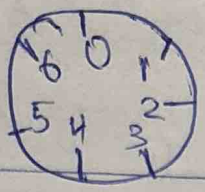
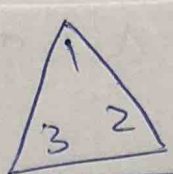
*apart from I (unchanged transformation) each of the other transformations is a combination of the two basic ones

* NOT COMMUTATIVE

* This is one way to study a shape.
↳ Look at all the ways we can transform the shape onto itself.

Integers Under +

• $\mathbb{Z} = \{..., -2, -1, 0, 1, 2, ...\}$
• x−y is just adding -ve numbers
∴ single add. operation.
• closed under +, not closed under ÷
• Zero: like 'I' transformation.

			$\mathbb{Z}$
Elements	$\{0,1,2,3,4,5,6\}$	$\{1, r, r^2, y, ry, r^2y\}$	$\{\ldots -2, -1, 0, 1, 2, \ldots\}$
Operation	$+$	$\times$ (6)	$+$
Closure	✓	" ✓ "	✓
Identity	0	1	0
Inverse	$3 \to (-3) = 4$. $x + (-x) = 0$	$r \to r^2 \because r \cdot r^2 = 1$ $xx^{-1} = 1$	~~$3 \to -3$~~ $x + (-x) = 0$
Associative	$a+(b+c) = (a+b)+c$	$(a \cdot b) \cdot c = a \cdot (b \cdot c)$	$(a+b)+c = a+(b+c)$.

- Set of objects in the example = elements.
  - Δ's obj. are trans
- for each set of elements, ∃ some way to combine any two elements to get another element in the set. (operation).
- for integers any subtr. can be done using add.

Group Definition

- set of elements G
- operation that allows you combine any two elements 'x'
- closed under this operation $*$
- Inverses exist for all x. $x * x^{-1} = e$
- Identity: $y * e = y = e * y$
- Associative
- if G is commutative too i.e. $x * y = y * x$. then it is an abelian group.

} generalise bw arithmetic, geometry, abstract alg? etc.

- In arithmetic ∃ basically + , × only.

Operation:	+	×
opposites (inverses):	negatives	reciprocals
identity	0	1

- Textbook definition of a group:
  - → set of elements
  - → operation *
  - ⇒ closed under *
  - → inverses
  - → Identity e (combine an element with its inverse).
  - → Associativity

↳ Why these properties?

$x+3=5$.

i) add (-3) to both sides

↳ integers under + (set + operation)

↳ (-3) ⇒ inverses

$x+3+(-3) = 5+(-3)$ → adding these too requires a closed operation

$= 2$

$x+(3+(-3)) = 2$ ⇒ associative

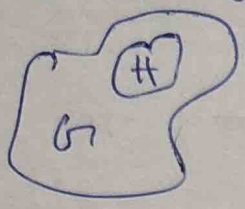
$x+0 = 2$ ⇒ identity

$\therefore x = 2$.

∴ the definition of a group is such that it lets us solve a basic equation

...inition of A Subgroup

- let G be a group
- A subgroup of G is a subset that is also a group



$H \leq G \Rightarrow$ "H is a subgroup of G"

"$H \subseteq G$, and $*$, $*$ same

if $H \neq G$, $H < G$ "H is a proper subgroup of G"!

Group Multiplication Tables (Cayley Tables)

- E.g. $\{1, -1, i, -i\}$, $\times$

$\times$	1 (iden.)	-1	i	$-i$
1 (iden.)	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

- if headers start with the identity elements
  - ↳ the first row and column just get copied ish?
- * every row and every col has the identity element.
  - ↳ This is because in a group every element has an inverse.
  - (here the inverse of i is $-i$ since their product is 1)

- This group's table is symmetric along the diagonal
  - ↳ this is because this group is abelian: $a \times b = b \times a$
  - ↳ if group was non-abelian, then the Cayley table would not be symmetric about the diagonal.
  - ⇒ can we draw cayley table and find commutativity of a group by checking symmetry about diagonal?

~~There are no duplicated elements~~

* There are no duplicate elements in any row / col. (excluding header)
* each row/col contains all the group elements in some order.

* Proof that this happens ∀ groups

*	g_1	g_2	g_3 (x)	g_4	g_5	g_6	g_7 (y)	g_8	...
g_1									
g_2									
g_3									
g_4 (a)			(Z)				(Z)		
g_5									
g_6									
g_7									
g_8									
⋮									

- Take any finite group.
  Assume there is a row with duplicate elements.
  Let the row be a and cols be x, y.

$a * x = a * y$

$a^{-1} * (a * x) = a^{-1} * (a * y)$

$(a^{-1} * a) * x = (a^{-1} * a) * y$

$1 * x = 1 * y$

$x = y$, but x and y are different.
contradiction!

∴ ∄ any row with duplicate elements.

Similarly, ∄ any col with duplicate elements. ∎ // Q.E.D.

$(R[V, +, \cdot)$

$\cdot b) = V + (a+b)$ | ideals

Order of a group = # of elements in the group's set?

$|G|$ = order of G.

Groups of Order 1, Using Cayley Tables

1) every group must have an identity element called the

*	e
e	e

$\therefore G = (\{e\}, *)$ is called the Trivial group.

Groups of order 2

- first element always e.

*	e	a
e	e	a
a	a	?

→ use the rule about cayley tables where "Every row and every column must contain all the elements of the group in some order!", we proved before.

$\therefore ? = e$. (no duplicates).

+	0	1
0	0	1
1	1	0 ✓

- Only one group of order 2
  - ↳ $\mathbb{Z}$ integers mod 2 $(\mathbb{Z}/2\mathbb{Z}), +$

Groups of order 3

- first e, then a, b say.

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

→ can't be a (already a in row and col)

$\therefore$ b or e.

↳ say: e, then last square must be b

$\therefore$ each row contains all elements in the group

but last col has duplicates $\therefore$ can't put e here. must be b

∴ ∃ only one group of order 3.
(only 1 cayley table)

↳ Notice that this table is symmetric about its diagonal.
∴ Abelian Group

↳ this group is identical to integers mod 3 under +.
↳ the two are "isomorphic groups!"

Group of order 3

*	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

e → 0
a → 1
b → 2

$\mathbb{Z}/3\mathbb{Z}$, +

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

replace e with 0
a with 1
b with 2.
} the two tables would be the same

- filling in a cayley table is like Sudoku.
  ↳ each row and each col must have all elements of the group
  ↳ there can't be any duplicates in a row/col.

Groups of Order 4

- make decisions, see which spots get autofixed.

fully understand a group G, we need to take it apart and study its pieces (i.e. its subgroups).

↳ but how do we find subgroups? ~~[illegible]~~ objects called cosets, help us narrow down the possible list of subgroups.

(if $|G|=n$, $\exists 2^n$ subsets, can't test them all for group condt.)

↳ we use cosets to establish Lagrange's Theorem, which narrows down the possible subgroups of G from 2^n to a smaller list.

↳ its linked to the size of subgroups?

(assume finite group henceforth)

- Subgroup = subset ∧ group itself.
  H is a subgroup of G: $H \leq G$
- Two standard sub-groups of G
  1) G
  2) $\{e\}$

  } like saying every integer has two divisors, itself and 1.

Lagrange's Theorem

- If $H \leq G$, then the order of H divides the order of G.
  $H \leq G \rightarrow |H|$ divides $|G|$
- This means that subgroups cannot be of any arbitrary size, ∃ strong restrictions on the possible sub-groups of G.
- Let $|G| = 323 = 17 \times 19$.
  divisors of 323: 1, 17, 19, 323 → $\{e\}$ → G.
  ∴ possible subgroup orders: 1, 17, 19, 323

  does LT say there are subgroups of order 17 & 19? NO!

  ∴ IF G has any other subgroups, their orders must be 17 or 19. ($H \leq G \rightarrow |H|$ divides $|G|$ is NOT a biconditional)

• e.g.) A_4: Alternating group on 4 elements.

order: $|A_4| = 12$

divisors: 1, 2, 3, 4, 6, 12

* A_4 does NOT have a subgroup of order 6.

subgroups

order 1: 1
order 2: 3
order 3: 4
order 4: 1
→ order 6: 0
order 12: 1

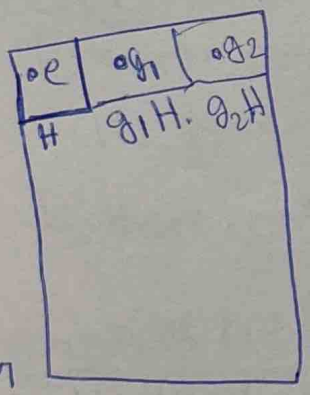
Proof of Lagrange's Theorem: if $H \leq G$, then $|H|$ divides $|G|$

• Let G be a finite group s.t. $|G| = n$

case 1: $\{e\} \leq G$ and $|\{e\}| = 1$, 1 divides n ✓

case 2: $G \leq G$ and $|G| = n$, n divides n ✓

case 3: $H < G$ and $H \neq \{e\}$
↓ proper subgroup. (smaller than G)
↳ not the trivial group $\{e\}$.



→ ∵ H is a group, it must contain e.
∴ the identity element for both G and H lies inside the H square.

Construction:

→ Pick $g_1 \in G$ not in H.

→ consider the set $g_1H = \{g_1 \cdot h \text{ for all } h \in H\}$ "Left Coset"

* ⇒ claim: H and g_1H do not overlap i.e. $H \cap g_1H = \emptyset$

assume there is an element in H and g_1H.

$\Rightarrow g_1 h_i = h_j$ for some h_i, h_j in H.

$(g_1 h_i) h_j^{-1} = h_j \cdot h_j^{-1}$

$g_1 (h_i h_i^{-1}) = h_j \cdot h_i^{-1}$

$g_1 = h_j \cdot h_i^{-1} \in H$ contradiction ∵ we picked g_1 not in H.

∴ claim is true, H and g_1H are disjoint.

eat this process until there is no element in G which is not in a coset.

- Pick $g_2 \in G$ not in H or g_1H.

Consider the left coset $g_2H = \{g_2h \text{ for all } h \in H\}$

*Claim1: H and g_2H do not overlap. (same as before)

*Claim2: g_1H and g_2H do not overlap.

Assume g_1H and g_2H overlap

$\Rightarrow g_1h_i = g_2h_j$ for some h_i, h_j in H.

$(g_1h_i)h_j^{-1} = (g_2h_j)h_j^{-1}$

$g_1(h_ih_j^{-1}) = g_2(h_jh_j^{-1})$

$g_1h_k = g_2$

$g_1h_k \in g_1H \Rightarrow g_2 \in g_1H$, contradiction $\because$ we chose g_2 not in g_1H.

$\therefore$ claim is true.

$\Rightarrow$ 

continue the same process till there is no element left that is not in a coset.

$\Rightarrow$ Result: G is split into non-overlapping left cosets:

$H, g_1H, g_2H, \ldots, g_nH$

*Claim: all cosets are the same size

Pick a left coset gH and suppose it contains a duplicate element

$\Rightarrow gh_1 = gh_2$ for different elements h_1, h_2.

$g^{-1}(gh_1) = g^{-1}(gh_2)$

$h_1 = h_2$ contradiction

$\Rightarrow$ each coset has size $|H| = d$ (say).

$\therefore$ each coset has d elements.

*H is a subgroup. The other cosets are NOT groups, they are just sets $\because$ only H contains e

$\Rightarrow$ Let the no. of cosets be k: called the index of H in G $\equiv |G:H| = k$

$\Rightarrow d \cdot k = n \Rightarrow d \mid n \equiv |H| \mid |G|$ // Q.E.D.

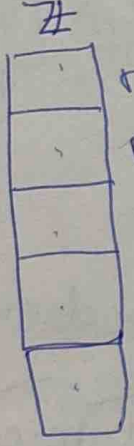
Summary of Proof:

1) Pick a subgroup $H \leq G$
2) Cover G with cosets (LHR work)
3) Show cosets don't overlap
4) Show cosets are all the same size.

Normal Subgroups and Quotient Groups

- Modular Arithmetic (Gauss)
  - ↳ takes $\mathbb{Z}$, partitions them into a finite no. of sets and treats each set as a new type of number.
- how do we adapt modular arithmetic in group theory?
  - ↳ use Normal Subgroups and Quotient Groups.

- e.g.) Integers mod 5
  - ↳ divide the integers into 5 sets depending on the remainder we get when we divide by 5



$\mathbb{Z}$

$r=0$: $\{\ldots, -10, -5, 0, 5, 10, \ldots\}$
$r=1$: $\{\ldots, -9, -4, 1, 6, 11, \ldots\}$
$r=2$: $\{\ldots, -8, -3, 2, 7, 12, \ldots\}$
$r=3$: $\{\ldots, -7, -2, 3, 8, 13, \ldots\}$
$r=4$: $\{\ldots, -6, -1, 4, 9, 14, \ldots\}$

* any no. with rem = 1 added with any no. with $r=2$, we get a no. with $r=3$
2 sets + 4 sets → 1 set

- these sets are called congruence classes $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}$
- $\mathbb{Z} \bmod 5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ (treat the sets as if they are numbers) forms a group under $+$.
- if a, b belong to the same congruence class we write $a \equiv b \pmod{n}$
- ↳ set $\bar{0}$ with multiples of 5 is identity.
  - each set has an inverse $\bar{2} + \bar{3} = \bar{0}$.

• $(R/U, +, \cdot)$

$\cdot\cdot$ $1+(a+b)$

(1): different perspective of the same:

Group: integers $\mathbb{Z}$, under +

Subgroups: has ∞ no. of subgroups

$\mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}, 4\mathbb{Z}, 5\mathbb{Z} \ldots$

↑ subgroup of the multiples of 5

$5\mathbb{Z} = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$ every int. in this subgroup has r=) when div by 5.

$1+5\mathbb{Z} = \{\ldots, -9, -4, 1, 6, 11, \ldots\} \leftarrow$ "coset"

$2+5\mathbb{Z} = \{\ldots, -8, -3, 2, 7, 12 \ldots\} \leftarrow$ "coset"

$3+5\mathbb{Z} =$

$4+5\mathbb{Z} =$

) numbers that are not already in this set and adding it to generate a new "coset"

stem from?

>where does the thought of choosing

• 1 is not in the subgroup $5\mathbb{Z}$, if we add 1 to every number in the subgroup we get a new set. (all ints of the form $5k+1$).

* $1+5\mathbb{Z}$ is called a coset. It is NOT a subgroup

- x not closed
- x no inverses
- x no identity element

} not a group

• this coset is disjoint from the subgroup $5\mathbb{Z}$

* 2 is not in any of the above sets.

∴ add 2 to each element of $5\mathbb{Z}$ to make a new coset.

∴ after $4+5\mathbb{Z}$, the original group $\mathbb{Z}$ is covered by one subgroup $5\mathbb{Z}$ and 4 cosets.

(5 subgroup $5\mathbb{Z}$ can also be thought of as the coset $0+5\mathbb{Z}$

* We used $5\mathbb{Z}$ (subgroup) to partition the group $\mathbb{Z}$ into 5 cosets, which form the group $\mathbb{Z}$.

* Since all the 5 cosets form a group, we call $5\mathbb{Z}$ a "Normal Subgroup", and the group of cosets is called a "Quotient Group"

• $\mathbb{Z}/5\mathbb{Z}$ ⇒ using the subgroup $5\mathbb{Z}$ to divide the gr... $\mathbb{Z}$ into cosets.

* These cosets (5) can be treated as the elements of a new group "coset group"

e.g. Adding cosets:

$(1+5\mathbb{Z}) + (3+5\mathbb{Z}) = 4+5\mathbb{Z}$

* Group: $\mathbb{Z}$
Normal Subgroup: $5\mathbb{Z}$ } → used these too to create a quotient group out of the cosets.
Quotient group: $\mathbb{Z}/5\mathbb{Z}$

$\mathbb{Z}/5\mathbb{Z} \not\leq_G \mathbb{Z}$ → completely different idea. Quotient group's elements are sets.

• Generalisation:

Group: G;
Subgroup: N

→ Use N to make a collection of ~~cosets~~ non-overlapping cosets

$N, g_1N, g_2N, \ldots, g_nN$.

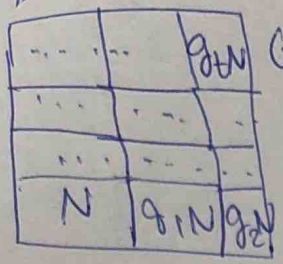
↳ N is a subgroup, while the other cosets are just sets (no e)

Q) do the cosets always form a group? NO!

↳ if the cosets don't form a group, we don't call N a normal subgroup, and we cannot make a quotient group.

What properties must the subgroup N have for the cosets to form a group?

9) Assume N divides G into t different cosets (left cosets)



- each left coset is of the form gN for some $g \in G$

Pick two cosets xN, yN $(x, y \in G)$

$\because e \in N$ ($\because N$ is a subgroup, it contains identity)

$\Rightarrow x \cdot e = x \in xN$ and $y \cdot e = y \in yN$

$g_1 g_2 = g_3 \in G$.
$g_3 \in g_3 N$.
$\because g_1 \in g_1 N, g_2 \in g_2 N$.
$g_1 g_2 \in g_1 g_2 N$.

* For cosets to act like a group:

(using closure?) $x \cdot y \in (xN)\cdot(yN)$?

i.e $(xN)(yN) = xyN$

if this is true, the product of any element in the coset xN with any element in the coset yN should lie in the coset xyN.

↳ When does this happen?

Pick an element from xN. let it be $x \cdot n_1$

Pick an element from $yN \Rightarrow y \cdot n_2$

* take an element in coset $1+5\mathbb{Z}$ and add with any element in $2+5\mathbb{Z}$, it is always in $3+5\mathbb{Z}$???

$(x n_1)\cdot(y \cdot n_2)$ if $\in xyN$, $(xn_1)\cdot(yn_2) = xyn_3$

$n_1 y n_2 = y n_3$

$= y^{-1} n_1 y n_2 = n_3$

$y^{-1} n_1 y = n_3 n_2^{-1} \in N$

$y^{-1} n_1 y \in N \Rightarrow y^{-1} N y \subseteq N$

let $n_1 \in N$.
$n_1 \in eNe$
$n_1 \in yy^{-1}Nyy^{-1}$
$n_1 \in y(y^{-1}Ny)y^{-1}$

claim: $y^{-1} N y \in N$ (conjugate)

$\Rightarrow$ if $(xN)(yN) = xyN$, then $y^{-1}Ny = N$

cosets do form a group:

Identity: $N = eN \Rightarrow (eN)(gN) = egN = gN$

Inverses: $(gN)^{-1} = g^{-1}N$. $\because (gN)(g^{-1}N) = (gg^{-1})N = eN$ identity.

∴ if $N \leq G$ and cosets form a group

$\Updownarrow$

$y^{-1} N y = N$ for any $y \in G$
(conjugate of N)

- Proof: (other dir^n)

Let $y^{-1} N y = N \ \forall y \in G$.

Claim: the cosets form a group.

Pick two cosets xN, yN, multiply two arbitrary elements in these cosets

$(xn_1)(yn_2) =$

$= x \cdot (yy^{-1}) n_1 y n_2 = xy(y^{-1} n_1 y) n_2$

$y^{-1} n_1 y \in N$, let it be n_3.

$= xy\, n_3 n_2$; $n_3 n_2 \in N$ call it n_4

$= xy\, n_4 \in xyN$

↳ element of this coset. ∴ $(xN)(yN) = xyN$.

⇒ The cosets do form a group

∴ Let $N \leq G$,

cosets form a group iff $y^{-1} N y = N$ for any $y \in G$.

When this is true, N is called a normal subgroup of G

" $N \trianglelefteq G$ "

↳ the group of cosets is called a Factor Group

" G/N "

Identity: N

inverse of xN is $x^{-1}N$.

very group has two subgroups, $\{e\}$ and $\{G\}$.
These are also Normal subgroups.

↳ if G has no other Normal subgroups then G is called a simple group.

↳ A simple group does not have any factor groups. They are generally the building blocks of other groups.

Q) Find a normal subgroup of S_8.

Cyclic Groups

- A group G is cyclic if it can be generated by a single element.

Q) Let G be a group with operation $*$.
Pick $x \in G$. What's the smallest subgroup of G that contains x?

Multiplicative Dgn:

1) any group that contains x must also contain x^{-1}.
2) It must contain the identity element.
3) to be closed under the operation, it has to contain all powers of x and x^{-1}

↳ This is how we construct the group generated by some element x.

$\langle x \rangle = \{\ldots x^{-3}, x^{-2}, x^{-1}, 1, x, x^2, x^3, \ldots\}$; This is the group generated by x. It is the smallest subgroup of G that contains x.

* if G has one element x s.t. $\langle x \rangle = G$, then G is a cyclic group.

Additive Notation

- let H be a group with operation +.
  pick $y \in H$.
  $\langle y \rangle = \{-3y, -2y, -y, 0, y, 2y, 3y, \dots\}$; This is the group generated by y; and is the smallest subgroup of H containing y.
  1) Any subgroup containing y must also contain $-y$.
  2) It must also contain the identity 0
  3) To be closed under the operation, it must also contain all multiples of y and $-y$.
- if $H = \langle y \rangle$ for some $y \in H$, then H is a cyclic group.

E.g.)

- Consider $\mathbb{Z}$ under +
  claim: $\mathbb{Z} = \langle 1 \rangle$.
  $\langle 1 \rangle = \{1$, its inverse -1, the identity $(1+-1=0)$, and all multiples of 1 and $-1\}$. $= \mathbb{Z}$ //

  $\therefore$ $\mathbb{Z}$ under + is a cyclic group (∞ cyclic group)

- Group: G = integers mod n under addition. $\mathbb{Z}/n\mathbb{Z}$ (Z mod n)
  Elements: $\{0, 1, 2, \dots, n-1\}$
  G is cyclic: $G = \langle 1 \rangle$.

  ($\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ are the only cyclic groups)

  $\langle 1 \rangle = \{\dots -2, -1, 0, 1, 2, \dots, n-1, n, n+1, n+2, \dots, 2n-1, 2n, 2n+1 \dots\}$
  $\downarrow$
  $\{n-2, n-1, 0, 1, 2, \dots, n-1, 0, 1, 2, \dots, n-1, 0, 1 \dots\}$

  $n \equiv 0 \bmod n$
  $n+1 \equiv 1 \bmod n$
  $-1 \equiv n-1 \bmod n$
  $-2 \equiv n-2 \bmod n$

  $\therefore \langle 1 \rangle = \{0, 1, 2, \dots, n-1\}$
  $\hookrightarrow$ cycles through 0 to $n-1$ over and over again.

  * $\mathbb{Z}$ mod n under + is a finite cyclic groups.

(1)...
The Fundamental Theorem on Finitely Generated Abelian Groups states that any finitely generated abelian group can be broken apart into a finite number of cyclic groups.

- Every cyclic group is $\mathbb{Z}$ or $\mathbb{Z}/n\mathbb{Z}$.
  ↳ these are the building blocks of finitely generated abelian groups.

Group Homomorphisms

- Say we have two groups G_1 and G_2.
  ↳ How do we compare them? How can we tell how similar or how different they are? What do we mean by similar? What features of the groups are we using to compare?
  ↳ Use a homomorphism.

$\mathbb{Z}$ (integers)
operation: +
↑
infinite group

$\mathbb{Z}/2\mathbb{Z}$ (integers mod 2) → quotient group of cosets: $\{\bar{0}, \bar{1}\}$.
operation: +
↑
finite group.

$\mathbb{Z} = \{\text{evens}\} \cup \{\text{odds}\}$

even + even = even
even + odd = odd
odd + even = odd
odd + odd = even.

(by replacing 'even' with 0, 'odd' with 1) ⟷ these two are saying the same thing

$0+0 \equiv 0 \bmod 2$
$0+1 \equiv 1 \bmod 2$
$1+0 \equiv 1 \bmod 2$
$1+1 \equiv 0 \bmod 2$.

- $\mathbb{Z} = \{\text{evens}\} \cup \{\text{odds}\}$: by splitting the integers into two sets, we see these two sets behave exactly the same as the group $\mathbb{Z}/2\mathbb{Z}$.

• formally:

$f: \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$

even → 0

odd → 1

* can we create a reverse function that encodes our observation that evens and odds behave like $\mathbb{Z}/2\mathbb{Z}$?

NO!

• Eg.)

* behaviour of elements in the o/p should be similar to behaviour of elements in the i/p.

• $g: \mathbb{Z}/\mathbb{Z} \to \mathbb{Z}$

$0 \bmod 2 \to x$ for some integer x (0)

$1 \bmod 2 \to y$ for some integer y (0)

$0+0 \equiv 0 \bmod 2 \longrightarrow x+x=x$

$\Rightarrow x=0.$

$1+1 \equiv 0 \bmod 2 \longrightarrow y+y=0 \Rightarrow y=0$ hmmm.

g does not encode our observation about the similarity b/w evens and odds and the integers mod 2.

: When using functions to compare two groups, the direction can matter.

eg.) Group 1: $\mathbb{Z}/\mathbb{Z}$ under +

Group 2: $\{1, -1, i, -i\}$, under ×.

To compare these groups, let's look at the cayley tables

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

×	1	-1	i	-i
1	1	-1	i	-i
-1	-1	1	-i	i
i	i	-i	-1	1
-i	-i	i	1	-1

switch order of headers.

we can see a pattern.

$0 \leftrightarrow 1$

$1 \leftrightarrow i$

$2 \leftrightarrow -1$

$3 \leftrightarrow -i$

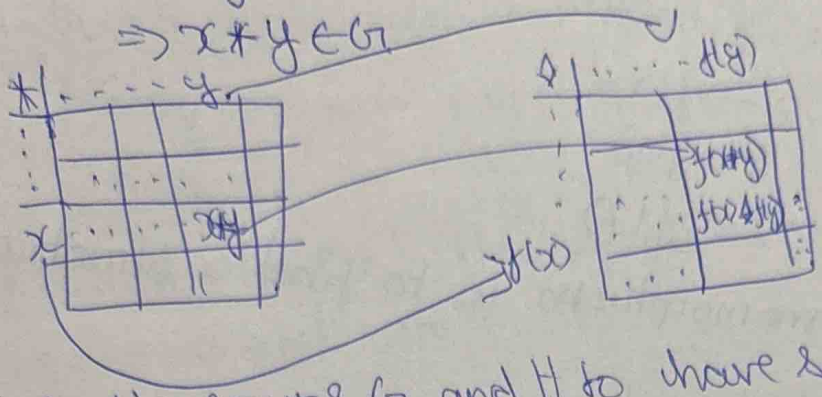
$\Rightarrow$ these two groups just use diff. elements and a diff. operation, other than that they are all the same.

↳ we say these two groups are isomorphic ("equal form").

Generalisation:

Consider two groups $(G,*)$ $(H,\diamond)$.
(They can be finite, ∞, abelian anything)

- choose any two elements $x, y \in G$.



* for the groups G and H to share similar group behaviour, $x, y, x*y$ must correspond to elements in H.

formally; $f: G \to H$, sends this part of the multiplication table for G to a similar part of the multiplication table for H.

$\Rightarrow f(x) \diamond f(y) = f(x*y)$ $\Rightarrow$ This type of function is what we use to compare two groups.

- Any function $f: G \to H$ $(G,*)$ $(H,\diamond)$ s.t. $f(x*y) = f(x) \diamond f(y)$ (group, group)
  is a tool we can use to compare G and H.
  1> such f's are called Group Homomorphisms.

- e.g.) $f: \mathbb{Z} \to \mathbb{Z}$, group operation $+$.
  $f(x) = 2x$. is f a homomorphism?
  ~~$f(x+x) = f(x) + f(x)$~~ need to show $f(x+y) = f(x) + f(y)$
  ~~$f(2x) = 2f(x)$.~~
  ~~$2x = 2x$ yes!~~ $2(x+y) = 2x+2y$ □ ∴ YES.

*notice that the dp of f is $2\mathbb{Z}$, $2\mathbb{Z} \leq \mathbb{Z}$.

• homomorphisms are ways to compare two groups for structural similarity.

↳ it is a function btw two groups which preserves the group structure in each group.

• consider $(G, *)$ (H, Δ), $f: G \to H$

pick $x, y \in G$ $\quad x \to f(x)$

$*x*y = z \in G$. $\quad y \to f(y)$

$z \to f(z)$

The whole point of a homomorphism is to find a structural similarity in two groups.

So if $x*y = z$ in G

we want $f(x) \Delta f(y) = f(z)$ in H. but $z = x*y$.

$\Rightarrow \boxed{f(x*y) = f(x) \Delta f(y)}$ → definition of a homomorphism

• e.g. $G = \mathbb{R}$ under $+$, $H = \mathbb{R}^+$ under $\times$

G is abelian, identity 0.

H is abelian, identity 1.

Consider $f: G \to H$, $f(x) = e^x$

is it a homomorphism?

$f(x+y) = f(x) \times f(y)$

$e^{x+y} = e^x \times e^y = e^{x+y}$ ∴ YES! //

• e.g. $G = \mathbb{R}$, under $+$

$H = \{z \in \mathbb{C} : |z| = 1\}$, under $\times$. is indeed a group.

↳ every complex no. $z \in \mathbb{C}$ with $|z| = 1$ can be written as $z = e^{i\theta}$.

let $f: G \to H$ $f(x) = e^{ix}$. is f a homomorphism?

is $f(x+y) = f(x) \times f(y)$

$e^{i(x+y)} = e^{ix} \times e^{iy} = e^{ix+iy} = e^{i(x+y)}$ ∴ YES! //

* not 1 to 1 mapping

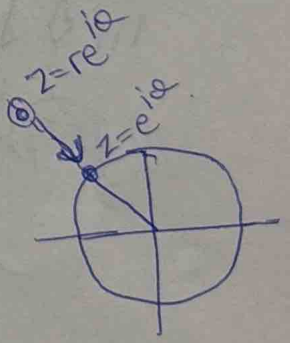
Homomorphisms do not have to be one-one mappings.

same shape

elements two groups are identical.
↳ then the function is called an isomorphism and the groups are isomorphic.

- $(G_1, *)$ (H, Δ)
  $f: G \to H$ homomorphism s.t. $f(x*y) = f(x) \Delta f(y)$.
  ↳ may not be 1-1 mapping (injection)
  may not be onto (surjection).
- if G, H are identical then we need the homomorphism f to be one-one and onto.
- An isomorphism is a homomorphism that is one-one and onto.
- e.g.) $G = \mathbb{R}^+$ under $\times$ $\log: G \to H$ is a homomorphism.
  $H = \mathbb{R}$ under $+$ $\log(x*y) = \log x + \log y$ ✓ Yes

  is $\log: G \to H$ an isomorphism?
  i) is log one-one?
  let $\log x_1 = \log x_2$
  $e^{\log_e x_1} = e^{\log_e x_2} \Rightarrow x_1 = x_2$ ∴ one-one.
  ii) is log onto? range $= (-\infty, \infty)$ ✓ ∴ onto
  ∴ the homomorphism $\log G \to H$ is a bijection ∴ it is an isomorphism
  $\Rightarrow G, H$ are isomorphic.
- e.g.) G_1 = non-zero complex numbers under $\times = \mathbb{C}^*$
  → no inverse for 0 under multiplication.
  S^1 = complex numbers z with $|z| = 1$ under $\times$
  (note: $z = re^{i\theta}$ ✗; S ⇒ sphere (1) ⇒ dimension)



$f: \mathbb{C}^* \to S^1$ $f(re^{i\theta}) = e^{i\theta}$ Yes. f is a homomorphism.
$f(r_1 e^{i\theta_1} \times r_2 e^{i\theta_2}) = e^{i\theta_1} \times e^{i\theta_2}$ but not 1-1 clearly (many-1).
$f(r_1 r_2 e^{i(\theta_1+\theta_2)}) = e^{i(\theta_1+\theta_2)} = e^{i(\theta_1+\theta_2)}$ ∴ not isomorpheism
✓ onto though.

The Kernel of a Group Homomorphism

- a homomorphism does not have to be one-one.

  ↳ then ∃ a group associated with that homomorphism which measures the degree to which the function is not an injection. This group is called the kernel.

- homomorphisms map
  identities → identities
  inverses → inverses

- $(G,*), (H, \Diamond)$ $f: G \to H$ is a homomorphism $\Rightarrow f(x*y) = f(x) \Diamond f(y)$.

i) $f: 1_G \to 1_H$.

pick any $x \in G$, $x \neq 1_G$.

$x * 1_G = x$

$f(x * 1_G) = f(x)$

$f(x) \Diamond f(1_G) = f(x)$

$f(x)$ is an element in H, call it y.

$y \Diamond f(1_G) = y$

$y^{-1} \Diamond y \Diamond f(1_G) = y^{-1} \Diamond y$

$1_H \Diamond f(1_G) = 1_H$

$\Rightarrow f(1_G) = 1_H$

ii) inverses → inverses

Let $x \in G$.

$f(x) = y \in H$.

Show $f(x^{-1}) = y^{-1}$.

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

$f(x * x^{-1}) = f(1_G)$

$f(x) \Diamond f(x^{-1}) = 1_H$.

$y \Diamond f(x^{-1}) = 1_H$

$y^{-1} \Diamond y \Diamond f(x^{-1}) = y^{-1} \Diamond 1_H$.

$1_H \Diamond f(x^{-1}) = y^{-1}$

$f(x^{-1}) = y^{-1}$ //.

(1+a) Definition:

⇒ suppose f is not one-one. Then $\exists$ at least two elements in G_1 which map to the same element in H.

Let $x_1, x_2 \ldots \to y$.

$f(x_i) = y \Rightarrow f(x_i^{-1}) = y^{-1}$ simplify RHS.

$\Rightarrow f(x_1) = y \Rightarrow f(x_1) \Delta f(x_1^{-1}) = y \Delta f(x_1^{-1}) = 1_H$

$f(x_2) = y \Rightarrow f(x_2) \Delta f(x_1^{-1}) = y \Delta f(x_1^{-1}) = 1_H$

$\Rightarrow f(x_1 * x_1^{-1}) = 1_H$

$f(x_2 * x_1^{-1}) = 1_H$

} this shows that there are multiple elements in G_1 which all map to 1_H.

these elements are called

- the kernel of f and: $\ker(f) = \{x \in G_1 \mid f(x) = 1_H\}$.

* the kernel is a property of the homomorphism (non-injective) and not of the groups.

- it is not obvious that there are always elements in $\ker(f)$ other than e, but there are!

if f is not 1-1, then $\ker(f)$ has more than 1 element.

$f(1_{G_1}) = 1_H$ so $1_{G_1} \in \ker(f)$ always.

- if $|\ker(f)| = 1$, then f is one-one

$\ker(f) \subseteq G_1$.

* $\ker(f)$ is a subgroup of G_1.

① show that the kernel of $f: G_1 \to H$ is a subgroup of G_1.

ez. done.

Order of an Element

- Group G with identity e.
  The order of $x \in G$ is the smallest positive integer n such that $x^n = e$.

- order of $x = |x| = n$.
- if there is no positive power of x which gives us the identity, then we say x has infinite order.

e.g.) $\mathbb{R}^\times$, multiplication ($\in$ to 3).
identity $= 1$
$|1| = 1 \Rightarrow |e| = 1$ in any group.
$|-1| = 2$
no other non-zero real can be raised to a positive number to give 1. $\therefore$ all other reals have ∞ order.

g.) $\mathbb{C}^*$.
identity $= 1$.
$\exists$ infinite z s.t. $z^n = 1$ (nth roots of unity)
$|i| = 4$

:) $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, where $a, b, c, d \in \mathbb{R}$.
operation: matrix multiplication
To have an inverse, $\begin{vmatrix} a & b \\ c & d \end{vmatrix} \neq 0$
he group of such matrices is called the "general linear group".
$GL_2(\mathbb{R})$; General Linear 2×2 matrices with Real entries.

$\therefore M = \begin{pmatrix} \frac{\sqrt{3}}{2} & -\frac{1}{2} \\ \frac{1}{2} & \frac{\sqrt{3}}{2} \end{pmatrix}$ rotation matrix → rotates $\vec{v}$ in the plane

$M^{12} = I \therefore |M| = 12$

Symmetric Groups

- S_n = Group of permutations on a set with n elements.
- A permutation is just a re-arrangement of the set.
- $|S_n| = n!$
- e.g) S_3 := permutations of $\{1,2,3\}$.

$$\left.\begin{matrix} 1\,2\,3 & 1\,3\,2 \\ 2\,1\,3 & 2\,3\,1 \\ 3\,1\,2 & 3\,2\,1 \end{matrix}\right\} \text{elements of } S_3.$$

What is the operation? How do you combine two permutations?

↳ $\begin{matrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{matrix}$ take 123, replace 1 with 2, 2 with 3, 3 with 1 to get 231.

- a permutation acts like a function $f: \{1,2,3\} \to \{1,2,3\}$.

$123 \to 231 \Rightarrow f(1)=2,\ f(2)=3,\ f(3)=1$

- the operation in S_3 is function composition.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} * \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \left.\begin{matrix} \to \text{i/p} \\ \to \text{o/p} \end{matrix}\right\} \text{permutation.}$$

* like function composition → do the right one first.

$1 \to 4$ and in the outer one $4 \to 2 \therefore$ after composing $1 \to 2$

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}.$$

* The only abelian symmetric groups are S_1, S_2
  ↳ $S_3, S_4 \ldots$ are all non-abelian.

* Every finite group is a subgroup of a symmetric group.
  ↳ Cayley's Theorem

Cycle Notation for Permutations

- $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 1 & 2 \end{pmatrix} \equiv (1 \to 3 \to 4)(2 \to 5)$
  3-cycle 2-cycle aka Transposition

- $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix} = (2 \to 4 \to 1)(3)(5)$ (no need to start with 1)
  ↳ expressed as a product of three cycles

- 1 cycles can be ignored (same number is mapped to itself)

  $(4 \to 1 \to 2)$, $(1 \to 2 \to 4)$ } the same cycle.

* When we decompose a permutation into products of cycles the order of the cycles does not matter.
  ↳ Why?
  any number is present in only one of the cycles, so the cycles commute with each other.

$a = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ $b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ → both cycles contain $(1 \to 3)$ ∴ the cycles don't commute eachother.

$a = (1 \to 3 \to 2)$ $b = (1 \to 3)$

$a \cdot b = (1 \to 3 \to 2) \cdot (1 \to 3)$
  1 ⇒ 3 by transposition
  3 ⇒ 2 by 3-cycle

$= (1 \to 2)(3)$

$a \cdot b = (1 \to 2)$

$b \cdot a = (2 \to 3)$

$1 + (a \neq b)$ ∴ Trivial

what is the order of the following cycles?

a) $|(a \to b)|$ c) $|(a\ b\ c\ d)|$

b) $|(a\ b\ c)|$ d) $|(1\ 2\ 3 \dots n)|$.

a) let $f = (a \to b)$

$f^2 = (a\ b)(a\ b) = \begin{pmatrix} a & b \\ a & b \end{pmatrix}$ ∴ order = 2.

b) let $f = (a\ b\ c)$

$f^2 = (a\ b\ c)(a\ b\ c) = \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix} =$

$f^3 = f \circ f \circ f$

$f \circ f^2$ only !!!

~~$f^3 = (a\ b\ c)(a\ b\ c) = (c\ a\ b)$~~

$f^3 = (a\ b\ c)(c\ a\ b) = (c$ etc you get the gist

*order of an n-cycle is n.

Dihedral Group

- We can create a group from any geometric shape by looking at the symmetries of the shape.
  - ↳ symmetries are flips or rotations performed on the shape so that it looks the same b4 and after.
  - ↳ when the shape is a regular polygon, the group of symmetries is called a Dihedral Group. (two faces)
- Examine the symmetries for a regular polygon with n-sides
  - ↳ simplest transformation = do nothing = e identity symmetry
  - ↳  CW rotation through a only. $\theta = \frac{360^\circ}{n} = \frac{2\pi^c}{n} = r$ symmetry.
  - ↳ repeated applications of r give us other symmetries $r^2, r^3, \dots, r^n = e$
  - ↳

↳ other elements of symmetries is reflection.

↳ if the polygon has n sides, $\exists$ n different

↳ if the polygon has an odd no. of sides, the axes of symmetry are the lines through the vertices

if even, lines through vertices + lines through midpoints of edges.

- consider the transformation about the vertical axis

call it f. $\Rightarrow f^2 = e$.

* the remaining symmetries are obtained by r's and f's.

$r^n f = f$.

$\therefore$ $\left.\begin{matrix} e, r, r^2, \dots, r^{n-1} \\ f, rf, r^2 f, \dots, r^{n-1} f \end{matrix}\right\}$ $\exists$ $2n$ symmetries for an n sided polygon.

$\therefore |D_n| = 2n$, D_n is not commutative.

- combining transformations is like function composition
- for an equilateral Δle: h $\left.\begin{matrix} e, r, r^2 \\ f, rf, r^2 f \end{matrix}\right\}$ are the symmetries.

$|r| = 3$, $|f| = 2$

- for an isosceles Δle, do nothing / flip are the only transformations possible.
- for a scalene triangle, e is the only transformation.

	finite groups	Infinite groups
abelian	Integers mod n under +	$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ under +
non-abelian	S_n for $n>2$	Matrices. $GL_n(\mathbb{R})$

- $SL_n(\mathbb{R})$ Special linear groups = $n \times n$ matrices with det 1 is a group.

- The building blocks of finite groups are simple groups

Direct Products of Groups

- one of the ways to piece simple groups together to form ~~more complicated~~ larger groups.

- $G_1 \times G_2 = \{(x,y) \mid x \in G_1, y \in G_2\}$.
  - $(a,b) \cdot (x,y) = (a \cdot x, b \cdot y)$
  - identity $= (e_1, e_2)$; e_1 = identity in G_1, e_2 = identity in G_2.

- eg) $G_1 = \mathbb{Z}$ under +
  $G_2 = \{1, i, -1, -i\}$ under $\times$
  $G_1 \times G_2 = \{(x,y) \mid x \in \mathbb{Z}, y = \pm 1 \text{ or } \pm i\}$
  $(7,-1) * (-3,i) = (4,-i)$
  identity $= (0,i)$
  inverse of $(12,-i) = (-12,i)$

- we can take dir. products of more than 2 groups.
  - operations are performed component wise
  - If $G = G_1 \times G_2 \times \cdots \times G_n$, $|G| = |G_1| \times |G_2| \times \cdots \times |G_n|$.

- $G = \mathbb{R} \times S_3 \in$ non-abelian. $\therefore$ G is non-abelian.
  ($\mathbb{R}$: abelian)

Let $G = G_1 \times G_2 \times \dots \times G_n$.
say G_i is non abelian $\rightarrow \exists\, a, b \in G_i$ with $a \cdot b \neq b \cdot a$.

$x = (a, e_2, e_3, \dots, e_n)$
$y = (b, e_2, e_3, \dots, e_n)$ $\Big\}$ $xy \neq yx$

- if all G_i's are abelian, G is abelian.

• $G = \mathbb{R} \times S_3 \in$ non-abelian. ∴ G is non-abelian.

Ring Theory

• Eg.) $\mathbb{Z} \subset \mathbb{R}$, $\mathbb{R}^{2\times3} = \{2\times3 \text{ matrices with real entries}\}$.

$\mathbb{C}[x] = \{\text{complex coeff. polynomials}\}$.

arithmetic operations: $+ - \times \div$; abstract algebra operations: $+, \times$.

	$+$	$-$	$\times$	$\div$ (closure)
$\mathbb{Z}$	✓	✓	✓	×
$\mathbb{R}$	✓	✓	✓	✓
$\mathbb{R}^{2\times3}$	✓	✓	×	×
$\mathbb{C}[x]$	✓	✓	✓	×

• A ring is a set R with two operations: $+, \times$.

↳ Both operations are closed.

↳ $(R, +)$ form an abelian group

↳ $(R, \times)$ is closed and associative only. ("ring with identity" ↔ (ie for $\times$ is debateable).

↳ these two operations are linked by a distributive property: $a\cdot(b+c) = a\cdot b + a\cdot c$

$(b+c)\cdot a = b\cdot a + c\cdot a$

• Types of Rings

↳ if a ring is commutative, we call it a comm. ring

↳ if a ring has multiplicative inverses under $\times$, its called a division ring.

↳ if a division ring is commutative, we call it a field.

• e.g.) Integers $(\mathbb{Z}, +, \times)$ is a ring.

↳ $+, -, \times$ $\mathbb{Z}$s.

cannot $\div$,

$+$ is commutative.

$\times$ is commutative.

↳ commutative ring with identity.

e.g.) (Real Polynomials, $+, \times$)

$+, -, \times$ any two poly. to get a new polynomial.

$+$ is abelian, identity $= 0$. for $+$

$\times$ is associative.

$\times$ is commutative for real polynomials

$\times$ has its identity (1), no inverse

$\mathbb{R}[x]$ = set of all polynomials with real coeff.

• Polynomial Ring:

coefficients of the polynomial can be

↳ integers

↳ complexes

↳ $\mathbb{Z}/n\mathbb{Z}$

↳ Matrices

} given a ring R, we can make a new ring R[x] = set of all polynomials with coefficients in R.

e.g.) $(2\mathbb{Z}, +, \times)$

abelian with $+$.

associative, commutative

but multiplicative element identity $\notin R$.

(Matrices, $+, \times$) are examples of non-commutative rings.

but they have their identity element.

$R = \left\{ \begin{pmatrix} 2a & 2b \\ 2c & 2d \end{pmatrix} \right\}$. not commutative, no identity.

... x Gn.

let ?
- commutative: $\mathbb{Z}$
- non-commutative: $\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\}$
- identity: $\mathbb{R}[x]$
- no identity: $2\mathbb{Z}$

- all infinite
- are there rings with only ∞ finite number of elements?

- Integers mod n are a finite ring with n elements.

$\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \dots, n-1\}$ "Quotient Group" notation. (group of cosets)

↑ group ↑ normal subgroup

This notation is carried over to rings.

$\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \dots, n-1\}$ "Quotient Ring"

ring ↗ ideal

finite ring, commutative, has identity! $\Rightarrow \forall n \in \mathbb{N}$.

* $\mathbb{Z}/p\mathbb{Z} = \{0, 1, 2, \dots, p-1\}$ is a field, if p is prime.

- finite non commutative ring: $GL_n(\mathbb{Z}/n\mathbb{Z})$.

Units In A Ring

- R does not form a group under x. multiplicative inverses of all elements may not exist in the ring (except 0 etc.).

* Elements in R which have an inverse under multiplication are called units.

Units form a group under x.

abelian

- Let R be a ring.
  $x \in R$ is a unit if $x \cdot y = 1 = y \cdot x$ for some $y \in R$.
  ↳ Set of all units of R is denoted by $R^\times$

e.g.) Ring: $(\mathbb{Z}, +, \times)$
multiplicative identity $= 1$
$R^\times = \{-1, 1\}$ ∵ $-1 \times -1 = 1$, $1 \times 1 = 1$ ∴ they are units of R.
no other integer has an inverse.
$R^\times = \mathbb{Z}^\times$ forms a group under $\times$.

e.g.) Ring: $(\mathbb{Z}/12\mathbb{Z}, +, \times)$ (take non-zero elements for $\times$).
multiplicative identity $= 1$
units $= R^\times = \{1, 5, 7, 11\}$, form a group under $\times$.

- Why do the units always form a group under $\times$?
  ↳ Let R be any ring, show the units $R^\times$ are a group:
  i) $1 \in R^\times$ ∵ $1 \times 1 = 1$ (inverse exists) identity ✓
  ii) associative - inherited ✓
  iii) inverses: x is a unit $\Rightarrow x$ has an inverse.
  iv) closed under $\times$ ✓ if $x \in R^\times$, $y \in R^\times$
  ~~$y^{-1} x^{-1} \in R^\times$~~ $xy \in R^\times$ ∵ $(xy)^{-1} = y^{-1} x^{-1}$ exists
  ~~$(xy)^{-1} \in R^\times$~~

= Integral Domains

- normally if $x \cdot y = 0$ we say one of them must be 0.
  - ↳ this is not always true in abstract algebra

- consider $x^2 + 5x + 6 \equiv 0 \pmod{12}$
  $(x+2)(x+3) \equiv 0 \pmod{12}$
  $\Rightarrow x \equiv 10 \bmod 12$, $x \equiv 9 \bmod 12$ } only soln. BUT, $x \equiv 1 \bmod 12$, $x \equiv 6 \bmod 12$ are also soln!

- what went wrong?
  $(x+2)(x+3) \equiv 0 \bmod 12$.
  - $x \equiv 1 \Rightarrow 3 \cdot 4 \equiv 0 \bmod 12$.
  - $x \equiv 6 \Rightarrow 8 \cdot 9 \equiv 0 \bmod 12$
  } we can multiply two non-zero numbers together and get 0.

- we say the integers mod 12 have "Zero Divisors"
  - ↳ it is these zero divisors which makes solving these equations more difficult.
  - ↳ $\mathbb{R}$s and $\mathbb{C}$s do not have zero divisors, ∴ we don't have this problem.

- $b|a$ if $b \cdot c = a$ for some c.
  $3 \cdot 4 \equiv 0 \bmod 12 \Rightarrow$ $3|0 \bmod 12$, $4|0 \bmod 12$ } "Zero Divisors"

* Integers mod 11 have no zero divisors.
  11 is prime $\Rightarrow 11 | a \cdot b$ only if $11|a$ or $11|b$.
  11 does not divide $\{0, 1, 2, \ldots, 10\}$.
  ∴ factoring and setting to zero works fine here.

* An Integral Domain is a
  1) commutative ring R ——why?——>
  2) multiplicative identity 1
  3) no zero divisors.

- $3x \equiv 6y \bmod 12$
  cannot cancel always in Rings.
  ↳ can only factor and cancel if the ring R has no zero divisors.
  let $a \cdot x = a \cdot y \quad (a \neq 0)$
  $a \cdot x - a \cdot y = 0$
  $a \cdot (x-y) = 0.$
  No zero divisors $\xrightarrow{\because a \neq 0}$ $x-y=0 \Rightarrow x=y.$
  $\therefore ax = ay$ ∴ Integral domains have the cancellation property.

Ideals in Rings

- ideals: rings :: normal subgroups: groups.
  ↳ most properties carry over.
- Suppose R is a ring; $I \subseteq R$ is a subset
  Goal: Cosets of I to form a ring.
  What properties must I have for this?

• $(R,+)$ is abelian, we want $(I,+) \trianglelefteq (R,+)$ to be abelian

but $\because (R,+)$ is abelian, every subgroup is normal.

Required Properties
- $(I,+) \leq (R,+)$
- $y \in R, i \in I \Rightarrow iy \in I$
- $x \in R, i \in I \Rightarrow xi \in I$.

• $\because I$ is a subgroup, we can cover R in its cosets. Choose two random cosets; $x+I$, $y+I$.

$\because I$ is a normal subgroup of R,

$$(x+I)+(y+I) = (x+y)+I.$$

but R is a ring. We want to be able to multiply two cosets.

$$(x+I)\cdot(y+I) \stackrel{?}{=} xy+I$$
$$(x+i_1)\cdot(y+i_2) \stackrel{?}{=} xy+i_3$$
$$i_1y + xi_2 + i_1i_2 \stackrel{?}{=} i_3$$

→ Requirement: $i_1y + xi_2 + i_1i_2 \in I$ (no matter which two elements we pick from the cosets (LHS $\in I$ always).

→ Trick #1: Pick elements from cosets

$x+i_1 \in x+I$

$y \in y+I \quad \because y = y+0.$

Question: When is $(x+i_1)\cdot y \in xy+I$?

$$xy + i_1y = xy + i_2$$
$$i_1y = i_2$$

for any $y \in R$, for any $i_1 \in I$, $i_1y \in I$.

→ Trick #2: $x \in x+I$

$y+i_1 \in y+I$.

Question: When is $x\cdot(y+i_1) \in xy+I$

$$xy + x\cdot i_1 \in xy + i_2$$
$$x\cdot i_1 = i_2 \Rightarrow x\cdot i_1 \in I.$$

→ for any $x \in R$, for any $i_1 \in I$, $x\cdot i_1 \in I$.

$\therefore$ cosets R/I form a ring "Quotient Ring"

I is an Ideal