EQUIVAL-
-ENCE
RELATIONS

Equivalence Relations – Gps – Perm gps – Rings

Equivalence Rels:

Any elt from col A + Any elt from col B = Some elt from col C

0	1	2	3	4	5
6	7	8	9	10	11
12	~~13~~	14	15	16	17
18	~~19~~	20	21	22	23
24	~~25~~	26	27	28	29

$N=6$

Define col by the smallest elt i.e. if col A contains 3 then write $[3]=$ col A

Note $[3]=\{3,9,15,21,27,\ldots\}=[9]=[15]$

eg $[63]+[19]=[82]$

$[63]=[3+10\cdot 6]=[3]$ $\quad [1]+[3]=[4]$

$[19]=[1+3\cdot 6]=[1]$ $\quad [82]=[4+13\cdot 6]=[4]$

Claim: $[a]+[b]=[a+b]$

Proof: $a=x_a+y_aN \quad 0\le x_a\le N-1$

$b=x_b+y_bN \quad 0\le x_b\le N-1$

$a+b=x_a+x_b+(y_a+y_b)N \in [x_a+x_b]$

$[a+b]=[x_a+x_b]$ ∎ Note $[a]+[0]=[a]$

We write $a\sim a+yN$

$\sim$ is called an equivalence Relation

Def $\sim$ is an equiv Rel. on a set A if

$a\sim a$ $\forall a\in A$ (Reflexive) $\quad a\sim b$ iff $b\sim a$ (Symmetry)

$a\sim b$ & $b\sim c \Rightarrow a\sim c$ (transitive)

$[a] = \{b \in A \mid a \sim b\}$ = Equivalence class

Examples

Most obviously $=$ is an equivalence Rel. ($\frac{1}{2} = \frac{4}{8}$)

Equiv Rel. is an extension of equality

$a \in \mathbb{R}$, $[a] = \{\frac{\lambda a}{\lambda} \mid \lambda \in \mathbb{R} \setminus \{0\}\}$

Modulo arithmetic: $a \equiv b \mod N$ if

$a = b + yN$, $y \in \mathbb{Z}$ $(a, b \in \mathbb{N})$

eg $17 \equiv 5 \mod 12$

Important thm: Fermat's little thm:

p prime, $x \in \mathbb{Z}$, then $x^p \equiv x \mod p$

ie $x^p - x$ is a multiple of p

eg $\frac{217^{61} - 217}{61} \in \mathbb{Z}$

Now:

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24

$5 \times 14 = 70$

$8 \times 11 = 88$

$[a] \cdot [b] = [a \cdot b]$

Note $[a] \cdot [1] = [a]$

70

88

So we could add or multiply integers and $\mathbb{N}$.

Binary Op.

We have seen examples of special operations now of the form input $*$ input $=$ output 2 inputs: these are called binary operations

More specifically: a binary operation is a correspondence between ordered pairs of elts of a set & elts of a set

Note that ordering is important here.

While addition of integers is a bin. op

eg $(3,5) = 3+5 = 8 = 5+3 = (5,3)$

So is subtraction

$$(3,5) = 3-5 = -2 \neq 2 = 5-3 = (5,3)$$

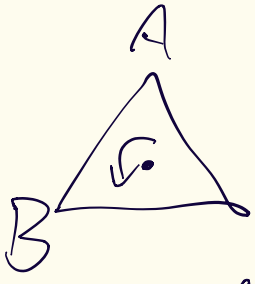
However: addition is a b.o. on $\mathbb{N}$, & subtraction is not!

i.e. b.o. : $A \times A \to A$ language of fcns.

TRANS-FORMATIONS

These are examples of structure. Lets do some geometry now.

Transformations



r_1: Rotate 120° CCW (counter-clockwise)

r_2: Rotate 240° CCW

Both fix the Δ.

$r_1 : {}_B\Delta_C \to {}_A\Delta_B$

$r_2 : {}_B\Delta_C \to {}_C\Delta_A$

$e : {}_B\Delta_C \to {}_B\Delta_C$

We can compose r_1 & r_2

$r_1 \cdot r_2$ means first do r_2 then r_1

We can write a table of compositions

	e	r_1	r_2
e	$e\cdot e$	$e\cdot r_1$	$e\cdot r_2$
r_1	$r_1\cdot e$	$r_1\cdot r_1$	$r_1\cdot r_2$
r_2	$r_2\cdot e$	$r_2\cdot r_1$	$r_2\cdot r_2$

=

	e	r_1	r_2
e	e	r_1	r_2
r_1	r_1	r_2	e
r_2	r_2	e	r_1

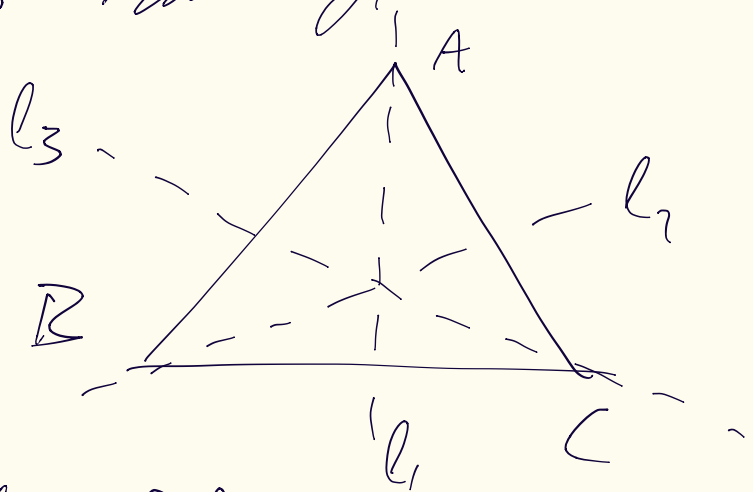
i.e. $r_2 \cdot r_2 : {}_B\Delta_C = r_1 : {}_C\Delta_A = {}_A\Delta_B = r_1 : {}_B\Delta_C$

Note $r_1 \cdot r_2 = r_2 \cdot r_1 = e$ identity

i.e. r_1 is the 'reverse' of r_2 & inverse
r_2 is the 'reverse' of r_1

Operations on a structure (could be a shape, but could be more abstract) that preserves the look are called plane symmetric operations.

$\triangle$ has more symmetries

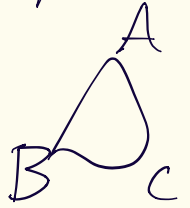


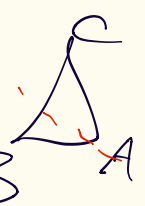
3 lines of symmetry

label by f_1, f_2, f_3 the flips along l_1, l_2, l_3

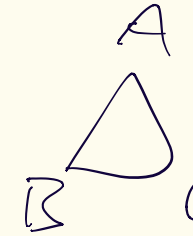
i.e. $f_2 : {}_B\triangle^A_C \to {}_B\triangle^C_A$ (flip because r was already used for rotation)

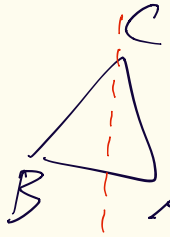
Two options for composing flips:

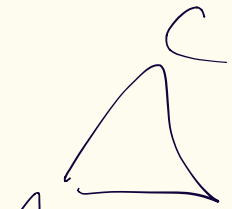
$f_1 f_2 :$ 

$\to f_1 :$ 

$= {}_C\triangle^B_A$ **Op 1**

$f_1 f_2 :$ 

$\to f_1$ 

$=$ 

Op 2

each is admissable. Convention is fixing lines of symmetry, not transposing them

So we go w/ Op 2

Now we compose transformations!

	e	r_1	r_2	f_1	f_2	f_3
e	e	r_1	r_2	f_1	f_2	f_3
r_1	r_1	r_2	e	f_3	f_1	f_2
r_2	r_2	e	r_1			
f_1	f_1					
f_2	f_2					
f_3	f_3	f_1	f_2	r_1	r_2	e

Cayley table

eg

$r_1 f_1 : \Delta^{A}_{BC} = r_1 : \Delta^{A}_{CB} = \Delta^{B}_{AC}$

$r_1 f_2 = r_1 \Delta^{C}_{BA} = \Delta^{A}_{CB}$

$r_1 f_3 = r_1 \Delta^{B}_{AC} = \Delta^{C}_{BA}$

HW: Fill in Table

HW: Complete table for square □

↳ for Rhombus ◇

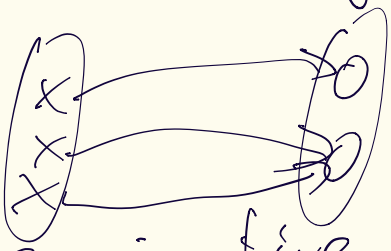
↳ for Rectangle ▭

	e	r_1	r_2	f_1	f_2	f_3
e	e	r_1	r_2	f_1	f_2	f_3
r_1	r_1	r_2	e	f_3	f_1	f_2
r_2	r_2	e	r_1	f_2	f_3	f_1
f_1	f_1	f_2	f_3	e	r_1	r_2
f_2	f_2	f_3	f_1	r_2	e	r_1
f_3	f_3	f_1	f_2	r_1	r_2	e

GROUPS

Groups

Recall bijections:



Surjective
Not injective

injective
Not surjective

Both!
Bijection

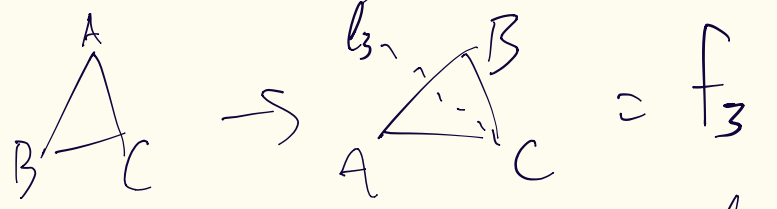
Defn
A mapping from a set to itself $T: A \to A$ that is bijective is called a transformation of the set.

On finite sets these are called permutations

In analysis we are concerned w/ what functions do to individual elts.
In abstract algebra we will study the structure of the transformations themselves.

For a finite set we can write a perm as

$\begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix}$ ← first row is a list of elts
second row is where elts are sent



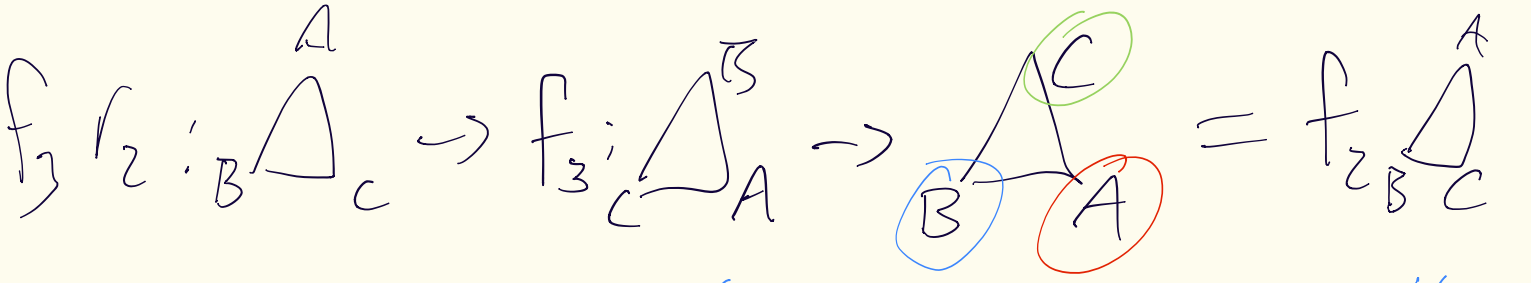
$= f_3$

(i.e. A means A ends up
B in the position that B was in.)

We can compose permutations in this notation

eg $f_3 \cdot r_2 = \begin{pmatrix} A & B & C \\ B & A & C \end{pmatrix} \cdot \begin{pmatrix} A & B & C \\ C & A & B \end{pmatrix} = \begin{pmatrix} A & B & C \\ C & B & A \end{pmatrix}$

2 2 2 1 1 1



HW: 10 computations on compositions of permutations

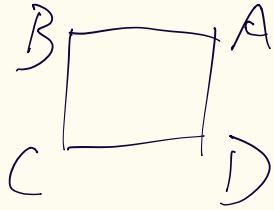
One can see these are bijections as every letter appears & appears precisely once in the second line.

As a bijection ∃ an inverse

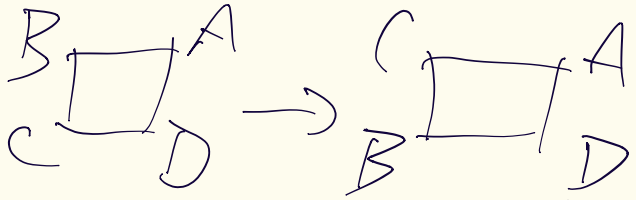
HW: Show
It is easy to see that swapping rows creates an inverse

The collection of plane symmetric transformations of a polygon, w/ composition, is called a group

Note that the set of permutations on a set w/ 3 elts $\{A, B, C\}$ is in correspondence w/ the set of the symmetric transformations of the equilateral Δ. But (in HW) You can see that this is not the case in general.

eg. 

The set of permutations on $\{A, B, C, D\}$ includes $\begin{pmatrix} A & B & C & D \\ A & C & B & D \end{pmatrix}$

which is 

Not the result of a plane symmetry!

So the notion of permutation is more general than plane symmetry

We give a general def^n of a group:

In general:

Def: A group is a set G on which we can define a binary operation $*$ (typically called multiplication) s.t. the following conditions hold.

1) $\exists e \in G$ s.t. $e*g = g*e = g$ $\forall g \in G$ (identity)

2) $\forall g \in G \; \exists g' \in G$ s.t. $g \cdot g' = g' \cdot g = e$ (inverse)

3) $\forall g_1, g_2, g_3 \in G$, $(g_1 * g_2) * g_3 = g_1 * (g_2 * g_3)$ (associativity)

HW Show dihedral/symm/cyclic gps satisfy 1), 2), & 3)

Q. is $(\{1, 3, 5, 7, 9, 11, \ldots\}, +)$ a gp?

Why not? (Closure, which comes from $*$ needing to be a binary operation!)

A group w/ finitely many elts is called finite. Else infinite

Def: The size of the gp (how many elts it has) is called the order of the gp.

Examples: $(\mathbb{Z}, +)$.

Plane symmetry gps of polygons (Dihedral gps)

Permutations of sets (Symmetric gps)

Rotations of polygons - Cyclic gps

Addition mod n: eg $\{0,1,2,3,4,5\}$

For any elt. eg 4 $\exists$ inverse (2) s.t. $4+2=0$

(Recall these are equiv. classes)

Commutativity

As we can see from the Cayley table of symmetries of an equilateral Δ

$f_1 \cdot f_1 = f_2$ These are not equal!

$r_1 \cdot f_1 = f_3$

Def^n. A binary operation $\cdot : S \times S \to S$ is called commutative if $a \cdot b = b \cdot a$ $\forall a, b \in S$.

A group is called abelian if its gp operation is commutative

Abelian gps are much simpler to work with. Non abelian gps are more complicated, but also more interesting.

An important example of non-abelian gps are groups of matrices.

By the end of the course we will be characterising non-abelian gps by how closely they resemble abelian groups

CYCLES

Aside on cycles

A permutation $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 2 & 5 \end{pmatrix}$ May be written in shorter notation

Consider σ applied iteratively to a single elt.

eg $\sigma(1) = 4$,

$\sigma^2(1) = \sigma(4) = 2$

$\sigma^3(1) = \sigma(2) = 3$

$\sigma^4(1) = \sigma(3) = 1$

1, 2, 3, 4 accounted for

$\sigma(5) = 5$

So $\sigma = (1\,4\,2\,3)(5)$

This is called a cycle decomposition

cycles of length 1 are often omitted: $\sigma = (1\,4\,2\,3)$

We read left to right.

Cycle decompositions are not unique:

eg $(1\,4)(2\,4)(3\,4) = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$

Thm: We can always write a permutation as a product of length 2 cycles

Proof: Note $(a_1 \dots a_n) = (a_1 a_n)(a_2 a_n) \dots (a_{n-1} a_n)$

Then decompose all cycles in a perm. into transpositions $\square$

Transpositions detail important properties about permutations:

Defn. Let a perm $\sigma = \tau_1 \dots \tau_n$. The parity of σ

denoted $\operatorname{sgn}(\sigma) = \begin{cases} +1, & n \text{ even} \\ -1, & n \text{ odd} \end{cases}$ → we say σ is <u>even</u>
→ we say σ is <u>odd</u>

Lemma: Parity is multiplicative

Proof: if σ_1 & σ_2 are both written with even # of transpositions then $\sigma_1\sigma_2$ & $\sigma_2\sigma_1$ both are clearly written w/ even #
if both odd then $\sigma_1\sigma_2$ & $\sigma_2\sigma_1$ are even
if one even & one odd then $\sigma_1\sigma_2$ & $\sigma_2\sigma_1$ odd
(just counting # of transpositions) □

Theorem: The parity is independent of the decomposition

i.e. parity is a property of permutations, not their specific decomps.

Lemma: Let τ_i denote transp. & let $\sigma = \tau_1 \tau_2 \cdots \tau_n$

(inverses of transp) Then $\sigma^{-1} = \tau_n \tau_{n-1} \cdots \tau_2 \tau_1$

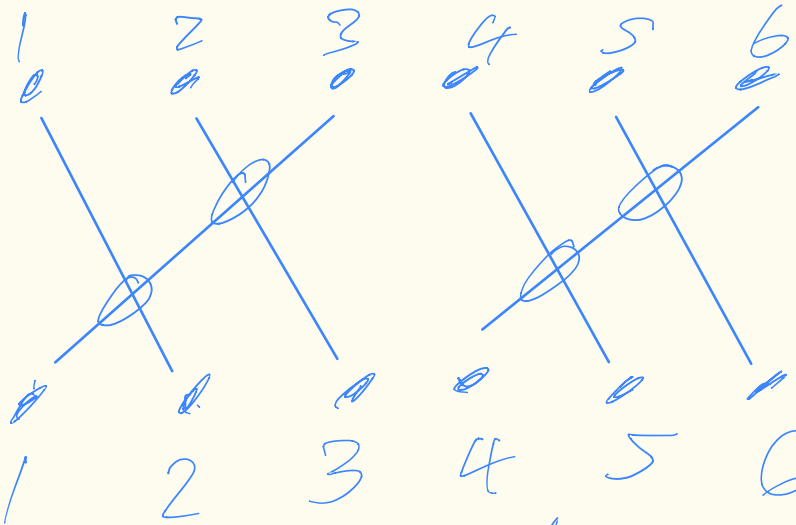
Proof: Consider (ab). Then $(ab)(ab) = \begin{pmatrix} a & b \\ a & b \end{pmatrix} = e$

So $\tau_1 \cdots \tau_n \tau_n \cdots \tau_1 = \tau_1 \cdots \tau_{n-1} e \tau_{n-1} \cdots \tau_1 = \cdots = e$ □

Note: transpositions are <u>involutions</u>: self inverse

Proof of thm: Say $\sigma = \tau_1 \cdots \tau_n = \rho_1 \cdots \rho_m$

ie. n even $\Leftrightarrow m$ even



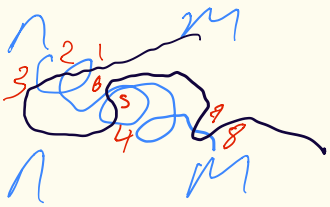
$(123)(456)$

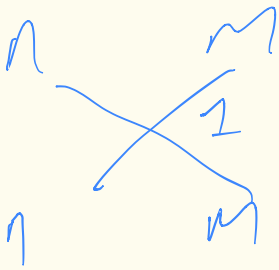
$= (13)(23)(46)(56)$

Ex: A_n = gp of rotations of n-simplex

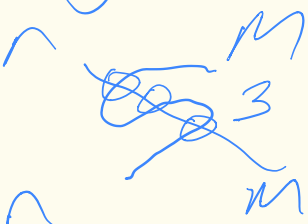
S_n = gp of symm. transformations of n-simplex.

crossing # = 0
topologically crossing # must be even



If 

crossing # odd



etc.

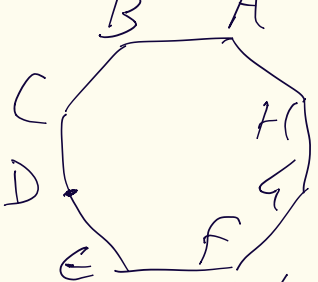
So intersection number is well defined mod 2.

Not complete?
Well, complete but not rigorous
Example w/ Broad
& p. See more in AA II

Cyclic Gps

Let's get to grps w/ the simplest type of gp: Cyclic gp.

Consider a regular n-gon eg octagon



Consider only the rot. symmetric transf. Note that every rot. R_α is a multiple of $360°/8 = 45°$. Rotating by $135°$: $R_{135} = R_{45} \circ R_{45} \circ R_{45}$

There are 8 possible rotations, sending A to one of the 8 vertices ($R_{45}: A \mapsto B$)

They are $\{R_0, R_{45}, R_{90}, R_{135}, R_{180}, R_{225}, R_{270}, R_{315}\}$

$= \{R_{45}^0, R_{45}^1, R_{45}^2, R_{45}^3, R_{45}^4, R_{45}^5, R_{45}^6, R_{45}^7\}$

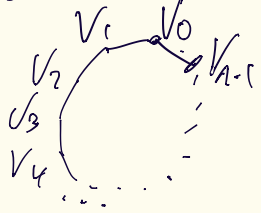
We call R_{45} the generator of this group.

Def^n A cyclic group C_n is one whose elts may be written in terms of a single elt. α, $C_n = \{\alpha^0, \alpha^1, \dots, \alpha^{n-1}\}$, where $\alpha^n = \alpha^0 = e$

$C_n = \langle \alpha \rangle$ α is called a generator

Theorem: The rotational symmetries of a reg. n-gon form C_n.

Proof: The smallest rotation is $\alpha = 360°/n$

label: 

$\alpha^0 : v_0 \mapsto v_0$

$\alpha^1 : v_0 \mapsto v_1$

$\alpha^k : v_0 \mapsto v_k$

$\alpha^n : v_0 \mapsto v_0$

Hence every rot. is a power of α. □

Def: The order of an elt a is the smallest number n s.t. $a^n = e$

Note: the order may not exist.

eg in $(\mathbb{Z}, +)$: $1^n = n \quad \forall n \in \mathbb{N}$ (i.e. $\neq 0$)

HW What are the orders of elts in C_8?

Prove or disprove: let $\alpha \in C_n$. Then $\text{ord}(\alpha) = n$ iff α is a generator

Note that in C_8, $\text{ord}(\alpha^7) = 8$ & $C_8 = \langle \alpha^7 \rangle = \langle \alpha \rangle$

Note also that in perm. language,

$$\alpha = \begin{pmatrix} v_0 & v_1 & v_2 & v_3 & v_4 & v_5 & v_6 & v_7 \\ v_1 & v_2 & v_3 & v_4 & v_5 & v_6 & v_7 & v_8 \end{pmatrix}$$

$$\alpha^{-1} = \begin{pmatrix} v_0 & v_1 & v_2 & v_3 & v_4 & v_5 & v_6 & v_7 \\ v_7 & v_0 & v_1 & v_2 & v_3 & v_4 & v_5 & v_6 \end{pmatrix}$$

HW: show every elt of C_n is of the form

$$\begin{pmatrix} v_0 & v_1 & \dots & v_{n-1} \\ v_{i_1} & v_{i_2} & \dots & v_{i_{n-1}} \end{pmatrix}$$ where $i_1, i_2, \dots, i_{n-1}$ is in cyclic order

Questions 32-36 in Alekseev

Cyclic groups can be infinite

Defn Let $C_\infty = \langle a \rangle$ where $\text{ord}(a) = \infty$

i.e. $C_\infty = \{\ldots a^{-1}, a^0, a, a^2, \ldots\}$ & $\text{ord}(C_\infty) = \infty$

C_∞ is called an inf. cyclic gp.

The notation is not accidental.

We will see shortly there is only one C_∞.

The key points of cyclic gps will be clear once we have another tool in our arsenal: homomorphisms.

Let us introduce them w/ a single ex.

Cayley table

	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

Let $G = \{e, a, b\}$ 3 elts w/ '$\cdot$' s.t. i.e. $a^2 = b$ & $b^2 = a$

The op. '$\cdot$' puts a structure on G. Note $a^2 = b$ means $G = \{e, a, a^2\} = C_3$

Note also $\mathbb{Z}_3 = (\{0, 1, 2\}, +)$ has $1 + 1 = 2$, $2 + 2 = 4 \equiv 1 \bmod 3$. This has same algebraic structure! Let's formalise this notion.