Group Vacation!

Recall: if S is a set with a binary operation $*$ and $e \in S$ is a $*$-identity. e is unique

Defn The set G w/ bin operation $*$ is a group p.t.

1. $*$ is associative
2. $\exists$ an identity wrt $*$ called $e \in G$
3. $\forall g \in G \ \exists g^{-1} \in G$ s.t. $g * g^{-1} = e = g^{-1} * g$

Remark inverses are unique in grps as $*$ is associative!

Eg:
- $(\mathbb{R}, +)$
- $(\mathbb{R} \setminus \{0\}, \times)$
- for an arbitrary field F $(F, +)$ is a grp & $(F \setminus \{0\}, \times)$ is a grp
- $\mathbb{Z}/n$ → mod n
  $= \{\bar{0}, \bar{1}, \bar{2} \dots \overline{n-1}\}$
  ↳ consists of equivalence classes
- $(\mathbb{Z}/n, +(\text{mod } n))$

Non Eg:
- $(\mathbb{R}, \times)$ → no inv of 0
- $(\mathbb{N}, +)$ → no inverses
- $(\mathbb{Z}/4 \setminus \{\bar{0}\}, +\text{ mod } 4)$
  ↳ $\bar{2}$ has no inverse

Defn let $(G, *)$ & $(G', *')$ be groups.
$\varphi: G \to G'$ is a grp homomorphism p.t.
$\forall a, b \in G$ we have
$\varphi(a * b) = \varphi(a) *' \varphi(b)$, note $\varphi(a), \varphi(b) \in G'$

Defn A grp homomorphism is a grp isomorphism p.t. it is bijective!

Lemma let $(G,*)$, $(G',*')$ be grps. Supp $\varphi: G \to G'$ is an isomorphism. Then

$\varphi^{-1}: G \to G'$ is an isomorphism.

Pf We note $\varphi^{-1}: G' \to G$ is a bijection. We need to show it is a grp homomorphism.

let $c,d \in G'$ we know $\exists!\, a \in G$ s.t $\varphi(a) = c$ and $\exists!\, b \in G$ s.t $\varphi(b) = d$ so,

$$\varphi^{-1}(c *' d) = \varphi^{-1}(\varphi(a) *' \varphi(b)) = \varphi^{-1}(\varphi(a*b))$$

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

as φ is a homomorphism

Consider $\ln: (0,\infty) \to \mathbb{R}$, $x \mapsto \int_1^x \frac{1}{t}$ we know,

1. $\ln(1) = 0$
2. $\ln$ is cts
3. $\ln$ is strictly increasing
4. $\ln$ is surjective

} it is bijective

By FTC1 $\ln'(x) = \frac{1}{x}$

Lemma $\ln: (0,\infty) \to \mathbb{R}$ is a grp homomorphism between $((0,\infty), \times)$, $(\mathbb{R}, +)$

This means $\forall a,b \in (0,\infty)$ $\ln(ab) = \ln(a) + \ln(b)$

Pf Fix $b \in (0,\infty)$ constant, consider 2 fnc

$(0,\infty) \to \mathbb{R}$, $a \mapsto \ln(ab)$ and $(0,\infty) \to \mathbb{R}$, $a \to \ln(a)$ — both are diffble

$$\frac{\partial}{\partial x}[\ln(a\cdot b)] = \frac{1}{a\cdot b} b = \frac{1}{a}$$

$$\frac{\partial}{\partial x}[\ln(a)] = \frac{1}{a}$$

equal derivatives! By FTC1 $\exists$ const c s.t

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

Let $a = 1$, $\ln(b) = \ln(1) + c \Rightarrow c = \ln(b)$ ∴

So, $\ln(a\cdot b) = \ln(a) + \ln(b)$ → grp iso!

Corollary $((0,\infty), \times)$ is isomorphic to $(\mathbb{R}, +)$

Pf $\ln: (0,\infty) \to \mathbb{R}$ is a bijective homomorphism □

What can we say abt $\exp: \mathbb{R} \to (0,\infty)$?

By previous lemma, it is a grp isomorphism
$\Rightarrow$ homomorphism thus.

$\forall a, b \in \mathbb{R}$ $\exp(s+t) = \exp(s) \cdot \exp(t)$

Inverse Function Thm Pt 2

if f is a function that is invertible & if f is diffble at a, then is f^{-1} diffble at $f(a)$?

If so, what is $(f^{-1})'(f(a))$?

guess $f^{-1}(f(x)) = x \Rightarrow \frac{\partial}{\partial x}(f^{-1}(f(x)) = \frac{\partial}{\partial x}(x)$

$\Rightarrow (f^{-1})'(f(x)) \cdot f'(x) = 1$

$\Rightarrow (f^{-1})'(f(x)) = \frac{1}{f'(x)}$

Let $w = f(x)$ & $x = f^{-1}(w)$

$(f^{-1})'(w) = \frac{1}{f'(f^{-1}(w))}$ $\Rightarrow$ all is bogus if $f'(x) = 0$

Thm Let $A \subseteq \mathbb{R}$ be an iwimp. Let $f: A \to \mathbb{R}$ be cts & injective. Sppse f is diffble at $f^{-1}(b)$ with $f'(f^{-1}(b)) \neq 0$

Then f^{-1} is diffble at b &

$$(f^{-1})'(b) = \frac{1}{f'(f^{-1}(b))}$$

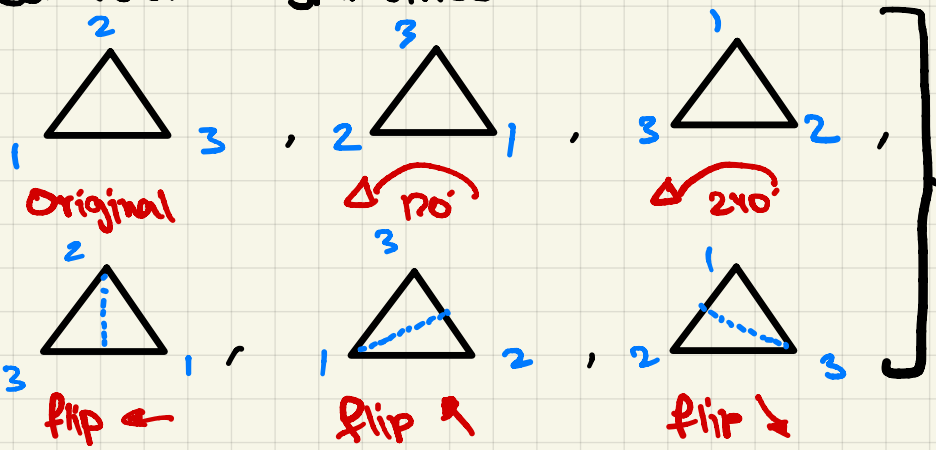
Pf Conrad and spivak (pg 237)

Cor $\ln'(x) = \frac{1}{x} \neq 0$ $\forall t \in (0,\infty)$ exp is diffble at $\ln(t)$

$\exp'(\ln(t)) = \frac{1}{t} = t = \exp(\ln(t)) \Rightarrow \exp'(s) = \exp(s)$

Back to Grps

Consider Symmetries



→ Any transformation of A can be de-composed as a composition of these moves

Let S be the set of these moves (transformations), think of S as a grp wrt composition

1. Composition is associative
2. 'Do nothing' move is identity!
3. Everything has inv → flips are self inversing!

This grp is D_3 → Dihedral grp

↳ In general given a regular polygon of n sides, $n \geq 3$, we can define a dihedral group to be the grp of symmetries with composition!

$D_n \to 2n$ elements

Defn The grp $(G, *)$ is abelian pt $*$ is commutative!

Lets prove D_3 isn't abelian (that is composition isn't comm)

→ we need to find $a, b \in D_3$ s.t $a * b \neq b * a$

→ consider a = rotate 120 b = flip ↖

→ Clearly $a * b \neq b * a$ → ∴ D_3 is not abelian!

for fact: D_n is not abelian, $\forall n \geq 3$

Permutation Groups

Let $n \in \mathbb{N}$ consider the set $X_n = \{1, \ldots, n\} = \mathbb{N}_n$

Let $S_n = \{f : X_n \to X_n \mid f \text{ is bijective}\}$ → Fun fact: not abelian

Note: a bijection from a set to itself is often called a permutation. ∴ S_n is the set of all permutations of X_n.

Q: How many elts does S_n have?

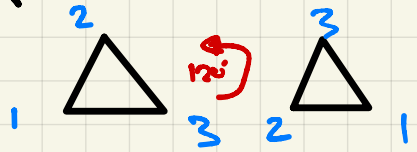
Ans: $n!$ → Prove by 'induction'.

We need a bin op! → use composition

① $e = Id_{X_n}$ ② Always Associative ③ bijections are invertible

Tagline: S_n is the "symmetric grp on n letters".

Q: Is S_3 isomorphic to D_3 → Yes!

Pf: exercise! Consider 

as $(1,2,3) \to (2,3,1)$

Defn: A subgroup is a subset of grp which inherits the binary operation
↳ Axioms must hold + closure

Eg: $G = (\mathbb{Z}, +)$ $H = 2\mathbb{Z} \subseteq \mathbb{Z}$ → evens
↳ ✓
↳ H = odds ✗ → no identity

D_3 → id + only rotate ✓
→ id + only flip ✗
→ id + one flip ✓
↳ self 'inverting'

Q: Is S_n isomorphic to D_n

Ans: No. $\forall n \geq 4$ $|S_n| = n! \neq 2n = |D_n|$

Since the cardinality of the underlying sets is diff → no bij

Hard prb

Given 2 groups $(G,*)$ & $(G',*')$, how do we know if they're isomorphic? (apart from different cardinality)

Consider $\mathbb{Z}/4\mathbb{Z} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$ as a grp wrt addition mod 4

$*$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

→ we see that this is abelian due to the symmetry along the diagonal

Here is another group with 4 elts

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

→ this is associative

→ this is also abelian.

→ every element is its own inv

Idea, is the "everything is its own 'inv'" property preserved by iso?

$\mathbb{Z}/4$ doesn't have this property but the other does!

---

easier example S_3 vs $\mathbb{Z}/6\mathbb{Z}$

S_3: non abelian

$\mathbb{Z}/6\mathbb{Z}$: abelian

→ not isomorphic → isomorphism will preserve abelian.

Pf let $(G,*)$, $(G',*')$ be groups with only G being abelian, let $\varphi: G' \to G$ be an iso

$\exists\, a,b \in G'$ s.t. $a *' b \neq b *' a$

Since φ is an iso, $\exists\, c,d \in G$ s.t. $\varphi(a) = c$, $\varphi(b) = d$

we have $a *' b = \varphi^{-1}(\varphi(a *' b)) = \varphi^{-1}(c * d)$

$b *' a = \varphi^{-1}(d * c) \neq \varphi^{-1}(c * d)$

oops....

Lemma Suppose G is a grp w/ identity e. Suppose $x \in G$.

We have $x * x = x \iff x = e$

Pf $\Leftarrow$ is immediate

$\Rightarrow$

$$e = e * e = e * (x * x^{-1}) = e * ((x * x) * x^{-1})$$
$$= e * (x * (x * x^{-1})) = e * (x * e) = x$$

Lemma Let G, H be grps.
Suppose $\varphi : G \to H$ is a homomorphism. Let e_G be id in G & e_H be id H. Then

1. $\varphi(e_G) = e_H$
2. $\forall x \in G \quad \varphi(x^{-1}) = (\varphi(x))^{-1}$
3. $\forall x \in G \quad \forall n \in \mathbb{N}$
$\varphi(x^n) = (\varphi(x))^n$

$x^n = \underbrace{x * \dots * x}_{n}$

Pf 1 $\varphi(e_g) = \varphi(e_g *_G e_g) = \varphi(e_g) *_H \varphi(e_g)$

$\Rightarrow \varphi(e_g) *_H \varphi(e_g) = \varphi(e_g)$

$\Rightarrow$ by lemma $\varphi(e_g) = e_H$

Pf 2 $(\varphi(x))^{-1} = (\varphi(x))^{-1} *_H e_H = (\varphi(x))^{-1} *_H \varphi(e_g)$

$\Rightarrow (\varphi(x))^{-1} *_H (\varphi(x) *_G x^{-1})$

$\Rightarrow (\varphi(x))^{-1} *_H (\varphi(x) *_H \varphi(x^{-1}))$

$\Rightarrow ((\varphi(x))^{-1} *_H \varphi(x)) *_H \varphi(x^{-1})$

$\Rightarrow e_H *_H \varphi(x^{-1}) = \varphi(x^{-1})$

Pf 3 Hw 11 Proof by Induction!

Corollary There is no isomorphism between $\mathbb{Z}/4\mathbb{Z}$ & $G = \{a, b, c, e\}$ defined previously.

Pf Since we have an isomorphism, $\varphi : G \to \mathbb{Z}/4$

then $\forall x \in G$ we have,

$$\overline{0} = \varphi(e) = \varphi(x \cdot x) \text{ as every elt is self-inv}$$

$$= \varphi(x) * \varphi(x)$$

But then $\varphi(x)$ must be in $\mathbb{Z}/4\mathbb{Z}$ and have the property that $\varphi(x) * \varphi(x) = \overline{0}$

$\therefore \varphi(x) = \overline{0}$ or $\overline{2}$

$\therefore$ φ isn't surjective .... oops