Proof

Let $z \in S$

$$\begin{aligned}(\rho_x \circ \rho_y)(z) &= \rho_x(\rho_y(z)) && \text{Defn of Composition of mappings}\\ &= \rho_x(z * y) && \text{Defn of Right reg. rep.}\\ &= \cancel{x}(z*y)*x && \text{Defn of Right reg. rep.}\\ &= z*(y*x) && \text{Semigroup Axiom : Associativity}\\ &= \rho_{y*x}(z) && \text{Defn of Right reg. rep.}\end{aligned}$$

3) Composition of Left Regular representation with Right.

Theorem

Let $(S,*)$ be a semigroup

Let λ_x and ρ_y be the left and right reg. rep of $(S,*)$ w.r.t x and y respectively.

Let $\lambda_x \circ \rho_y$ and ~~x~~ $\rho_y \circ \lambda_x$ etc.. be defined as the composition of mappings λ_x and ρ_y.

Then $\forall x,y \in S$

$\lambda_x \circ \rho_y = \rho_y \circ \lambda_x \longleftarrow$

Proof Let $z \in S$

$$\begin{aligned}(\lambda_x \circ \rho_y)(z) &= \lambda_x(\rho_y(z)) && \text{Defn Comp. of mappings}\\ &= \lambda_x(z*y) && \text{Defn right reg. rep}\\ &= x*(z*y) && \text{Defn left reg. rep}\\ &= (x*z)*y && \text{Semigroup Axiom : Associativity}\\ &= \rho_y(x*z) && \text{Defn r.r.r}\\ &= \rho_y(\lambda_x(z)) && \text{Defn L.r.r}\\ &= (\rho_y \circ \lambda_x)(z) && \text{Defn Comp. of mappings.}\end{aligned}$$

Additional Definitions & Theorems

Homomorphism

Defn

Let $(G,\circ)$ and $(H,*)$ be groups

Let $\phi\, G \to H$ be a mapping such that $\circ$ has the morphism property under ϕ.

That is

Then $\forall a,b \in G$

$\phi(a \circ b) = \phi(a) * \phi(b)$

Then $\phi : (G,\circ) \to (H,*)$ is a group homomorphism.

Let $\phi : (S,\circ) \to (T,*)$ be a mapping from one algebraic structure $(S,\circ)$ to another $(T,*)$.

~~Then ϕ~~ Then $\circ$ has the morphism property under ϕ iff $\forall x,y \in S$

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

Kernel of Group Homomorphism

Defn

Let $(G,\circ)$ and $(H,*)$ be groups.

Let $\phi : (G,\circ) \to (H,*)$ be a group Homomorphism.

The Kernel of ϕ is the subset of the domain of ϕ defined as :

$\ker(\phi) = \{x \in G \mid \phi(x) = e_H\}$

Where e_H is the identity of H.

That is $\ker(\phi)$ is the subset of G that maps to the identity of H.

S to itself.

Identity Mapping

The identity mapping of a set S is the mapping $I_S : S \to S$ defined as:

$I_S = \{(x,y) \in S \times S \mid x = y\}$

Identity mapping is injection.
$\forall\ I_S(x) = I_S(y) \Rightarrow x = y$ (injection)

or Alternatively

$I_S = \{(x,x) \mid x \in S\}$

Identity mapping is Surjection.
$\forall y \in S : I_S(y) = y$ Defn of id mapping
We have $\forall y \in S : \exists x \in S : x = y$ (y is itself)
$\to \forall y \in S : \exists x \in S : I_S(x) = y$ Defn I_S
$\Rightarrow$ Surjection

That is

$I_S : S \to S : \forall x \in S : I_S(x) = x$

$\Rightarrow I_S$ is a bijection.

Informally, it is a mapping for which every element is a fixed element.

↳ The identity mapping of a group is a mapping from the group to itself whereby every element is mapped to itself.

Kernel is trivial iff group Monomorphism.

Theorem

Let $\phi : (S, \circ) \to (T, *)$ be a group homomorphism.

Let $Ker(\phi)$ be the kernel of ϕ.

Then ϕ is a group monomorphism if and only if $ker(\phi)$ is trivial.

Contains only identity e_S.

Let $(G, \circ)$ and $(H, *)$ be groups

Let $\phi : G \to H$ be a group homomorphism

Then ϕ is a group monomorphism if and only if ϕ is an injection.

Proof

Necessary Condition

Let $\phi : (S, \circ) \to (T, *)$ be a group monomorphism

By Homomorphism to Group preserves identity $\to$ ie. $\phi(e_S) = e_T$

$e_S \in Ker(\phi)$

If $Ker(\phi)$ contained another element $s \neq e_S$ then $\phi(s) = \phi(e_S) = e_T$ and ϕ would not be injective, thus not a group monomorphism.

So $Ker(\phi)$ can contain only one element, and that must be e_S, which is therefore the trivial subgroup of S.

□

Sufficient Condition

Now Suppose $Ker(\phi) = \{e_S\}$

Then for $x, y \in S$:

??

$\phi(x) = \phi(y)$	
$\phi(x) * (\phi(y))^{-1} = \phi(y) * (\phi(y))^{-1}$	Group Axioms
$\phi(x \circ y^{-1}) = e_T$	Defn of Morphism property
$x \circ y^{-1} \in Ker(\phi)$	Defn of Kernel of Group Homomorphism
$x \circ y^{-1} = e_S$	by hypothesis
$x = e_S \circ y = y$	Group Axiom

Thus ϕ is injective and therefore a group monomorphism.

■

Monomorphism Image is Isomorphic to Domain.

Theorem

"The image of a monomorphism is isomorphic to its domain."

That is : If $\phi : S_1 \rightarrow S_2$ is a monomorphism, then :

$\cancel{\phi(S_1)}$

$\phi : S_1 \rightarrow Img(\phi)$ is an isomorphism.

Proof

Requirements : 1) Def$\underline{n}$ of domain & Image ✓

2) How to prove injection & Surjection (bijection) ✓ ??

3) Restriction of injection is injection

4) Def$\underline{n}$ Of Restriction & Inclusion ✓

5) Restriction of Mapping is Mapping

6) Restriction of Mapping to image is Surjection.

6) Binary Relations. ✓

7) Morphism property preserves closure.

Defn of function.

Group Theory Cont.

- A function is a binary relation which is $\underbrace{\text{left-total}}_{\forall x}$ and $\underbrace{\text{right unique}}_{\exists y}$.

Definition of

① Mapping

Defn 1

A mapping from S to T is a binary relation on $S \times T$ which associates each element of S with only one element of T.

Defn 2

A mapping f from S to T denoted $f: S \to T$ is a relation $f = (S, T, G)$ where $G \subseteq S \times T$ such that

$\forall x \in S : \forall y_1, y_2 \in T : (x, y_1) \in G \wedge (x, y_2) \in G \Rightarrow y_1 = y_2$

in words: If f sends $x \in S$ to both y_1 and y_2 then $y_1 = y_2$

(and $\forall x \in S : \exists y \in T : (x, y) \in G$)

denotes right unique

Defn 3

A mapping f from S to T denoted $f: S \to T$ is a relation $f = (S, T, R)$ where $R \subseteq S \times T$ such that:

$\forall (x_1, y_1)(x_2; y_2) \in f : y_1 \neq y_2 \Rightarrow x_1 \neq x_2$

and $\forall x \in S : \exists y \in T : (x, y) \in f$.

↳ NOTE: Suppose $x \in S$ and $y \in T$

$f: S \to T : f(x) = y$ → interpreted to mean $(x, y) \in f$

~~NOTE:~~

(As can be seen, binary relations are represented by mappings.)

Defn 4

A mapping from S to T is a relation on $S \times T$ which is

1) Many-to-One
2) Left-total.

(Departure Set) (Arrival set)

Dom(f) Cdm(f)

Domain Codomain

$f: S \to T$ $(f \in S \times T$ & $f^{-1} \in T \times S)$

Preimage - $Img^{-1}(f)$

$= \{s \in S \mid \exists t \in T \text{ s.t } f(s) = t\}$

$f^{-1}[T]$ is the image of T under f^{-1}

Defn of Domain & Image.

Image

Let S and T be sets

Let $f: S \to T$ be a mapping

Let $X \subseteq S$ be a subset of S.

Then the image of X (under f) is defined and denoted as:

$f[X] \overset{def}{=} \{t \in T \mid \exists s \in X : f(s) = t\}$ {Set of values taken by f is $f[S]$ and is denoted $Img(f)$. (entie domain.)

Image of Subset as Element of Direct Image Mapping.

The image of X under f can be seen to be an element of the codomain of the direct image mapping $f^{\to} : \mathcal{P}(S) \to \mathcal{P}(T)$ of f:

$\forall X \in \mathcal{P}(S) : f^{\to}(X) := \{t \in T : \exists s \in X : f(s) = t\}$

Thus

$\forall X \subseteq S : f[X] = f^{\to}(X)$

Direct Image Mapping [Mapping induced (on the power set) by f.]

Let S and T be sets

Let $\mathcal{P}(S)$ and $\mathcal{P}(T)$ be their Power sets.

Let $f \subseteq S \times T$ be a mapping from S to T.

↳ Binary Relation.

The direct image mapping of f is the mapping $f^{\to} : \mathcal{P}(S) \to \mathcal{P}(T)$ that sends a subset $X \subseteq S$ to its image under f:

$$\forall X \in \mathcal{P}(S) : f^{\to}(X) = \begin{cases} \{t \in T : \exists s \in X : f(s) = t\} & : X \neq \emptyset \\ \emptyset & : X = \emptyset \end{cases}$$

The direct image mapping of f can be seen to be the set of images of all the subsets of the domain of f :

$\forall X \subseteq S : f[X] = f^{\rightarrow}(X)$

Note f and $f^{\rightarrow}$, $f^{\leftarrow}$ are not the same.

$f^{\rightarrow}$ and $f^{\leftarrow}$ are mappings induced on the power sets by the mapping f.

Examples

1) Arbitrary mapping from $\{0,1,2,3,4,5\}$ to $\{0,1,2,3\}$

Let $f : S \to S$ be the mapping defined as :

$f(0) = 0$

$f(1) = 0$

$f(2) = 0$

$f(3) = 1$

$f(4) = \cancel{2}\,1$

$f(5) = 3$

~~Then Image of f under~~

① ~~A~~

Let

$A = \{0,3\}$ $B = \{0,1,3\}$ $C = \{0,1,2\}$

Then $f[A] = \{0, 1\}$

Set of Domain

Generated Image Set

$f[B] = \{0,0\ 1\} = \{0,1\}$

All the values of the domain is sent to all of these.

$f[C] = \{0\}$ and $Img(f) = \{0,1,3\}$

ie. $Img(f)$ where f on entire domain | $f[X]$ image of subset X of domain.

2) Image of $[-3\,..\,2]$ under $x \mapsto x^4 - 1$

Let $f : \mathbb{R} \to \mathbb{R}$ be the mapping defined as :

$\forall x \in \mathbb{R} : f(x) = x^4 - 1$

$f[(-3\,..\,2)] = [-1\,..\,80]$

Image of closed interval $[-3\,..\,2]$

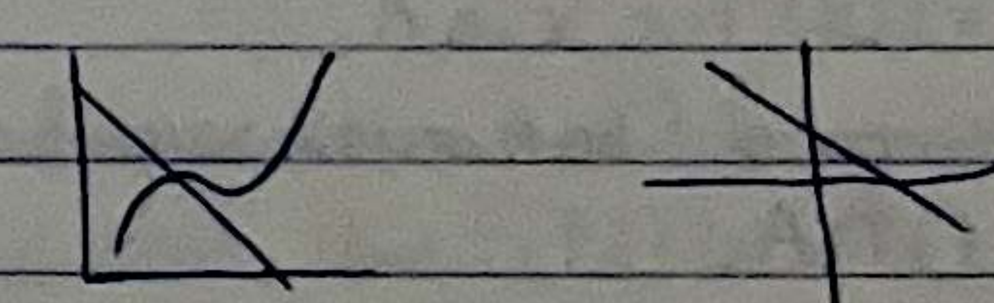
$(-3)^4 - 1 = 80$

$\frac{d}{dx}(x^4 - 1) = 4x^3$

minimum image occurs at $4x^3 = 0$

$\Rightarrow f(0) = -1 \leftarrow$ minimum image.

(f is strictly increasing on $x > 0$ and strictly decreasing on $x < 0$)



$f(-3) = 80$ $f(2) = 15$ but $f_{min} = -1$

$\Rightarrow [-1, 80]$

min

max for given [-3 ... 2]

amongst

~~Domain~~

Restrictions & Inclusions

Restrictions

- The restriction of a function f is a new function denoted $f \restriction A$ obtained by choosing a smaller domain A for the original function f.

Formally.

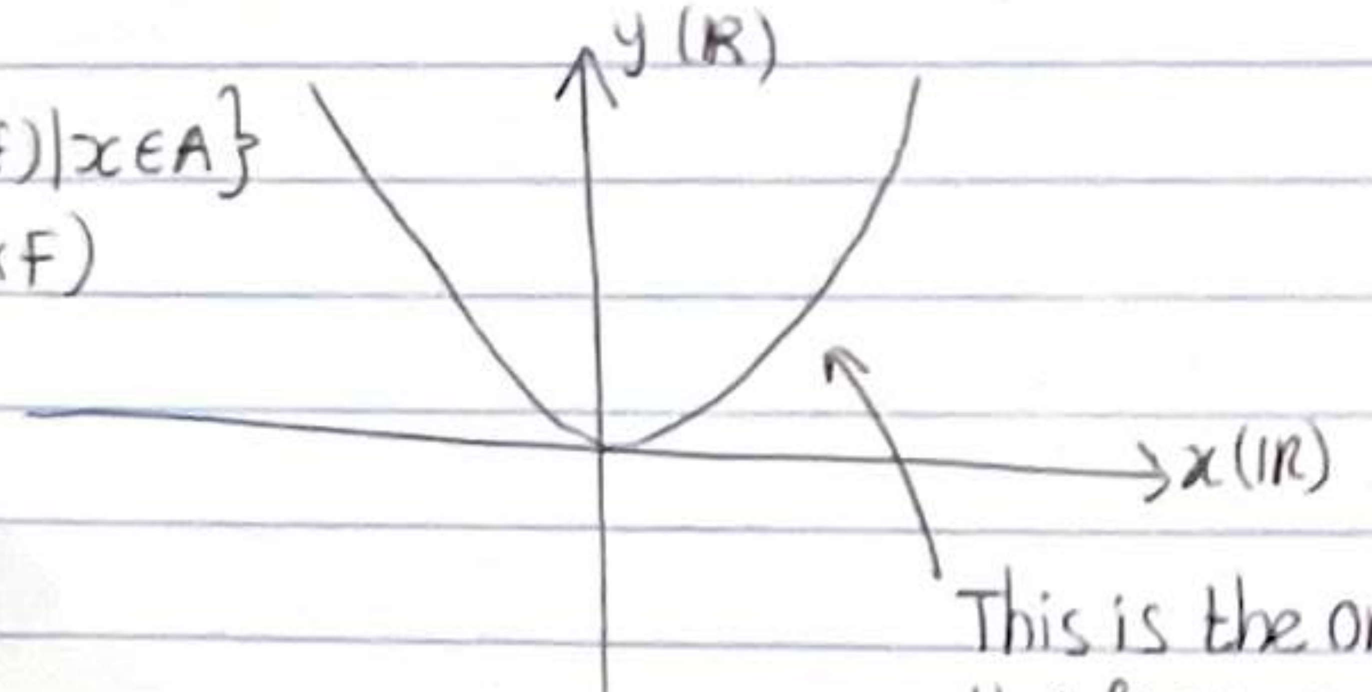
- Let $f : E \to F$ be a function from a set E to a set F. If a set A is a subset of E, then the restriction of f to A is the function
  $f\restriction_A : A \to F$
  given by $f\restriction_A(x) = f(x)$ for x in A.
- Informally, the restriction of f to A is the same function as f but is only defined on $Dom(f) \cap A$.

- If the function f is thought as a relation $(x, f(x))$ on the cartesian product $E \times F$, then the restriction of f to A can be represented by its graph* (graph of a function)

eg. $y = x^2 \to f(x) = x^2 \Rightarrow (x, x^2) = (x, f(x))$ on $\mathbb{R} \times \mathbb{R}$

*$G(f\restriction_A) = \{(x, f(x)) \in G(f) \mid x \in A\}$
$= G(f) \cap (A \times F)$

where $(x, f(x))$ represent ordered pairs in the graph G.



This is the only part of $\mathbb{R} \times \mathbb{R}$ that $f(x)$ is allowed to take ie. its graph.

Examples

1) The restriction of the non-injective function $f : \mathbb{R} \to \mathbb{R}, x \mapsto x^2$ to the domain $\mathbb{R}_+ = [0, \infty)$ is the injection $f : \mathbb{R}_+ \to \mathbb{R}, x \mapsto x^2$
(used during exams to find inverse for $x \geq 0$ (domain))

2) The factorial function is the restriction of the gamma function to the +ve integers, with the argument shifted by one: $\Gamma\restriction_{\mathbb{Z}^+}(n) = (n-1)!$

Properties of restrictions

- Restricting the function $f : X \to Y$ to its entire domain X gives back the original function f ie. $f\restriction_X = f$.

- Restricting a function twice ~~(same restriction parameter)~~ is the same as restricting it once ie. if $A \subseteq B \subseteq \text{dom} f$ then $(f\restriction_B)\restriction_A = f\restriction_A$

- The restriction of a continuous function is continuous

- The restriction of the identity function on a set X to a subset A of X is just the inclusion map from A into X.

Bin.-rel.

Left/Domain Restriction (More general)

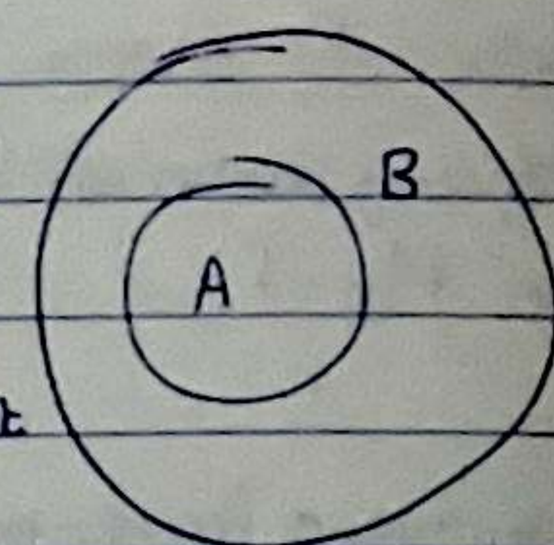
$A \lhd R$ of a binary relation R between E and F may be defined as a relation having domain A and codomain F and graph
$G(A \lhd R) = \{(x,y) \in G(R) \mid x \in A\}$
Similarly right/range restriction can be defined ($R \rhd B$)

Anti-Restriction

- The domain anti-restriction (or domain subtraction) of a function f or a binary relation R (with domain E and codomain F) by a set A may be defined as $(E/A) \lhd R$; it removes all elements of A from E.
  It is sometimes denoted $A ⩤ A ⩤ R$
- Similarly the range anti-restriction (or range subtraction) of a function or binary relation R ~~on~~ by a set B is defined $R \rhd (F/B)$. It removes all elements of B from the codomain F. It is sometimes denoted $R ⩥ B$.

Inclusion Map

- If A is a subset of B then the inclusion map (canonical injection) is the function f that sends each element x of A to x treated as an element of B. (It sorts of "properly" include A in B)



$f : A \to B \quad f(x) = x$

also $f : A \hookrightarrow B$

A is a subset of B and B is a superset of A.

Theorem: Restriction of Injection is Injection.

Let $f : S \to T$ be an injection

Let $X \subseteq S$ be a subset of S.

Let $f[X]$ denote the image of X under f.

Let $Y \subseteq T$ be a subset of T such that $f[X] \subseteq Y$

* → The restriction $f\restriction_{X \times Y}$ of f to $X \times Y$ is an injection

Theorem: Restriction of mapping is mapping.

Let $f : S \to T$ be a mapping

Let $X \subseteq S$

Let $f\restriction_X$ be the restriction of f to X.

Then

$f\restriction_X : X \to T$ is a mapping

whose domain is X

whose preimage is X

Proof

As $f : S \to T$ is a mapping we have that :

$\forall x \in S : (x, y_1) \in f \land (x, y_2) \in f \Rightarrow y_1 = y_2$ Defn of mapping as binary relation.

From the definition of subset we have that :

$x \in X \Rightarrow x \in S$ and so

$\forall x \in X : (x, y_1) \in f\restriction_X \land (x, y_2) \in f\restriction_X \Rightarrow y_1 = y_2$ Mapping induced by restriction of f on X.

Also from the definition of mapping

$\forall x \in S : \exists y \in T : (x, y) \in f$

Again from the definition of a subset, $x \in X \Rightarrow x \in S$, and so

$\forall x \in X : \exists y \in T : (x, y) \in f\restriction_X$ Defn of mapping recovered for $f\restriction_X$.

So $f\restriction_X : X \to T$ is a mapping

Theorem: The preimage of a mapping is the same set as its domain ie. $\mathrm{Img}^{-1}(f) = \mathrm{Dom}(f)$

Proof

Let $f \subseteq S \times T$ be a mapping

Then : $\forall x \in S : \exists y \in T : (x, y) \in f$ Defn of mapping

$\Rightarrow \forall x \in S : x \in \mathrm{Img}^{-1}(f)$ Preimage of mapping

$\Rightarrow S \subseteq \mathrm{Img}^{-1}(f)$ Subset.

Set equality

$S = T \iff (\forall x \in S \iff x \in T)$

$S = T$ iff $S \subseteq T$ and $T \subseteq S$

$f: S \to T$ injection
$X \subseteq S$
$Y \subseteq T$

* Proof of Restriction of Injection is Injection

First we show that $f \restriction_{X \times Y}$ is a mapping from X to Y.

By restriction of mapping is mapping, $f \restriction_{X \times T}$ is a mapping from X to T.

We need to show $f \restriction_X : X \to T$ where $X \subseteq S$ is same as $f \restriction_{X \times T}$.

Defn of mapping $\forall x \in S : \exists y \in T : (x, y) \in f$ for $f: S \to T$

We know that a mapping is a binary relation.

A binary relation over set S and T is a subset of $S \times T$.

Note: $f \restriction_X = \{(x, f(x)) \mid x \in X\}$ where $X \subseteq S$

Another Definition of Restriction

Let $f: S \to T$ be a mapping

Let $X \subseteq S$

Let $f[X] \subseteq Y \subseteq T$

The restriction of f to $X \times Y$ is the mapping $f \restriction_{X \times Y}$ $X \to Y$ defined as
$f \restriction_{X \times Y} = f \cap (X \times Y)$

↳ Remember: f is a mapping, a binary relation over S and T $(S \times T)$
therefore like bin rel. $f \subseteq S \times T$

For the mapping $X \to Y$ where $X \subseteq S$ and $Y \subseteq T$, the values of f are also restricted ie. only $X \times Y$ in $S \times T$

$\Rightarrow f \restriction_{X \times Y} = f \cap (X \times Y)$ ie $(S \times T) \cap (X \times Y)$

Since $(X \times Y) \subseteq (S \times T)$

$f \restriction_{X \times Y} \subseteq X \times Y$

If $Y = T$ (eg. in case of subset of domain to whole codomain)

$\Rightarrow$ The restriction is called simply restriction of f to X denoted $f \restriction_X$.

Also $f \restriction_X = \{(x, y) \in f \mid x \in X\}$

or $f \restriction_X = \{(x, f(x)) \mid x \in X\}$

*

~~First the~~ $f: S \to T$ is an injection

$X \subseteq S$ and $Y \subseteq T$ and $f[X] \subseteq Y$ ← Img of X under f. → Subset of codomain.

$\Rightarrow f \restriction_{X \times Y}$ is an injection from X to Y.

↑ restriction of f to $X \times Y$ $f \restriction_{X \times Y} : X \to Y$.

Proof

First we show that $f \restriction_{X \times Y}$ is a mapping from X to Y.

By restriction of mapping is mapping, $f \restriction_{X \times T}$ (or simply $f \restriction_X$) is a mapping from X to T.

If $x \in X$, then by definition of image $f(x) \in f[X]$

Since $f[X] \subseteq Y$, $f \restriction_{X \times Y}$ is a mapping from X to Y.

By definition of an injection

$\forall s_1, s_2 \in S : f(s_1) = f(s_2) \Rightarrow s_1 = s_2$

Aiming for contradiction, suppose $f \restriction_{X \times Y} : X \to Y$ were not an injection.

Then:

$\exists x_1, x_2 \in X$ s.t. $x_1 \neq x_2$, AND $f(x_1) \overset{?}{=} f(x_2)$ $\neq$?? Let there be x_1, x_2 where $x_1 \neq x_2$

$X \subseteq S$

But then

$\exists x_1, x_2 \in S : x_1 \neq x_2$, AND $f(x_1) \overset{?}{=} f(x_2)$ $\neq$??

Which implies $f: S \to T$ is not an injection. ↯

$\Rightarrow f \restriction_{X \times Y} : X \to Y$ is an injection.

~~Right restriction of codomain to image.~~

Right restriction of codomain to image.

Restriction of Mapping to Image is Surjection.

1) Surjection (right total)

Let S and T be sets or classes.

Let $f : S \to T$ be a mapping from S to T.

↳ same as function ??

$f : S \to T$ is a Surjection if and only if

$f[S] = T$

in direct image mapping notation $f^{\to}(S) = T$

ie. f is a surjection iff its image equals its codomain

ie. $Img(f) = Cdm(f)$ → Right Total (No one is left unpaired)

Note surjection is sometimes denoted as follows $f : S \twoheadrightarrow T$.

2) Surjective Restriction

Let $f : S \to T$ be a mapping which is not surjective.

Then a surjective restriction of f is a restriction $g : S' \to T'$ of f such that

$g\restriction_{S'} : S' \to T'$ is a surjection.

$(\times T')$??

3) Theorem

Let $f : S \to T$ be a mapping

Let $g : S \to Img(f)$ be the restriction of f to $S \times Img(f)$

Then g is a surjective restriction of f.

Proof

From Image is subset of Codomain

$Img(f) \subseteq \cancel{Cdm(f)} T$

By defn of image we have

$\forall s \in S : g(s) \in Img(g)$

Therefore g may be viewed as a mapping

$g : S \to Img(g)$

Thus by defn, g is a surjection.

Thus for any mapping $f : S \to T$ which is not surjective, by restricting its codomain to its image can be made surjective.

Bijection

For mappings

1) A mapping $f : S \to T$ is a bijection iff both 1) f is an injection 2) f is a surjection.

2) f has both a left inverse and a right inverse (composite functions)

3) The inverse f^{-1} of f is a mapping $T \to S$

4) A mapping $f \subseteq S \times T$ is a bijection iff for each $y \in T$ there exists one and only one $x \in S$ such that $(x, y) \in f$.

5) A relation $f \subseteq S \times T$ is a bijection iff.

1) for each $x \in S$ there exists one and only one $y \in T$ such that $(x,y) \in f$

2) for each $y \in T$ there exists one and only one $x \in S$ such that $(x,y) \in f$.

Symbol for bijection $f: S \leftrightarrow T$

injection : $S \rightarrowtail T$ or $S \hookrightarrow T$

surjection : $S \twoheadrightarrow T$

Note : We still need to show Morphism property preserves closure and give the definition for Algebraic Structure.

Algebraic Structure

An algebraic Structure is an ordered tuple $(S, \circ_1, \circ_2, \cdots, \circ_n)$ Where S is a set which has one or more binary operation $\circ_1, \circ_2, \cdots \circ_n$ defined on all the elements of $S \times S$.

Since operation is binary

ie. ~~$S \circ S$ or S~~

$s \circ_1 s$ or $s \circ_2 s$ where $s \in S$

An algebraic structure with one binary operation is thus an ordered pair denoted $(S, \circ)$, $(T, *)$, and so on.

Theorem : Morphism property preserves closure.

Let $\phi : (S, \circ_1, \circ_2, \cdots, \circ_n) \longrightarrow (T, *_1, *_2, \cdots, *_n)$ from one algebraic structure to another.

Let $\circ_k$ have the morphism property under ϕ for some operation $\circ_k$ in $(S, \circ_1, \circ_2, \cdots \circ_n)$

Then the following properties hold

If $S' \subseteq S$ is closed under $\circ_k$ then $\phi[S']$ is closed under $*_k$.

If $T' \subseteq T$ is closed under $*_k$ then $\phi^{-1}[T']$ is closed under $\circ_k$.

Where $\phi[S']$ is the image of S'.

Proof

Suppose that $\circ_k$ has the morphism property under ϕ

Suppose $S' \subseteq S$ is closed under $\circ_k$.

Thus : $s_1, s_2 \in S' \Rightarrow s_1 \circ_k s_2 \in S'$

Similarly suppose $T' \subseteq T$ is closed under $*_k$

Thus : $t_1, t_2 \in T' \Rightarrow t_1 *_k t_2 \in T'$

First we prove that $\phi[S']$ is closed under $*_k$:

$t_1, t_2 \in \phi[S']$

$\Rightarrow \exists s_1 \in S' : t_1 = \phi(s_1) \land \exists s_2 \in S' : t_2 = \phi(s_2)$ Defn image of subset

$\Rightarrow t_1 *_k t_2 = \phi(s_1) *_k \phi(s_2) = \phi(s_1 \circ_k s_2)$ Defn of morphism property

$\Rightarrow t_1 *_k t_2 \in \phi[S']$ S' is closed under $\circ$.

Homomorphism - Morphism for magmas.

??

Then we prove that $\phi^{-1}(T')$ is closed under $\circ_K$:

$S_1, S_2 \in \phi^{-1}[T'] \Rightarrow \phi(S_1), \phi(S_2) \in \phi^{-1}[T']$ Defn of inverse mapping

$\phi(S_1) *_K (S_2) \in T'$

$\Rightarrow \phi(S_1 \circ_K S_2) \in T'$ Defn of morphism property

$\Rightarrow S_1 \circ_K S_2 \in \phi^{-1}[T']$ Defn of inverse mapping.

We now have Everything required for our theorem.

Monomorphism Image is isomorphic to Domain.

The image of a monomorphism is isomorphic to its domain.
That is if $\phi : S_1 \to S_2$ is a monomorphism, then:
$\phi : S_1 \to Img(\phi)$ is an isomorphism.

Proof

Let $(S_1, \circ_1)$ and $(S_2, \circ_2)$ be closed algebraic Structure.
Let ϕ be a monomorphism from $(S_1, \circ_1)$ to $(S_2, \circ_2)$
Let $T = Img(\phi)$ be the image of ϕ
By morphism property preserves closure $(T, \circ_2)$ is closed
As ϕ is a monomorphism it is by definition an injective homomorphism
From Restriction of injection is injection, $\phi : S_1 \to Img(\phi)$ is an injection.
From Restriction of mapping to image is Surjection, $\phi : S_1 \to Img(\phi)$ is a Surjection.
Thus $\phi \to Img(\phi)$ is by definition a bijection
Thus $\phi : S_1 \to Img(\phi)$ is a bijective homomorphism
Hence by definition, $\phi : S_1 \to Img(\phi)$ is an isomorphism.

Cayley's Representation Theorem.

Let S_n denote the Symmetric group on n letters
Every finite group is isomorphic to a Subgroup of S_n for some $n \in \mathbb{Z}$

General Case

Let $(G, \cdot)$ be a group
Then there exists a permutation group P on some set S Such that $G \cong P$.

Proof

Let G be any arbitrary finite group whose identity is e_G.
Let S be the Symmetric group on the elements of G, where e_S is the identity of S.
For any $x \in G$, let λ_x be the left regular representation of G w.r.t x
From Regular representations in Groups are permutations, $\forall x \in G : \lambda_x \in S$

So we can define a mapping $\theta : G \to S$ as : $\forall x \in G : \theta(x) = \lambda_x$
From Composition of regular representations, we have:
$\forall x, y \in G : \lambda_x \circ \lambda_y = \lambda_{xy}$ Where in this context $\circ$ denotes composition of mappings.

Thus by definition of θ : $\theta(x) \circ \theta(y) = \theta(xy)$ demonstrating that θ is a homomorphism.

Having established that fact, we can now consider $Ker(\theta)$ (kernel of θ)

Let $x \in G$

We have that

$x \in Ker(\theta)$

$\Rightarrow \theta(x) = e_S$ Defn of Kernel of group homomorphism

$\Rightarrow \lambda_x = I_G$ Where I_G is the identity mapping of G.

$\Rightarrow \lambda_x(e_G) = I_G(e_G)$ Defn of identity mapping

$\Rightarrow x = e_G$ Defn of λ_x and I_G

So $Ker(\theta)$ can contain no element other than e_G.

So since clearly $e_G \in Ker(\theta)$ it follows that

~~Ker(θ) =~~

$Ker(\theta) = \{e_G\}$

By kernel is trivial iff Monomorphism, it follows that θ is a monomorphism.

By Monomorphism image is isomorphic to domain, we have that :

$\theta[G] \cong Img(\theta)$

that is θ is isomorphic to its image.

Hence the result.

θ sends Group to Symmetric group

G codomain

permutation group (domain)

$\theta[G] \cong Img(\theta)$

group

Permutation group (Image)

Subset of Symmetric group

$$\boxed{\theta[G] \cong Img(\theta)}$$

Cosets of a group

- A Subgroup H of Group G may be used to decompose the underlying set of G into disjoint equal size pieces called Cosets.

- There are 2 types of cosets namely left Coset and right coset. Cosets of either type have the same number of elements (Cardinality) as does H.

- (due to identity)
  Futhermore, H is itself a coset which is both a left coset and a right coset. The number of left cosets of H in G is equal to the number of right cosets of H in G.

Definition

Let $H \leq G$

Given an element ~~g∈G~~ $g \in G$

The left cosets of H in G are the sets obtained by multiplying each element of H by a fixed element ~~of~~ g of G (where g is a left factor.

ie. $gH = \{gh : h \text{ is an element of } H\}$ for each g in G

The right cosets are defined similarly (except g is a right factor)

$Hg = \{hg : h \text{ is an element of } H\}$ for each g in G.

As g varies through the group, it would appear that many (left & right) cosets are generated.
However, not all these cosets are distinct. Infact, we will see that if ~~an~~ one element is common in 2 or more cosets, then these cosets are the same.

Example 1) Consider $S(\Delta)$

We know that $(\{e,r,s\},\circ) < S(\Delta)$ (Subgroup) — We call this H.

So we will use the latter to generate cosets.

H (Subgroup)

$\circ$	e	r	s	a	b	c
① e	e	r	s	a	b	c
② r	r	s	e	b	c	a
③ s	s	e	r	c	a	b
④ a	a	c	b	e	s	r
⑤ b	b	a	c	r	e	s
⑥ c	c	b	a	s	r	e

Elements of G ($S(\Delta)$) g

* But for the same subgroup H, the all the cosets have the same size (even left & right ones) all left ones & all right ones (Trivial)

$e\circ H$
$r\circ H$
$s\circ H$
⋮

① $eH = \{e,r,s\}$
② $rH = \{r,s,e\}$
③ $sH = \{s,e,r\}$
④ $aH = \{a,c,b\}$
⑤ $bH = \{b,a,c\}$
⑥ $cH = \{c,b,a\}$

- These are the left cosets generated by the Subgroup H.
- We can see that for example r is present in eH, rH and sH. These cosets as can be seen are equal (order does not matter in sets)
- ~~Some~~ An additional cosets ~~are~~ is also obtained namely $\{a,b,c\}$ by a, b and C multiplication.

$S\circ H = \{s\circ e, s\circ r, s\circ s\}$

Important. * (We also see that all cosets have same cardinality (size) (no. of elements)
→ NOT True: Subgroups of different sizes might exist
→ We also know no. left cosets of H = no. right cosets of H.

If we calculate the right cosets we shall see that they are different from the left ones

Like in ← In an Abelian Group left coset (of eg. g) ie $gH = Hg$ (right coset by g)

residue class of Z mod n — * If for a Subgroup of G which has $gH = Hg$ for all elements in H, then the Subgroup is known as a normal subgroup.

Why do we not look at each integer / element of G but a "collection" ie Subgroup, collection under mod n..

We can see that the cosets $\{e,r,s\}$ and $\{a,b,c\}$ generated are infact disjoint.

* Like in quotient sets in equivalence relations the cosets of a normal subgroup form a group known as quotient group.

Coset, Index.

If G is not abelian, then the partition induced on G by the left cosets will be different from the ~~fo~~ ones induced by the right cosets.

If $G \trianglelefteq H$ (Where H is a normal Subgroup) the partition will be the same and thus the "set of all cosets" can be properly defined and considered for the group G. This group is known as the quotient group (and is similar to quotient sets obtained with equivalance classes).

Example 2) Consider the Dihedral Group of Order 6 (D_3) with $a^3 = b^2 = I$ and $ba = a^{-1}b = a^2b$

$*$	I	a	a^2	b	ab	a^2b
I	I	a	a^2	b	ab	a^2b
a	a	a^2	I	ab	a^2b	b
a^2	a^2	I	a	a^2b	b	ab
b	b	a^2b	ab	I	a^2	a
ab	ab	$\cancel{a}b$	a^2b	a	$\cancel{a}I$	a^2
a^2b	a^2b	ab	b	a^2	a	I

Let T be the Subgroup $\{I,b\}$

The left cosets of T are:

$IT = T = \{I,b\}$
$aT = \{a, ab\}$
$a^2T = \{a^2, a^2b\}$

We stop here as all the elements of D_3 has appeared (once) in the cosets we calculated and any ~~thos~~ more generating cosets would be ones with same elements and hence equal ones

The right cosets of T are:

$TI = \{I,b\}$ $(=T)$
$Ta = \{a, ba\} = \{a, a^2b\}$
$Ta^2 = \{a^2, ba^2\} = \{a^2, ab\}$

As we can see consider a, $aT \neq Ta$ ie left coset of T w.r.t a $\neq$ right coset of T w.r.t a.

In an abelian group all the left cosets w.r.t an element must equal all the right cosets w.r.t the same element

{ Cosets L & R coincide. ↖ Although $IT = TI$ (possible) for other cases too.

Only unequal one makes this fail to be Abelian. If $\exists a : aT \neq Ta \Rightarrow$ Group not abelian

Centre of a Group

For some elements other than the identity, left & rights cosets may coincide even if the group is not abelian. This element is known as the centre of a group.

- The centre of a group G, denoted $Z(G)$ is the set of elements that commute with all the elements of the group.

$Z(G) = \{ z \in G \mid \forall g \in G, zg = gz \}$

- The centre is a normal subgroup $Z(G)$

ie. $Z(G) \trianglelefteq G$ → A group G is abelian iff $Z(G) = G$

The elements of the centre are sometimes called central.

A group G is centreless if $Z(G)$ is trivial ie. $Z(G) = \{e_G\}$

~~For the elements in a centre eg. 6 (a central)~~

Review

Note: A group may be non-Abelian and possess a centre.

For the centre, the cosets (L & R) will coincide.

Also a central will multiply both left & Right with a subgroup to yield the same coset.

Index of a Subgroup

The index of a subgroup H in a group G is the "relative size" of H in G: equivalently the number of "copies" (cosets) of H that fill up G.

eg. If H has index 2 in G, half the elements of G lie in H. The index of H in G is usually denoted $[G:H]$ or $|G:H|$

Formally, the index of H in G is defined as the number of cosets of H in G. (It is always the case that the number of left cosets of H in G is equal to the number of right cosets.)

Example: Let $\mathbb{Z}$ be the group of integers under addition. Let $2\mathbb{Z}$ be the subgroup of even integers. Then $2\mathbb{Z}$ has 2 cosets in $\mathbb{Z}$, namely the even integers and odd integers. So $[\mathbb{Z} : 2\mathbb{Z}] = 2$

Generally $[\mathbb{Z} : n\mathbb{Z}] = n$

If N is a normal subgroup in G, then the index of N in G is also equal to the order of the quotient group G/N since the latter is defined in terms of a group structure on the sets of cosets of N in G.

Properties

- If H is a subgroup of G and K is a subgroup of H, then $|G:K| = |G:H||H:K|$

- If H and K are subgroups of G then $|G : H \cap K| \leq |G:H||G:K|$, with equality if $HK = G$ (If $|G : H \cap K|$ is finite, then equality holds iff $HK = G$)

Equivalently

- If $H \leq G \wedge K \leq G$ then $|H : H \cap K| \leq |G:K|$ with equality if $HK = G$ (If $|H : H \cap K|$ is finite, then equality holds iff $HK = G$).

- If G and H are groups and $\varphi : G \to H$ is a homomorphism, then the index of the kernel of φ in G is equal to the order of the image.

$[G : \ker(\varphi)] = |\operatorname{img}(\varphi)|$

* In general

Let $a_1, a_2, a_3, \ldots, a_n$ with inverse $a_1^{-1}, a_2^{-1}, a_3^{-1}, \ldots a_n^{-1}$

Then $(a_1 \circ a_2 \circ \ldots, a_n)^{-1}$
$= a_n^{-1} \circ \ldots, a_2^{-1} \circ a_1^{-1}$

Some additional Theorems

1) Cosets are equivalent ✓
2) Cosets are identical or disjoint. ✓
→ 3) Formal Def$\underline{n}$ of Index of a Subgroup.
4) Left congruence modulo H. ✓
5) Set equivalance is equivalance relation. ✓
6) Element in Left/Right Coset iff product with inverse in Subgroup. ✓
7) Congruence class modulo Subgroup is Coset. ✓

Theorem 1) Element in Left coset iff product with inverse in Subgroup.

Let G be a group
Let $H \leq G$ be a Subgroup of G
Let $x, y \in G$
Let yH denote the left coset of H by y.
Then $x \in yH \iff x^{-1} y \in H$

Proof

$x \in yH$
$\iff \exists h \in H : x = yh$ — Def$\underline{n}$ of left Coset
$\iff \exists h \in H : x^{-1} = h^{-1} y^{-1}$ — Inverse of Group product
$\iff \exists h \in H : x^{-1} y = h^{-1}$ — Product with y on the right.
$\iff x^{-1} y \in H$ — H is a Subgroup.

* Inverse of Group Product.

Theorem: Let $(G, \circ)$ be a group whose identity is e.
Let $a, b \in G$ with inverses a^{-1}, b^{-1}
Then $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$

Proof

$(a \circ b) \circ (b^{-1} \circ a^{-1}) = ((a \circ b) \circ b^{-1}) \circ a^{-1}$
$= (a \circ (b \circ b^{-1})) \circ a^{-1}$
$= (a \circ e) \circ a^{-1}$ — def of inverse element.
$= a \circ a^{-1}$
$= e$

↑ Group product iden[illegible]
$\Rightarrow$ inverse.

Element in Right Coset iff Product with inverse in Subgroup.

Let G be a group
Let $H \leq G$ be a subgroup of G
Let $x, y \in G$
Let $H \circ y$ denote the right coset of H by y.
Then $x \in Hy \iff xy^{-1} \in H$

Proof

Let $(G, *)$ be the Opposite Group of G.

→ Let $(G, \circ)$ be a group
We define a new operation $*$ on G by:
$\forall a, b \in G : a * b = b \circ a$
$(G, *)$ is called the opposite group to G.

Then:
$x \in Hy \iff x \in y * H$
$xy^{-1} \in H \iff y^{-1} * x \in H$
Since H is closed under inverses:
$xy^{-1} \in H \iff x^{-1} * y \in H$
By element in left coset iff product with inverse in subgroup.
$x \in y * H \iff x^{-1} * y \in H$
Hence the result.

Theorem 2) Set equivalance is equivalance relation.

Proof

For two sets to be equivalent, there needs to be a bijection between them.
In the following, let $\emptyset, \emptyset_1, \emptyset_2$, etc. be understood as bijections.

Reflexive

From identity mapping is bijection, the id mapping $I_S : S \to S$ is the required bijection.
Thus there exists a bijection from S to itself and S is therefore equivalent to itself

$\Rightarrow$ Set equivalance is reflexive.

□

Set Equivalance.
Let S & T be sets
S and T are equivalent iff there exists a bijection $f : S \to T$ between elements of S and those of T.
That is they have the same cardinality.
Written as $S \sim T$
for non-equivalence we write $S \nsim T$

Symmetric

$S \sim T$

$\to \exists \emptyset : S \to T$ Defn set equivalence

$\to \exists \emptyset^{-1} : T \to S$ Bijection iff inverse is bijection

$\to T \sim S$ Defn set equivalence: $\emptyset^{-1}$ is also a bijection.

$\Rightarrow$ Set equivalence is Symmetric.

Inverse of a bijection (bijective function) is also a bijection.

□

Transitive

$S_1 \sim S_2 \land S_2 \sim S_3$

$\to \exists \emptyset_1 : S_1 \to S_2 \land \exists \emptyset_2 : S_2 \to S_3$ Defn of Set equivalence

$\to \exists \emptyset_2 \circ \emptyset_1 : S_1 \to S_3$ Composite of bijection is bijection $\emptyset_2 \circ \emptyset_1$ is a bijection

$\to S_1 \sim S_3$ Defn of set equivalence.

$\Rightarrow$ Set equivalence is transitive

$\Rightarrow$ Set equivalance is equivalence relation.

■

Set Equivalence (of cosets)

Theorem 3) Cosets are Equivalent

All left cosets of a group G w.r.t a Subgroup H are equivalent

$\to$ That is any 2 left cosets are in one-to-one correspondance.
The same applies to right Cosets.
As a special case of this:

$\forall x \in G : |xH| = |H| = |Hx|$ where $H \leq G$

Proof 1

Follows directly from Set equivalence of regular representations.

If S is a finite subset of group G then

$|a \circ S| = |S| = |S \circ a|$ ie. $a \circ S$, S and $S \circ a$ are equivalent: $a \circ S \sim S \sim S \circ a$

Proof - Follows directly from both the left & right regular representations are permutations and therefore bijections.

Proof 2

Let us set up the mappings as follows: $\theta : H \to Hx$ and $\emptyset : Hx \to H$ as follows:

$\forall u \in H : \theta(u) = ux$

$\forall v \in Hx : \emptyset(v) = vx^{-1}$

From element in right coset iff Product with inverse in Subgroup.

$v \in Hx \Rightarrow vx^{-1} \in H$

Now

$\forall v \in Hx : \theta \circ \emptyset(v) = vx^{-1}x = v$

$\forall u \in H : \emptyset \circ \theta(u) = uxx^{-1} = u$

Thus $\theta \circ \emptyset = I_{Hx}$ and $\emptyset \circ \theta = I_H$ are Identity mappings

So $\theta = \phi^{-1}$: both are bijections and one is the inverse of the other.
This establishes, for each $x \in G$, the set equivalance between H and Hx:
$H \simeq Hx$
In particular for any $x, y \in G$, ~~the set equivalance~~ it follows from $Hx \simeq H$ and $Hy \simeq H$ that $Hx \simeq Hy$
by Set equivalance is equivalence relation.

Similarly we can set up mappings $\alpha: H \to xH$ and $\beta: xH \to H$ as follows:
$\forall u \in H: \alpha(u) = xu$
$\forall v \in xH: \beta(v) = x^{-1}v$
Analogous to above reasoning gives $\alpha = \beta^{-1}$ which establishes $H \simeq xH$
Also similarly $xH \simeq yH$ for all x, y in G
Hence the result.

Congruence Modulo Subgroup.

Left congruence modulo subgroup

Let G be a group
Let $H \leq G$ be a subgroup of G.

We can use H to define a relation on G as follows:

$$\mathcal{R}^l_H := \{(x,y) \in G \times G \mid x^{-1}y \in H\}$$

This is called left congruence modulo H.
When $(x,y) \in \mathcal{R}^l_H$, we write $x \equiv^l y \pmod H$ read as x is left congruent to y modulo H.

What is the function of modulo here??

Right congruence modulo subgroup.

Let G be a group.
Let $H \leq G$
We can use H to define a relation on G as follows:
$\mathcal{R}^r_H = \{(x,y) \in G \times G \mid xy^{-1} \in H\}$ ← This is called the right congruence modulo H.
When $(x,y) \in \mathcal{R}^r_H$ we write $x \equiv^r y \pmod H$ read as ~~y~~ x is right congruent to y modulo H.

By defn congruence classes are identical & disjoint.

Congruence Class modulo Subgroup is Coset.

Like residue class integers modulo n. Partitions set of integers.

1) Theorem: Left congruence class modulo subgroup is left coset
Let G be a group and $H \leq G$
Let $\mathcal{R}^l_H$ be ~~defined as~~ the equivalance defined as left congruence modulo H.
Then the equivalance class $[[g]]_{\mathcal{R}^l_H}$ of an element $g \in G$ is the left coset gH. This is known as the left congruence class of g mod H.

Proof

Let $x \in [[g]]_{\mathcal{R}^l_H}$ Defn left congruence modulo H. Thus $[[g]]_{\mathcal{R}^l_H} = gH$ ie. the equivalance class $[[g]]_{\mathcal{R}^l_H}$ of an element $g \in G$ equals the left coset gH.

Then $\to \exists h \in H: g^{-1}x = h$ Group properties
$\exists h \in H: x = gh$ Defn left Coset
$\to x = gH$ Defn Subgroup
$\to [[g]]_{\mathcal{R}^l_H} \subseteq gH$
Now let $x \in gH$ ~~Defn Coset~~ left
$\to \exists h \in H: x = gh$ ~~Group properties~~ Defn left coset
$\to g^{-1}x = h \in H$ ~~Defn left congruence modulo H~~ ~~Group~~ Group properties
$\to x \in [[g]]_{\mathcal{R}^l_H}$ Defn left congruence modulo H.
$\to$ $\therefore gH \subseteq [[g]]_{\mathcal{R}^l_H}$ Defn Subgroup.

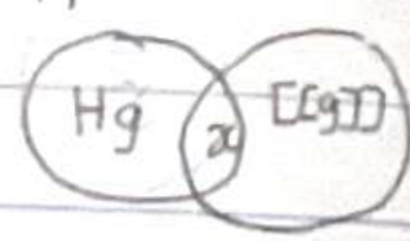
Theorem 2) Right congruence class modulo subgroup is Right Coset.

Let G be a group and $H \leqslant G$
Let $\mathcal{R}_H^r$ be the equivalence ~~relation~~ defined as right congruence modulo H.
Then the equivalence class $[[g]]_{\mathcal{R}_H^r}$ of an element $g \in G$ is the right coset Hg.
This is known as the right congruence class of g mod H.

Proof

Let $x \in [[g]]_{\mathcal{R}_H^r}$
Then:
$\exists_y\ \exists h \in H : xg^{-1} = h$ Defn of right congruence mod H.
$\rightarrow \exists h \in H : x = hg$ Group properties
$\rightarrow x = Hg$ Defn right Coset
$\rightarrow [[g]]_{\mathcal{R}_H^r} \subseteq Hg$ Defn Subgroup.

Suppose



Both need to be subsets of each other for set equivalence.

Now
Let $x \in Hg$
$\rightarrow \exists h \in H : x = hg$
$\rightarrow \exists h \in H : xg^{-1} = h \in H$
$\rightarrow x \in [[g]]_{\mathcal{R}_H^r}$
$\rightarrow Hg \subseteq [[g]]_{\mathcal{R}_H^r}$

Thus $[[g]]_{\mathcal{R}_H^r} = Hg$ ie. the equivalence class $[[g]]_{\mathcal{R}_H^r}$ of an element $g \in G$ equals the right coset gH.

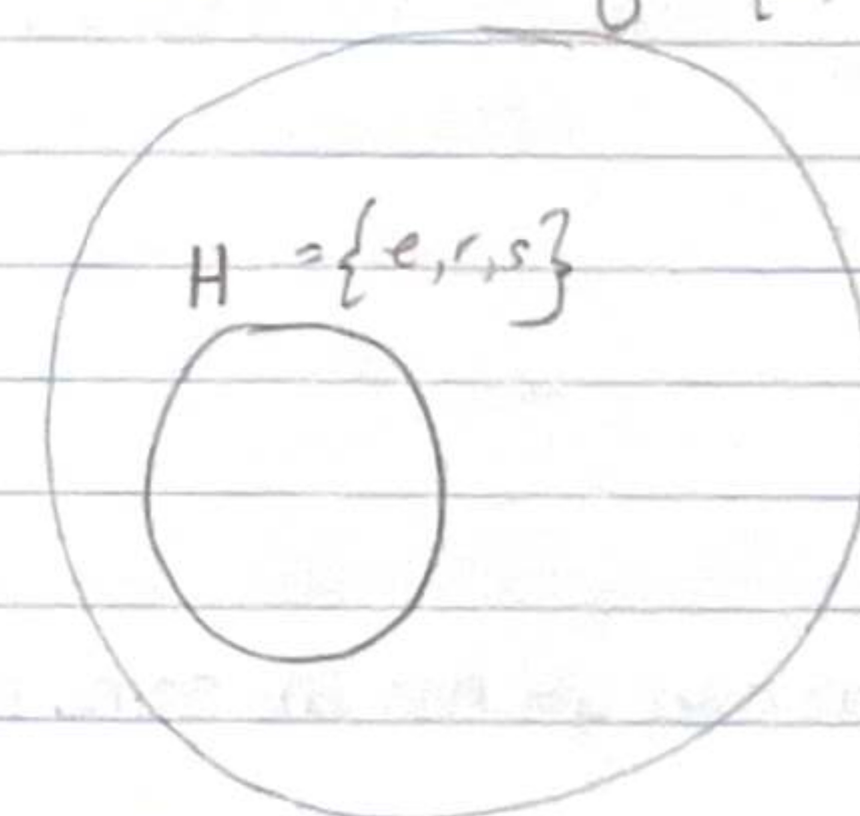
Another definition of the index of a subgroup. $|\text{left coset}| = |\text{right coset}|$
Let G be a group and $H \leqslant G$

The index of H (in G) is the cardinality of the left (or right) coset space G/H.
denoted $[G : H]$

The left coset space of G modulo H is the quotient set of G by left congruence modulo H, denoted G/H^l
It is the set of all the left cosets of H in G.
Same for right..

But why is a Coset Congruence class of elements of G modulo Subgroup ??
Intuition.

$G = \{e, r, s, a, b, c\}$



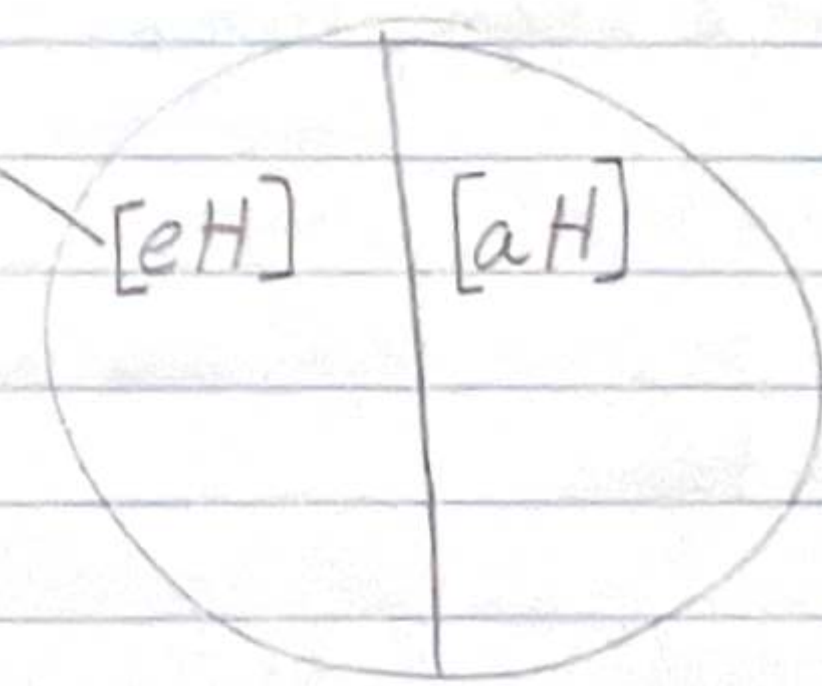
Review This.

Cosets are a way of decomposing a group
We shall consider left Cosets.

Congruence Classes $\begin{cases} eH = rH = sH = \{e, r, s\} \\ aH = bH = cH = \{a, b, c\} \end{cases}$

When we concider the congruence class of g mod H we are reffering to $g = \{e, r, s, a, b, c\}$ and $H = \{e, r, s\}$
Like in a modulo n for integers $[a]$ when n is known.
H is known $\Rightarrow [e], [a], \ldots$ class of set of Element of G congruent to Subgroup H.

a Congruence class



Lagrange's Theorem

Let G be a finite group.
Let H be a subgroup of G.

Then $|H|$ divides $|G|$ where $|H|$ and $|G|$ are the orders ~~of H and G~~ of H and G respectively.

In fact: $\boxed{[G:H] = |G|/|H|}$ where $[G:H]$ is the index of H.

Proof

Let G be a group
Let $H \leq G$

From Cosets are equivalent, a left coset gH has the same number of elements as H namely $|H|$

Since left cosets are either identical or disjoint, each element of G belongs to exactly one left coset.

From the definition of the index of a subgroup there are $[G:H]$ left cosets and therefore:

$$|G| = [G:H]\,|H|$$

→ (no of cosets x size of coset) gives size of group

Let G be of finite order
→ All 3 numbers are finite and the result follows

Let G be of infinite order

If $[G:H] = n$ is finite, then $|G| = n|H|$ and so H is of infinite order.
If H is of finite order such that $|H| = n$, then $|G| = [G:H] \times n$ and so $[G:H]$ is infinite.
↑ Coset Space G/H is infinite set.

What to do?

1. Review Previous Work.
2. Group Actions
3. General Linear Group & Special Linear Group
4. $SO(3)$
5. Orbit = Stabiliser Theorem
6. Sylow Theorems
7. Circle Group
8. Cyclic Groups
9. Normal Subgroups
10. Quotient Groups

11. Lie Algebra
12. General Relativity _ Group
13. Special relativity - Lorentz group
14. Klein-4 group
15. Gauge group
16. Other Algebras