Lecture 14 – Introduction to Group Theory

February 08, 2022

Section 5. Equivalence Relations and Partitions.

1. Prove that the non-empty fibres of a map form a partition of the domain.

Solution.

Let $\varphi : S \longrightarrow T$ be a map.

$\varphi^{-1}(t) = \{ s \in S$ such that $\varphi(s) = t \}$ is called fibre

I. (Method I) Show that

$S = \bigcup_{t \in T} \varphi^{-1}(t)$ and if $t_1 \neq t_2$, then $\varphi^{-1}(t_1) \cap \varphi^{-1}(t_2) = \phi$. for any $t_1, t_2 \in T$

Define $\varphi^{-1}(t) = \phi$ if $t \notin Im(\varphi)$.

[Since φ need not be onto map)

Now, it is enough to show pairwise disjointness.

If $\varphi^{-1}(t_1) \cap \varphi^{-1}(t_2) \neq \phi \Rightarrow \exists\, s \in S$ s.t. ~~$\varphi(t_1) = s$~~

$$\left.\begin{array}{l} \varphi(s) = t_1 \\ \varphi(s) = t_2 \end{array}\right\} \Rightarrow t_1 = t_2$$

II. (Method)

You may also show that

$$s_1 \underset{S}{\sim} s_2 \quad \text{if} \quad \varphi(s_1) = \varphi(s_2) \text{ in } T.$$

With this, consider

$$\varphi^{-1}(t) = \{ s \in S \text{ such that } \varphi(s) = t \}$$

Now prove that $s_1 \underset{S}{\sim} s_2$ defines an equivalence relation on S. Then you can conclude that equivalence classes partitions the set S.

[corresponding to non-empty fibre]

Remark. $\varphi : S \longrightarrow T$

Above approach works for any set S and T, hence in particular, when we introduce new structures such as Groups etc.

Q2. $S = \{ \text{Collection of Groups} \}$

Let $G_1, G_2 \in S$, define

$G_1 \sim G_2$ in S if G_1 is isomorphic to G_2.

Prove that "$\sim$" is an equivalence relation on S.

Solution.

Many choices

Reflexive. $G \sim G$ $\begin{cases} id : G \longrightarrow G \\ f : G \longrightarrow G, \ f \in Aut(G) \end{cases}$

Symmetric If $G \sim H$, then

$\exists \ \varphi : G \longrightarrow H$ isomorphism.

Then to show,

$\exists \ \psi : H \longrightarrow G$ an isomorphism

[Exercise: $\psi = \varphi^{-1}$]

Transitive. If $G \sim H$ and $H \sim K$, then prove that $G \sim K$.

$$\begin{tikzcd} G \arrow[r, "\varphi_1"] \arrow[dr, dotted, "\varphi_3 = \varphi_2 \circ \varphi_1"'] & H \arrow[d, "\varphi_2"] \\ & K \end{tikzcd}$$

$(Aut(G), \circ)$

Pro

3. Determine the number of equivalence relations on a set of five elements.

Solution. $S = \{a_1, a_2, a_3, a_4, a_5\}$

no. of equivalence relations on S = ?

In general, set $[n] = \{1, 2, \cdots, n\}$

Determine the $\underbrace{\text{number of equivalence}}$ on $[n]$?

$[1] = \{1\}$ ~ ?

$[2] = \{1, 2\}$ ~ ?

$[3] = \{1, 2, 3\}$ ~ ?

$\vdots$

$[5]$ ~ ?

Recall

Given a partition, one can define an equivalence relation $\xleftrightarrow[\text{correspondence}]{1-1}$ Given an equivalence relation, one can define partition

Conclusion. To know the number of equivelence relation on n element set, it is enough to know the number of all set partitions of n element set into non-empty parts.

[Combinatorics]. The number of all set partitions of n element into non-empty parts is given by

n-th Bell number $\quad B(n) = \sum_{i=0}^{n} S(n,i)$

$S(n,i)$ = The no. of partition of n-element set into i- non empty blocks.

"Stirling number of the second kind".

n	$B(n)$
$[1]$	$\{1\} = S(1,1)$
$[2] = \{1,2\}$	$\underbrace{\{1\}\{2\}}_{= S(2,2)}$ and $\underbrace{\{1,2\}}_{S(2,1)}$
$[3] = \{1,2,3\}$ $B(3) = 5$	$\underbrace{\{1\}\{2\}\{3\}}_{S(3,3)}$, $\left.\begin{matrix}\{1,2\}\{3\}, \\ \{1,3\}\{2\} \\ \{2,3\}\{1\}\end{matrix}\right\} S(3,2)$ $\quad \underbrace{\{1,2,3\}}_{S(3,1)}$

$S \neq \phi$

4. $R \subseteq S \times S$ and $R' \subseteq S \times S$

Given R and R' are equivalence relations on $S \times S$

(a). Is $R \cap R'$ an equivalence relation?

(b) Is $R \cup R'$ an equivalence relation?

(Exercise)

Solution.

(a). $R \cap R'$

Reflexive. If $(a,a) \in R$ and $(a,a) \in R'$ for all $a \in S$,

then $(a,a) \in R \cap R'$ for all $a \in S$.

Symmetric. Let $(a,b) \in R \cap R'$

$\Rightarrow$ $(a,b) \in R$ and $(a,b) \in R'$

$\Rightarrow$ $(b,a) \in R$ and $(b,a) \in R'$

$\Rightarrow$ $(b,a) \in R \cap R'$

Transitive. Let $(a,b) \in R \cap R'$ and $(b,c) \in R \cap R'$

Show that $(a,c) \in R \cap R'$. [Easy verification]

Hence $R \cap R'$ is an equivalence relation.

Part (b) Exercise.

5. [Done in class]

6. Similar problem.

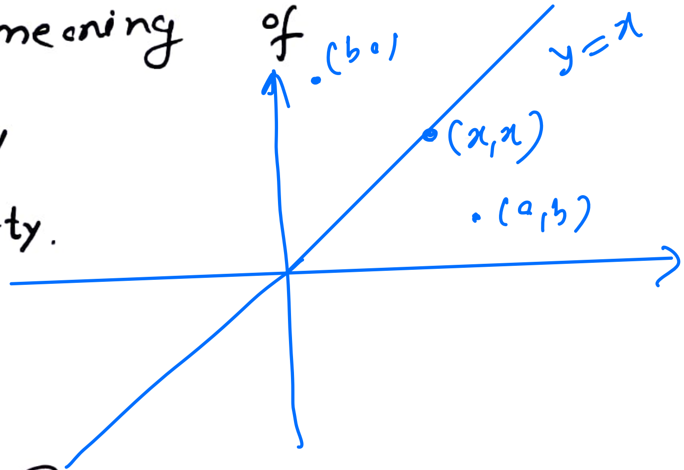
7. $\mathcal{R}$: A relation on the set $\mathbb{R}$ of real numbers

$$\mathcal{R} \subseteq \mathbb{R} \times \mathbb{R} \quad (x\text{-}y \text{ plane})$$

Explain the geometric meaning of

(a) reflexive property

(b) Symmetric property.



Solution.

(a) Reflexive. $(a,a) \in \mathcal{R}$ i.e. $a \sim a$

or $(a,a) \in \mathbb{R}\times\mathbb{R}$ ~~with~~ s.t. $(a,a) \in \mathcal{R}$

(b) Symmetric.

$a \sim b \Rightarrow b \sim a$ in $\mathcal{R}$.

8. $R \subseteq \underbrace{\mathbb{R} \times \mathbb{R}}_{x\text{-}y \text{ plane}}$

Axiom:

(i) Reflexive

(ii) Symmetric

(iii) Transitive

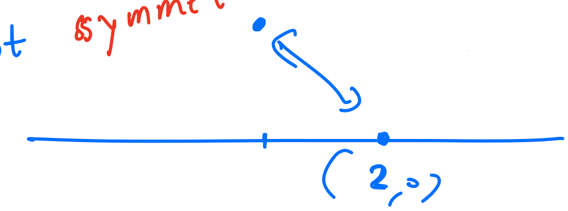
Which axioms are satisfied and whether R is an equivalence reation on $\mathbb{R}$.

(a). $R = \{(s,s) \mid s \in \mathbb{R}\}$

(b) $R =$ empty set

not symmetric

(c) $R =$ locus $\{y=0\}$



(d) $R =$ locus $\{xy+1=0\}$

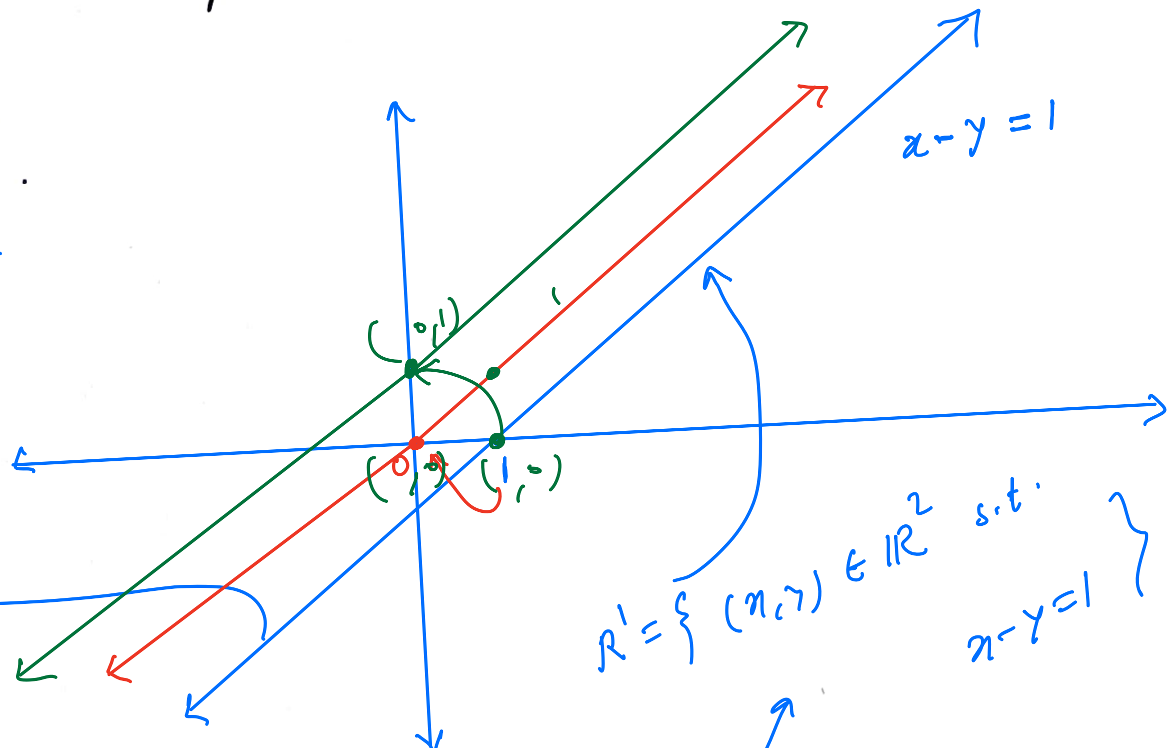
(e) $R=$ locus $\{x^2y - xy^2 - x + y = 0\}$

(f) $R=$ locus $\{x^2 - xy + 2x - 2y = 0\}$

9. Draw the smallest equivalence relation on the set of real numbers which contains the line $x-y=1$ in the x-y plane and sketch it.

[Exercise]

$R \subseteq \mathbb{R}\times\mathbb{R}$



$R' = \{(x,y) \in \mathbb{R}^2 \text{ s.t. } x-y=1\}$

more elts.

reflexive property

(x,x) in R'

$x - x = 1$
$\Rightarrow 1 = 0$

{ Work out the details to find smallest equivalence relation and draw them in the x-y plane

Section 6. [Cosets]

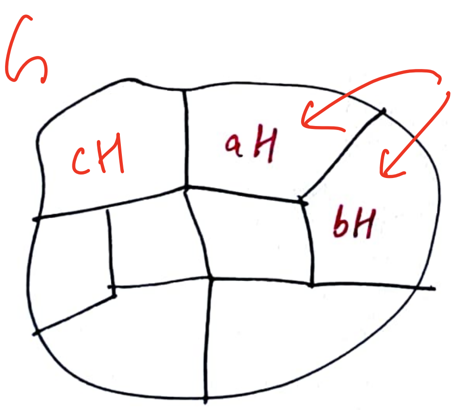
Recall. Let H be a subgroup of a group G. A left coset is a subset of the form

$a \in G$, $$aH = \{ \underbrace{a * h}_{ah} \mid h \in H \}$$

Clearly, $1_H \cdot H = H$ [i.e. H itself is a coset]

Recall. $a, b \in G$, $a \underset{G}{\sim} b$ if $b = ah$ for some $h \in H$

[Equivalence relation on G by H]



$\downarrow$ Partitions G into equivalence classes (left cosets)

$$aH = bH \iff a = b$$

$$aH \cap bH = \phi \quad \text{or} \quad aH = bH$$

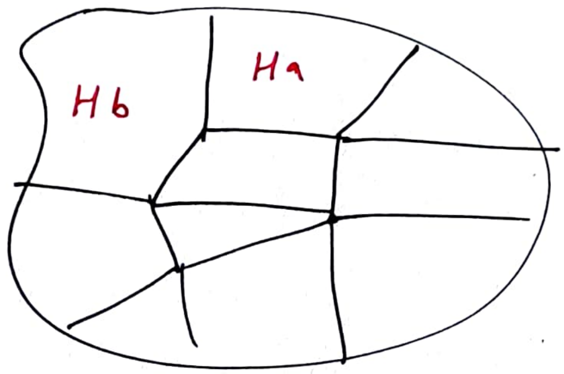
$[G : H] :=$ number of left cosets of H in G

[Index of H in G]

In a similar way, one can define right cosets of H in G.

$$Ha = \{ ha \mid h \in H \}$$

$a \underset{G}{\sim} b$ if $b = ha$ for some $h \in H$



Remark. "aH need not be Ha" for $a \in G$.

Exercise. Find three examples for this.

Proposition. A subgroup H of a group G is

normal $\iff$ $aH = Ha$ for every $a \in G$.

$ah = h'g$ $\quad h' = ahg^{-1}$

[self reading, Artin, page 59]

1. Determine the index $[\underset{G}{\mathbb{Z}} : \underset{H}{n\mathbb{Z}}]$

Left cosets of $n\mathbb{Z}$ in $\mathbb{Z}$ are

$$\left.\begin{array}{l} \bar{0} + n\mathbb{Z} \\ \bar{1} + n\mathbb{Z} \\ \vdots \\ \overline{n-1} + n\mathbb{Z} \end{array}\right\} \quad n \text{ distinct (left) cosets}$$

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

3. Prove that every group whose order is a power of prime p contains an element of order p.

Solution. $|G| = p^n$ for some $n \geq 1$ and p is prime no..

[To show $\exists\, a \in G$ s.t. $a^p = id.$]

Cases:

If $n = 1$, then $|G| = p$

$\Rightarrow$ No non-trivial subgroup

$$\Rightarrow \quad G = \langle a \rangle \text{ with } a^p = 1$$
$$\qquad \| $$
$$\langle 1, a, a^2, \ldots, a^{p-1} \rangle$$

$$\boxed{|G| = |\langle a\rangle| \cdot |G : \langle a\rangle|}$$

$\left[|G| = |H| \cdot [G:H] \right]$ Lagranges theorem.

$\Rightarrow$ $|\langle a\rangle|$ divides $|G|$.

<u>Case</u>:

<u>Let $n > 1$,</u> and $|G| = p^n$

then $|a|$ divides p^n $\quad p \cdot p^{m-1}$ $\quad a^{\cdot p(p^{m-1})} = id.$

$\Rightarrow$ $|a| = p^m$ for some $m \leq n$

$\Rightarrow$ $|a^{p^{m-1}}| = p$

Recall Exercise

$|x| = rs$, then

$|x^r| = s$

Infact. $|a^{p^m}| = 1$

4. Give an example

left cosets and right cosets of $GL_2(\mathbb{R})$ in $GL_2(\mathbb{C})$ are not equal.

Find $g \in GL_2(\mathbb{C})$ such that

$g \cdot GL_2(\mathbb{R}) \neq GL_2(\mathbb{R}) \cdot g$

8. W : Additive subgroup of $\mathbb{R}^m$ of solutions of a system of homogeneous equation (linear) $AX = 0$.

Show that the solution of an inhomogeneous system $AX = B$ form a coset of W.

Solution.

Is W a subgroup of $\mathbb{R}^m$?

(i) identity element $0 = (0, 0, \dots, 0) \in \mathbb{R}^m$ $\quad A \cdot 0 = 0$

(ii) If $\underset{X}{(u_1, \dots, u_m)}$ & $\underset{Y}{(v_1, \dots, v_m)}$ are solutions of $AX = 0$

then $(u_1 + v_1, \dots, u_m + v_m)$ is also a solution of $AX = 0$

$A(X+Y) = 0$

(iii) Inverse element exists for every $w \in W$.

<u>Cosets</u> $\{ \underline{x} + W$ such that $\underline{x} \in \mathbb{R}^m \}$

$\|$ [$\because \mathbb{R}^m$ is Abelian]

$\{ W + \underline{x}$ such that $\underline{x} \in \mathbb{R}^m \}$

Given $[G:H]=2$

10. (a) Prove that every subgroup of index 2 is normal.

(b) Give an example of a subgroup of index 3 which is not normal.

Solution

(a) $[G:H]=2 \Rightarrow G = H \cup gH$

Let $g \notin H$ then we can write $G = H \cup Hg$

(why)

$\Downarrow$

$gH = Hg$ for all $g \in G$

$\Downarrow$

H is normal. $\left(\Leftrightarrow gH = Hg\right)$

(b) $[\underset{G}{S_3} : H] = 2$

H: subgroup of S_3 of order 2

then

$$|S_3| = |H| \cdot [G:H]$$

$$6 = |H| \cdot 3 \Rightarrow |H| = 2$$

Take $H = \{e,(12)\}$ or $\{e,(13)\}$ or $\{e,(23)\}$

Find $g \in S_3$ s.t. $gH \neq Hg$

(Exercise)

Revision.

Assume $|G| < \infty$ (finite)

g. Let $|G| = p$; p a prime number. Then G is cyclic and $G \cong \mathbb{Z}/p\mathbb{Z}$

Proof. $G = \langle a \rangle$ to be shown

$\exists\, a \in G$ s.t. $|a| \neq 1$ $(\because p > 1)$

$\Rightarrow \langle a \rangle = \langle 1, a, a^2, \dots \rangle$

Since $|\langle a \rangle|$ divides $|G| = p$

$\Rightarrow |\langle a \rangle| = p$

$\Rightarrow \langle a \rangle$ is cyclic & $G \cong \mathbb{Z}/p\mathbb{Z}$

[$\Rightarrow \langle a \rangle$ is also Abelian.]

$$(\mathbb{Z}/p\mathbb{Z})^* = \{1, 2, \dots, p-1\}$$

$$x \in$$

Since $|(\mathbb{Z}/p\mathbb{Z})^*| = p-1$

$$\Rightarrow \quad x^{p-1} = 1 \quad \text{in } (\mathbb{Z}/p\mathbb{Z})^*$$

Equivalent to

$$x^{p-1} \equiv 1 \mod (p)$$

$$\Rightarrow \quad x \cdot x^{p-1} \equiv x \mod (p)$$

$$\Rightarrow \quad x^p \equiv x \mod (p)$$

{Fermat's Little Theorem}

Number Theory

Given $n \in \mathbb{N}$ and $x \in \mathbb{Z}$ with $\gcd(x, n) = 1$, Then

$$x^{\varphi(n)} \equiv 1 \pmod{n}$$

(Euler's generalization of Fermats Little theorem)