

PROOFS OF SOME CLASSICAL THEOREMS USING GROUP THEORY

TISYA CHANDRASHEKHAR RAWAT

CONTENTS

1. Equivalence Relation and Partition	1
2. Mapping between sets	3
3. Groups, Homomorphism, Modular Arithmetic, and Wilson's Theorem	6
4. Quotient Group and theorems of Lagrange, Fermat, Euler on Finite Groups	11
5. Future work	14
6. Acknowledgement	14

ABSTRACT. This is an evolving document on my attempt to write first expository article on some interesting elementary results of group theory and applications to prove elementary number theoretic theorems of Wilson, Lagrange, Fermat and Euler. I did this project under the guidance of my mentor [Yaashaa Golovanov](#).

1. EQUIVALENCE RELATION AND PARTITION

Definition 1.1 (Partition of Set). Let X be a set. Let $\mathcal{C} = \{X_i | i \in \mathcal{I}, X_i \subset X\}$ be some collection of non empty subsets of set X . We say $\mathcal{C}$ defines a **partition** of X if followings are true

- for every $i, j \in \mathcal{I}$ whenever $i \neq j$ we must have $X_i \cap X_j = \emptyset$
- $\cup_{i \in \mathcal{I}} X_i = X$

Definition 1.2 (Equivalence Classes). Let X be a set. Let $\sim$ be an equivalence relation on X . Define **equivalence class** of an element $x_o \in X$ as collection : $[x_o]_{\sim} = \{x \in X | x \sim x_o\}$. Since $\sim$ is an equivalence, and thus reflexive relation on X . Therefore, for each $x \in X$, $x \sim x$, and hence $x_o \in X$, $x_o \in [x_o]_{\sim}$. So, equivalence class of any element is never an empty set.

Theorem 1.1 (Equivalence Classes are mutually disjoint). Let $x_1, x_2 \in X$. Let $[x_1]_{\sim}$ and $[x_2]_{\sim}$ be respective equivalence classes. We claim, if $x' \in [x_1]_{\sim} \cap [x_2]_{\sim}$ then $[x_1]_{\sim} = [x_2]_{\sim}$

Proof. Let $x' \in [x_1]_{\sim} \cap [x_2]_{\sim}$. So, by definition 1.2 of equivalence class, $x' \sim x_1$ and $x' \sim x_2$. This means $x_1 \sim x' \sim x_2 \implies x_1 \sim x_2 \implies [x_1]_{\sim} \subset [x_2]_{\sim}$. Verbatim argument also implies $[x_2]_{\sim} \subset [x_1]_{\sim}$. So, if one element is common in two equivalence classes then they coincide. Which, contra-positively means, if two equivalence classes do not coincide then they have no element in common at all. That means any two equivalence classes are mutually disjoint. $\square$

Theorem 1.2 (Equivalence classes form a set theoretical cover). *Let X be a set. Let $\sim$ be an equivalence relation on X . Then $X = \bigcup_{i \in \mathcal{I}} [x_i]_{\sim}$.*

Proof. Note that by definition 1.2, for each $x \in X$ and for each $i \in \mathcal{I}$, $[x_i]_{\sim} \subset X$. So, $\bigcup_{i \in \mathcal{I}} [x_i]_{\sim} \subset X$. For other side inclusion, note that for each $x \in X$, $x \in [x]_{\sim}$ therefore, $X \subset \bigcup_{i \in \mathcal{I}} [x_i]_{\sim}$. This closes the proof. $\square$

So, theorem 1.2 establishes that corresponding to each equivalent relation we have a partition of the underlying set. In what follows we will prove that converse is true as well. That is "given a partition there exist a corresponding equivalent relation on the given set".

Theorem 1.3 (Partition induces an equivalence relation). *Let $\mathcal{P} = \{X_j | j \in \mathcal{J}, X_j \subset X\}$ be a partition of the set X . We claim that this partition induces an equivalence relation on set X .*

Proof. Define a relation $\mathcal{R}$ on the set X as : $x_1 \mathcal{R} x_2$ iff there exist a $j \in \mathcal{J}$ such that $x_1, x_2 \in X_j$.

- **Reflexive.** For each $x \in X$, there exists exactly one $X_j \in \mathcal{P}$ such that $x \in X_j$. So, x is $\mathcal{R}$ related to itself and hence $\mathcal{R}$ is a reflexive relation on X .
- **Symmetric.** Let $x_1 \mathcal{R} x_2$. This means, by definition of $\mathcal{R}$, that there exist a $j \in \mathcal{J}$ and corresponding $P_j \in \mathcal{P}$ such that $x_1 \in P_j$ and $x_2 \in P_j$. However, this effectively means $x_2 \mathcal{R} x_1$. So, $\mathcal{R}$ is symmetric relation on X .
- **Transitive.** Let $x_1 \mathcal{R} x_2$, and $x_2 \mathcal{R} x_3$. By definition of $\mathcal{R}$, there exist $j, k \in \mathcal{J}$ and corresponding $P_j, P_k \in \mathcal{P}$, such that $x_1, x_2 \in P_j$ and $x_2, x_3 \in P_k$. However, $\mathcal{P}$ is a partition of X and $x_2 \in P_j \cap P_k$. So, j must be equal to k . That is, $P_j = P_k$ and this gives $x_1, x_3 \in P_j$. Hence, the relation $\mathcal{R}$ is transitive on X . $\square$

Example 1.1 (Every function defines an equivalence relation). $f : X \rightarrow Y$ be any mapping. Define a relation $\sim$ on X as $x_1 \sim x_2 \iff f(x_1) = f(x_2)$. This $\sim$ obviously is an equivalence relation because equality implies equivalence. Though converse is not true.

What are equivalence classes of this equivalence relation ?. Well, all elements which are mapped to a common image form an equivalence class. That is $[x_0]_{\sim} = \{x \in X | f(x) = f(x_0)\}$.

Example 1.2. *Every equality defines an equivalence relation. However, converse is not true.*

Once can ask a basic question can we turn an equivalence into equality. The answer is yes. It is possible in certain suitable sense - equivalence becomes equality in quotient set, quotient group or say in quotient object. By this we mean that if $\sim$ is an equivalence relation on X and $\mathcal{C}$ is collection of equivalence classes corresponding to this relation, then $[x]_{\sim} = [x']_{\sim}$, (equality of equivalence classes) if and only if $x \sim x'$, Theorem 1.1. In this sense one can say that equivalence relation induced equality in quotient set or quotient object.

2. MAPPING BETWEEN SETS

In this section, we will prove the necessary and sufficient condition for a mapping between two sets to be **injective, surjective and bijective**.

Definition 2.1 (Injection). Let $\phi : X \rightarrow Y$ be a mapping. We say ϕ is an injections of X into Y if any of the following are true

- (1) whenever $x_1 \neq x_2$ then $\phi(x_1) \neq \phi(x_2)$; that is, distinct element have distinct images. Contra-positively, we say that ϕ is an injection if $\phi(x_1) = \phi(x_2) \implies x_1 = x_2$

Definition 2.2 (Left Inverse). Let $\varphi : X \rightarrow Y$ be a function. We say that $f : Y \rightarrow X$ is a left inverse of φ if $f \circ \varphi = I_X$, the identity mapping on set X .

Theorem 2.1 (Injection and Left Inverse). Let $\varphi : X \rightarrow Y$ be a mapping. Followings are equivalent

- (1). φ is an injection
(2). φ has a left inverse

Proof. We prove both implications using Definitions 2.1, 2.2.

- (2) $\rightarrow$ (1) Let us assume that $f : Y \rightarrow X$ is left inverse of $\varphi : X \rightarrow Y$. By definition, $f \circ \varphi = I_X$. Now, let $\varphi(x_1) = \varphi(x_2)$. Given that f is a function defined on Y , so equal inputs to f must give equal outputs. That is, $f(\varphi(x_1)) = f(\varphi(x_2))$. However, we know that $f \circ \varphi : X \rightarrow X$ is an identity map of X . Therefore, $f(\varphi(x_1)) = x_1 = f(\varphi(x_2)) = x_2$. This proves that $\varphi : X \rightarrow Y$ is indeed an injective map, Definition 2.1.
- (1) $\rightarrow$ (2) Let us assume that φ is an injection. We need to construct a function $f : Y \rightarrow X$ such that $f \circ \varphi = I_X$. So, by definition, we have to ensure that for each $y \in Y$, $f(y)$ is uniquely defined. Recall that inverse image of an element under any map, and thus for φ , is well defined as set $\varphi^{-1}(y) := \{x \in X | \varphi(x) = y\}$. Furthermore, if φ is an injective map then $\varphi^{-1}(y) := \{x \in X | \varphi(x) = y\}$ is singleton. Hence we define map f as, for any arbitrary but fixed element $x_o \in X$,

$$(1) \quad f(y) := \begin{cases} x & \text{if } \varphi(x) = y \\ x_o & \text{if } y \notin \text{Im}(\varphi) \end{cases}$$

Indeed, it is obvious that $f \circ \varphi = I_X$. □

Definition 2.3 (Surjection). Let $\varphi : X \rightarrow Y$ be a mapping. We say φ is a surjection of X into Y if any of the followings are true

- (1) $\forall y \in Y, \exists x \in X$ such that $\varphi(x) = y$. That is, if each element in Y is image of at least one element in X .
(2) for any $y \in Y$, the collection $\varphi^{-1}(y)$ is never an empty set, Φ .

Definition 2.4 (Right Inverse). Let $\varphi : X \rightarrow Y$ be a function. We say that $f : Y \rightarrow X$ is a right inverse of φ if $\varphi \circ f = I_Y$, the identity mapping on set Y .

Theorem 2.2 (Surjections and Right Inverse). *Let $\varphi : X \rightarrow Y$ be a mapping. Followings are equivalent*

- (1). φ is an Surjection
- (2). φ has a Right inverse

Proof. We prove both implications using Definitions 2.3, 2.4.

- (2) $\rightarrow$ (1). Let us assume that $f : Y \rightarrow X$ be right inverse of $\varphi : X \rightarrow Y$. That is, $\varphi \circ f(y) = I_Y$. In sense of Definition 2.3, we need to show that for each $y \in Y$, $\varphi^{-1}(y) \neq \Phi$. So, let y_0 be an arbitrary element of Y . We can choose such element as set $Y \neq \Phi$. Since $f : Y \rightarrow X$ is a function so $f(y_0) = x_0$ is unique image of y_0 under f . Also, given that $\varphi \circ f = I_Y$, so $\varphi \circ f(y_0) = \varphi(f(y_0)) = \varphi(x_0) = y_0$. That is, $x_0 \in \varphi^{-1}(y_0)$. This closes the proof.
- (1) $\rightarrow$ (2). Let us assume that $\varphi : X \rightarrow Y$ is a surjection. Then we have to construct a right inverse $f : Y \rightarrow X$ of φ . That is, $\varphi \circ f = I_Y$. Let $y_0 \in Y$ be an arbitrary element. Since, φ is surjection, therefore by Theorem 2.3, there exists at least one $x_0 \in X$ such that $\varphi(x_0) = y_0$. Now, the question is why can't we just define $f(y_0) = x_0$? Well, it is not necessary that $\varphi^{-1}(y_0)$ is exactly one element. There may be more than one preimages of y_0 under φ . Therefore, the preceding definition of $f(y_0) = x_0$ would not be a well defined single valued function. To circumvent this problem, we decompose X into family of non empty mutually disjoint sets as $X = \bigcup_{y \in Y} \varphi^{-1}(y)$. This forms the partitions, in sense of Definition 1.1, of X . We can use axiom of choice to choose an element from each member of the collection $\mathcal{C} = \bigcup_{y \in Y} \varphi^{-1}(y)$ and we define $f(y) := x$ such that x is arbitrarily fixed element of $\varphi^{-1}(y)$. An important point of this construction is that it right inverse of a function is not unique because we have multiple elements available, in each sub-collection $\varphi^{-1}(y)$, if φ were not necessarily injection, however, surely a surjection.

□

Definition 2.5 (Bijection). *Let $\varphi : X \rightarrow Y$ be a mapping. We say, f is a bijection if it is injection and surjection both.*

Theorem 2.3. *Let $\phi : X \rightarrow Y$ be a mapping. We say φ is a bijection if and only if φ has left as well as right inverse.*

Proof. This immediately follows from the Definition 2.5 and Theorems 2.1, 2.2. □

Theorem 2.4. *If a function $f : X \rightarrow Y$ has left and right inverse both then these two inverses must coincide.*

Proof. Let $f : X \rightarrow Y$ be a map and let $g : Y \rightarrow X$ be its left inverse and $h : Y \rightarrow X$ be its right inverse. That is, $g \circ f = I_X$ and $f \circ h = I_Y$. Now, let $g \neq h$ then there exist at least one $y_0 \in Y$ such that $g(y_0) = x_1 \neq h(y_0) = x_2$. Now, f has right inverse so it is a surjection and hence there exist an element $x_0 \in X$ such that $f(x_0) = y_0$. Now, g is a function and left inverse of f , so $g(f(x_0)) = x_0 = g(y_0) = x_1$. Also, f is a function and h is its right inverse, so $f(h(y_0)) = y_0 = f(x_2)$. So, $f(x_0) = f(x_2)$, but f

is an injection so $x_0 = x_2$. We conclude that $x_1 = x_0 = x_2$. But this contradicts our initial assumption. Hence, $g(y_0) = x_1 \neq h(y_0) = x_2$. Hence, if map is bijective then it has unique left and right inverse and these left and right inverses coincide with each other. $\square$

Example 2.1 (Canonical projection). Let $\sim$ be an equivalence relation on set X . Then the mapping $X \rightarrow X/\sim$ defined by $x \mapsto [x]_\sim$ is known as canonical projection and is obviously a surjective map.

To see why it is obvious, we invoke the Definition 2.3 of surjection. Collection $\mathcal{C} = \{[x]_\sim | x \in X\}$ forms partition of X and this partition is induced by equivalence relation of Example 1.1. In example 1.1, the equivalence class of an element x' consists of essentially those and only those elements in X which have the same image, under the mapping f , in set Y .

The object $X/\sim$, in example 2.1, is called as **quotient set** induced by equivalence relation $\sim$.

Injection and Surjection maps, defined in Definitions 2.1 2.3, form the basic building blocks out of which any map can be constructed. Theorem 2.5 establishes this assertion and is one of the significant result with deep manifestation in proof of first isomorphism theorem of the group.

Theorem 2.5 (Function decomposition and Quotient set). Let $f : X \rightarrow Y$ be any function. Define equivalence relation on X as defined in example 1.1. That is $x_1 \sim x_2$ if and only if $f(x_1) = f(x_2)$. Then we have following elegant decomposition of function

- $\pi : X \rightarrow X/\sim$ is a natural surjection in the sense of Definition 2.3
- $\varphi : X/\sim \rightarrow \text{Im}(f)$ defined by $\varphi([x]_\sim) = f(x)$ is a bijection in the sense of Definition 2.5
- $\iota : \text{Im}(f) \rightarrow Y$ given by is a natural injection, also called as inclusion, in the sense of Definition 2.1

Proof. I learnt this non trivial beautiful theorem and its proof from my mentor **Yaashaa Golovanov** I will explain the proof here.

Note that for any $[x_0]_\sim \in X/\sim$, $x_0 \in X$, so $\pi(x_0) = [x_0]_\sim$ is, by definition, a surjection. ι also is, by definition, an injection. The difficult part is to prove that $\varphi([x]_\sim) = f(x)$ is a bijection. To prove this, we need to show three things

- $\varphi([x]_\sim) = f(x)$ is **well defined**. To prove that it is well defined we have to basically establish that equal inputs gives equal output. So, let us assume that $[x_1]_\sim = [x_2]_\sim$. Then by Theorem 1.1, $x_1 \sim x_2$ and by definition of equivalence relation, given in statement of this theorem, $f(x_1) = f(x_2)$ which, by definition of φ , implies that $\varphi([x_1]_\sim) = \varphi([x_2]_\sim)$
- φ is an **injective map**. We have to prove that equal output $\varphi([x_1]_\sim) = \varphi([x_2]_\sim)$ gives equal input $[x_1]_\sim = [x_2]_\sim$. To begin with, let $\varphi([x_1]_\sim) = \varphi([x_2]_\sim)$. By definition of φ , $\varphi([x_1]_\sim) = f(x_1)$ and $\varphi([x_2]_\sim) = f(x_2)$. So, $f(x_1) = f(x_2)$. By definition of equivalence relation under consideration, $f(x_1) = f(x_2) \implies x_1 \sim x_2$ and this means, by Theorem 1.1, $[x_1]_\sim = [x_2]_\sim$.

- **φ is a surjective map.** Let $y_0 \in \text{Im}(f)$. This means there exist an $x_0 \in X$ such that $f(x_0) = y_0$. Since, equivalence classes form the partition of X , one candidate for an equivalence class which contains x_0 is $[x_0]_{\sim}$ itself and image of this class under φ is $f(x_0) = y_0$. This closes the proof. $\square$

Remark 2.1. Notice that this theorem says that *Every set theoretical map, $f : X \rightarrow Y$, is composition of surjective map, followed by bijective map, followed by injective map. Moreover, the bijection φ induced by f itself.*

Remark 2.2. There is deep implication of this equivalence relation in canonical (natural) projection and this later manifest itself in isomorphism theorems of group, which we state here for its own sake and leave the proof for later section.

Theorem 2.6 (First isomorphism theorem of group). Let G be a group in sense of Definition 3.1. Let $\varphi : (G, *) \rightarrow (H, \Delta)$ be a group homomorphism. Let N be kernel of φ in sense of Definition 3.8. Then followings are true

- The kernel N of φ is a **normal subgroup** of G .
- The image $\varphi(G)$, of homomorphism φ , is a subgroup of H in sense of Definition 3.3 and
- The image $\varphi(G)$ is isomorphic to the quotient group G/N . One classic example of quotient group is introduced in example 3.4.

3. GROUPS, HOMOMORPHISM, MODULAR ARITHMETIC, AND WILSON'S THEOREM

Definition 3.1 (Group). Let G be a set with $*$ as binary operation on G . We say G is a group or has structure of group if followings are simultaneously true

- $*$ is an associative operation, that is, for each $g_1, g_2, g_3 \in G$, $g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$
- There exists an unique element $e_G \in G$ such that for each $g \in G$

$$g * e_G = e_G * g = g$$

This element e_G , with above stated property, is called as **identity element** of G

- for each $g \in G$, there exist an unique element $g' \in G$ such that $g * g' = g' * g = e_G$. We denote g' as g^{-1} and call it as **inverse of element** $g \in G$

Definition 3.2 (Abelian or Commutative group). Let $(G, *)$ be a group. We say that G is Abelian or commutative group with respect to $*$ if and only if $g_1 * g_2 = g_2 * g_1$ for all $g_1, g_2 \in G$

In mathematics, we study mathematical objects and their properties. When one mathematical object interacts with other mathematical objects, we get to know more about the given objects. The interaction among mathematical objects, say for now, happens through the mapping between them. So, for example, when a group $\mathbf{G}$ interacts with an abstract set $\mathbf{A}^1$, $\mathbf{G}$ reveals more about itself. By this we mean that we get

¹By abstract set, we mean an structure free object, that is, having no algebraic operation a prior.

to know more substructure, $\mathbf{S}$ of $\mathbf{G}$, satisfying same set of axioms as $\mathbf{G}$. **One of the recurring theme in study of modern mathematics** is that **Given a mathematical object $\mathbf{O}$ does there exist a sub-object $\mathbf{S}$ of it ? That is a $\mathbf{S} \subset \mathbf{O}$ which exactly has same set of axioms endowed on it as on $\mathbf{S}$.** One particular instance of this theme forms the content of Definition 3.3.

Definition 3.3 (Subgroup). Let $(G, *)$ be a group with binary operation $*$. Let H be a subset of G . We say H is subgroup of G , and write it as $H \leq G$ if restriction of $*$ on H satisfies all three axioms of group listed in 3.1 So, any subset of G which is a group in its own right, however, with same binary operation and unit element as that of G

Theorem 3.1. Let $(G, *)$ be a group and let $H \subset G$. H is subgroup of G , written as $H \leq G$, if and only if for each $h_1, h_2 \in H$, $h_1 * h_2^{-1} \in H$.

Proof. Let us assume that $H \leq G$ in sense of Definition 3.3. This means $(H, *)$ is group in its own right. Let $h_1, h_2 \in H$. $(H, *)$ being group guarantees, by Definition 3.1, that $h_2^{-1} \in H$, and hence $h_1 * h_2^{-1} \in H$. Now assume that, for each $h_1, h_2 \in H$, $h_1 * h_2^{-1} \in H$. In particular, $h_1 * h_1^{-1} = e_G \in H$. Let $h \in H$. Since, $e_G \in H$, therefore, $e_G * h^{-1} = h^{-1} \in H$. Let $h_1, h_2 \in H$, given that $h_1 * h_2^{-1} \in H$, implies $(h_1^{-1})^{-1} * h_2 = h_1 * h_2 \in H$. Associativity in H is induced due to closure of $*$ on H and associativity of $*$ on G . Hence, $H \leq G$. $\square$

Definition 3.4 (Order). Let $(G, *)$ be a group. Let $g \in G$. We say a positive integer n is the order, denoted as $|g|$, of g if and only if $g^n = e_G$ and n is the smallest such positive integer. If there is no such integer n , then we say that order of g is infinite.

Theorem 3.2. Let $(G, *)$ be a group. Let m be a positive integer such that $g^m = e_G$. Then $|g|$ divides m .

Proof. Let $|g| = n$. That is, $g^n = e_G$. It is given that $g^m = e_G$. By Euclid's division lemma, there exist integers q, r such that $m = nq + r$, where $0 \leq r < n$. Using this we get $g^m = g^{nq+r} = g^{nq} * g^r = g^r = e_G$ and $r < n$, and n is the smallest positive integer for which $g^n = e_G$. Hence, $r = 0$. That is $m = nq$. That is, n divides m . $\square$

Definition 3.5 (Group Homomorphism). Let $(G, *)$ and (H, Δ) be groups. Then a map $\varphi : (G, *) \rightarrow (H, \Delta)$ is said to be a group homomorphism if

$$(2) \quad \forall g, g' \in G, \varphi(g * g') = \varphi(g) \Delta \varphi(g')$$

Example 3.1 (An appealing Example). The exponential map

$$e : (\mathbb{R}, +) \rightarrow (\mathbb{R}, \times) \text{ defined as } x \mapsto e^x$$

respect the binary operations of respective group $e^{a+b} = e^a \cdot e^b$.

One particular examples of great application in number theory is following.

Example 3.2. Let $(G, *)$ be any group. Let g_0 be a fixed element of G . Then map $\mathbb{Z} \rightarrow (G, *)$ defined as $n \mapsto g_0^n$ is a nice candidate for homomorphism.

In fact note that $n = 1 + 1 + \dots + 1$, so, image of $\mathbb{Z}$, under this map, is entirely generated by powers of g . Group generated by integral powers of an element $g \in G$ will be called as **cyclic group** and g will be called as generator of cyclic group $\{g^n | n \in \mathbb{Z}\}$.

Theorem 3.3 (Identity goes to identity). *Let $\varphi : (G, *) \rightarrow (H, \Delta)$ be a group homomorphism then $\varphi(e_G) = (e_H)$, where e_H is identity element of H .*

Remark 3.1. *In Theorem 3.3, Δ stands the corresponding binary operation under which H is a group.*

Proof. Note that $e_G * e_G = e_G$ and $\varphi : (G, *) \rightarrow (H, \Delta)$ is fundamentally a set theoretical map. Let $\varphi(e_G) = h$ then $h = \varphi(e_G) = \varphi(e_G * e_G) = \varphi(e_G) \Delta \varphi(e_G) = h \Delta h$. Now, cancellation law gives $h = e_H$. $\square$

Theorem 3.4 (Image of inverse element is inverse of image). *Let $\varphi : (G, *) \rightarrow (H, \Delta)$ be a group homomorphism then $\varphi(g^{-1}) = \varphi(g)^{-1}$.*

Proof. We know that $g * g^{-1} = e_G$. This also means that $\varphi(e_G) = e_H = \varphi(g * g^{-1}) = \varphi(g) \Delta \varphi(g^{-1})$. Multiply on left, by $\varphi(g)^{-1}$, to equation $e_H = \varphi(g) \Delta \varphi(g^{-1})$ and use associativity of binary operation Δ . This yields $\varphi(g)^{-1} \Delta e_H = (\varphi(g)^{-1} \Delta \varphi(g)) \Delta \varphi(g^{-1})$. Hence, $\varphi(g^{-1}) = \varphi(g)^{-1}$. $\square$

Theorem 3.5 (Order and Homomorphism). *Let $\varphi : (G, *) \rightarrow (H, \Delta)$ be a group homomorphism. Let $|g| = n$. Then $|\varphi(g)|$ divides n .*

Proof. By Definition 3.5, $\varphi(g^n) = \underbrace{\varphi(g) \cdots \varphi(g)}_{n \text{ - times}}$. Also, $g^n = e_G$ and φ is a set theoretical function and group homomorphism as well, therefore, $\varphi(g^n) = \varphi(e_G) = e_H$. This yields $\varphi(g^n) = \underbrace{\varphi(g) \cdots \varphi(g)}_{n \text{ - times}} = e_H$. Hence, by Theorem, 3.2, $|\varphi(g)|$ divides n . From this we conclude that $|\varphi(g)| \leq n$. The question is when does the equality $|\varphi(g)| = |g| = n$ holds ?. Theorem 3.6 precisely addresses this question. $\square$

Definition 3.6 (Isomorphism of Groups). *Let $\varphi : (G, *) \rightarrow (H, \Delta)$ be a group homomorphism. We say, φ is an isomorphism of groups if and only if $\varphi^{-1} : (H, \Delta) \rightarrow (G, *)$ is also a group homomorphism. That is, φ^{-1} is a set theoretical bijection as well as group homomorphism from H to G .*

Theorem 3.6 (Isomorphism preserves the structure). *Let $\varphi : (G, *) \rightarrow (H, \Delta)$ be a group isomorphism. Then followings are true*

- $|g| = |\varphi(g)|$ for all $g \in G$.
- G is Abelian² or commutative if and only if H is so.

Proof. From theorem 3.5 we already know that $|\varphi(g)| \leq |g|$. We know that φ^{-1} is a homomorphism so, repeating the application of Theorem 3.5, $|\varphi^{-1}(\varphi(g))| = |g| \leq |\varphi(g)|$. Thus, $|\varphi(g)| = |g|$. $\square$

Theorem 3.7 (Distinct elements of cyclic group). *Let G be a group generated by single element a of order n . That is, $G = \{g^i | 1 \leq i \leq n\}$. We claim that $g^j \neq g^k$ whenever $1 \leq j \neq k \leq n$. That is, $g^1, g^2, g^3, \dots, g^n$ are all different.*

²In honor of pioneering Mathematician Neils Henrik Abel, who proved that it is impossible to solve the general quintic equation in radicals. In his honor, Mathematician Sophius Lie proposed to institute Abel Prize, the closest equivalent of Nobel Prize

Proof. Anticipating a contradiction, let us assume that $j \neq k$ and $g^j = g^k$. Without loss of generality let us assume that $j < k$ and we multiply on both side of $g^j = g^k$ with g^{-j} . This gives, $g^{-j} * g^j = g^0 = e_G = g^{-j} * g^k = g^{k-j}$. That is, $1 \leq j < k \leq n$ and $g^{k-j} = e_G$. This means, by Theorem 3.2, n divides $k - j$ which is impossible. Hence, $g^1, g^2, g^3, \dots, g^n$ are all distinct powers of g . $\square$

Definition 3.7 (Generators of a cyclic group). Let G_n be cyclic group of order n . We say an element $g \in G_n$ generates G_n if every elements of G_n is some power of g . That is, if $a \in G$, then $g^j = a$ for some $0 \leq j \leq n$

Theorem 3.8 (Multiple generators of a cyclic group). Let G_n be a cyclic group of order n generated by an element $g_0 \in G$. We say g_0^m generates G_n if and only if $\gcd(m, n) = 1$.

Proof. Let us assume that $\gcd(m, n) = 1$. We know that there exist integers a, b such that $am + bn = 1$. We have to prove that every element of G_n is some powers of g_0^m . Let $g \in G$. Since G_n is generated by g_0 so $g = g_0^i$ for some $1 \leq i \leq n$. So, i is a fixed (given) value for us. We need to find $1 \leq k \leq n$ such that $g_0^{m(k)} = g_0^i$. Since $am + bn = 1$, so, $g_0^{am+bn} = g_0^1$. This gives $g_0^{am} g_0^{bn} = g_0^{bm} = g_0$. Raising the index i on both side of last equation we get $g_0^{bmi} = g_0^i = g$. We set $k := ib$. Note that i, b are both known as fixed value for us.

Now, we need to prove the other side of the implication : Assume that g_0^m generates G_n . Then prove that $\gcd(m, n) = 1$. It is enough to prove that $g_0^m, g_0^{2m}, g_0^{3m}, g_0^{4m}, \dots, g_0^{nm}$ are all distinct. This will prove that nm is the order of g_0^m . Let us assume that d is the order of g_0^m . That is, d is the smallest positive integer such that $g_0^{md} = e_G$. This means, by Theorem 3.2, that n divides md . Which means that md is the smallest multiple of m and is also a multiple of n . So, $md = \text{lcm}(m, n)$. Now, we can use the result that $\frac{\text{lcm}(x, y)}{x} = \frac{y}{\gcd(x, y)}$. That is $\text{lcm}(x, y) \gcd(x, y) = xy \iff \gcd(x, y) = \frac{xy}{\text{lcm}(x, y)}$. $md = \text{lcm}(m, n)$. This gives $\gcd(m, n) = \frac{mn}{\text{lcm}(m, n)}$ and we already have proven that $md = \text{lcm}(m, n)$, hence, $\gcd(m, n) = \frac{mn}{\text{lcm}(m, n)} = 1$. That is m, n are coprime. $\square$

Example 3.3 (Modular arithmetic, equivalence relation, cyclic group). Let us fix a positive integer n and consider the equivalence classes of equivalence relation, defined on $\mathbb{Z}$, $a \sim b$ if and only if n divides $a - b$. This relation is also denoted as $a \equiv b \pmod{n}$. The collection $\mathbb{Z}/n\mathbb{Z} = \{[0]_n, [1]_n, [2]_n, [3]_n, \dots, [n-1]_n\}$ of equivalence class of the modular relation forms a group structure with following definition of addition of equivalence classes $[a]_n + [b]_n := [a + b]_n$. One can prove that this is indeed a binary operation on $\mathbb{Z}/n\mathbb{Z}$. This operation is well defined because of an easy consequence of the fact that $a \sim a' \iff [a]_n = [a']_n$. Also, $[0]_n$ is additive identity of this binary operation. It is easy to verify $-[a]_n = [-a]_n$. So, $\mathbb{Z}/n\mathbb{Z}$ indeed has a group structure. This group is also cyclic. To see it, note that $[a]_n = [1 + \dots + 1]_n = a[1]_n$. So, $[1]_n$ is at least one generator of $\mathbb{Z}/n\mathbb{Z}$. The order of $[1]_n$ is n , this is an immediate consequence of 3.4.

Example 3.4 (Multiplicative group induced by modulo relation). Let p be a fixed prime. Then, collection of non-zero equivalence classes, as defined in example

3.3. $(\mathbb{Z}/p\mathbb{Z})^\times = \{[1]_p, [2]_p, [3]_p, \dots, [p-1]_p\}$ forms a group under multiplication of equivalence classes defined as $[a]_n \cdot [b]_n := [ab]_n$. Furthermore, this group is cyclic. $(\mathbb{Z}/p\mathbb{Z})^\times$ is an example of what is called as quotient group.

Lemma 3.1. *Let G be a finite Abelian group with exactly one element f of order 2. Prove that*

$$\prod_{g \in G} g = f$$

Proof. Let $|G| = n$. First note that every element of order 2 is its own inverse in G . To see this, we can directly work with given information that f is an element of G with $|f| = 2$, that is, $f * f = e_G$. To this equation, multiply on left by f^{-1} . This gives $(f^{-1} * f) * f = e_G * f = f = f^{-1} * e_G = f^{-1}$. Now let $g_1 = e_G, g_2, g_3, \dots, g_{n-1}, g_n = f$ be total n distinct elements of G . It is given that f is the only element of order 2. Therefore, for every other element, there exist inverse in G , however, different from element itself. These elements are precisely $g_2, \dots, g_{n-1}$. So, we have $\frac{n-2}{2}$ pairs of the form $g_i * g_i^{-1} = 1$ in $\prod_{g_i \in G} g_i$. That is, elements in the product $\prod_{g_i \in G} g_i$ can be rearranged so that an element and its inverse are put together. This is possible due to previous assertion and that G is Abelian. So,

$$\prod_{g_i \in G} g_i = \prod_{g_i \in G} (g_i * g_i^{-1}) * f = \prod e_G * f = f$$

, where $2 \leq i \leq n-1$. □

Now, it is time to state the first application of theory developed so far to prove an elementary but a significant theorem of number theory in language of group theory. An immediate consequence of example 3.3, example 3.4 and Lemma 3.1 is the following simple yet powerful theorem of elementary number theory

Theorem 3.9 (Wilson's Theorem). *An integer $p > 1$ is a prime if and only if $(p-1)! \equiv -1 \pmod{p}$*

Proof. Let us denote $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}_p^\times$. The order of cyclic group $\mathbb{Z}_p^\times = \{[1]_p, \dots, [p-1]_p\}$ is $p-1$. Note that, we say $[m]_n \in \mathbb{Z}_p^\times$ has order k if and only if $m^k \equiv 1 \pmod{p}$. Let us figure out which element of $\mathbb{Z}_p^\times$ has order 2. The general element of $\mathbb{Z}_p^\times$ can be written as $[p-i]_p$, where $1 \leq i \leq p-1$. Element $[p-j]_p$ has order 2 if and only if $(p-j)^2 \equiv 1 \pmod{p}$ and this precisely is equivalent to say $j^2 \equiv 1 \pmod{p}$. This is possible if and only if $j = 1$. Therefore, there is exactly one element of order 2 in multiplicative group $\mathbb{Z}_p^\times$. And that element is $[p-1]_p$. Now by Lemma 3.1, we know that

$$\prod_{1 \leq i \leq p-1} [p-i]_p = \prod_{2 \leq i \leq p-1} ([p-i]_p * [p-i]_p^{-1}) * [p-1]_p = [p-1]_p.$$

Also, $\prod_{1 \leq i \leq p-1} [p-i]_p = [(p-1)!]_p$. Hence, $[(p-1)!]_p = [p-1]_p \iff (p-1)! \sim p-1 \iff (p-1)! \equiv p-1 \pmod{p}$ and last equation is equivalent to $(p-1)! \equiv -1 \pmod{p}$. This closes the proof. □

Definition 3.8 (Kernel). Let $\varphi : (G, *) \rightarrow (H, \Delta)$ be a group homomorphism in sense of Definition 3.5. The collection $N = \{g \in G \mid \varphi(g) = e_H\}$ is non - empty (why?). Obviously, by Theorem 3.3, $\varphi(e_G) = e_H$, so $e_G \in N$.

Theorem 3.10 (Kernel of an homomorphsim is a subgroup). Let $\varphi : (G, *) \rightarrow (H, \Delta)$ be a group homomorphism. Then $N = \ker(\varphi)$, with respect to φ , is a subgroup of G .

Proof. Let us denote kernel of an homomorphism φ as $\ker(\varphi) = N$. So, $\ker(\varphi) = N = \{g \in G \mid \varphi(g) = e_H\} = \varphi^{-1}(e_H)$. That is kernel of an homomorphism is set of all element of G whose image under φ is e_H . Suppose $g_1, g_2 \in \ker(\varphi)$. That is, $\varphi(g_1) = \varphi(g_2) = e_H$. By application of Theorem 3.1, it is enough to prove that $g_1 * (g_2)^{-1} \in \ker(\varphi)$. Now, $\varphi(g_1 * (g_2)^{-1}) = \varphi(g_1)\Delta\varphi(g_2)^{-1}$ which means $e_H\Delta e_H^{-1} = e_H$. Thus, $\ker(\varphi) \leq G$. $\square$

Definition 3.9 (Normal Subgroup). Let $(G, *)$ be a group. Let $N \leq G$. Then we say N is normal subgroup of G , and write as $N \trianglelefteq G$, if and only if $g * n * g^{-1} \in N$ for all $g \in G, n \in N$.

Note that if the group operation $*$ is commutative on G , then every subgroup of G would be normal subgroup of G . For example, every subgroup of any cyclic group is always a normal subgroup of given cyclic group. A particular interesting case is **every subgroup of group of complex roots of unity is its normal subgroup**.

Theorem 3.11 (Kernel of every group Homomorphism is a normal subgroup). Let $\varphi : (G, *) \rightarrow (H, \Delta)$ be a group homomorphism. Then Kernel N , with respect to φ , is a subgroup of G

Proof. Let $n \in N$ and let $g \in G$. We have to show that $g * n * g^{-1} \in N$ That is $\varphi(g * n * g^{-1}) = e_H$. Note that $\varphi(n) = e_H$. This makes $\varphi(g * n * g^{-1}) = \varphi(g)\Delta\varphi(n)\Delta\varphi(g^{-1}) = \varphi(g)\Delta e_H\Delta\varphi(g)^{-1} = e_H$. This closes the proof. $\square$

So, we proved that kernel of every group homomorphsim, of G into any other group, is a normal subgroup of G . In fact, given any normal subgroup, H of G , one can construct an homomorphism of G such that H is precisely the kernel of newly constructed group homomorphsim.

4. QUOTIENT GROUP AND THEOREMS OF LAGRANGE, FERMAT , EULER ON FINITE GROUPS

Now, we will discuss concepts of orbits and Lagrange's theorem. Using Lagrange's theorem 4.1, we will prove Fermat's little theorem 4.2. We will generalize Fermat's little theorem, also known as Euler's Theorem.

Definition 4.1 (Group action). Let G be a group. Let X be a set. A group action of G on set X is any map of $G \times X$ into X which satisfies following axioms

- for all $g_1, g_2 \in G$ and for all $x \in X$, $g_1 \cdot (g_2 \cdot x) = (g_1 * g_2) \cdot x$.
- $e_H \cdot x = x$ for all $x \in X$.

Note that $g_2 \cdot x$ is an element of X , so it indeed makes sense to act on it by g_1 . Also, $g_1 * g_2$ is product inside the group G . And dot $\cdot$ is not a binary operation.

Lemma 4.1 (Concept of orbit). *Let H be a group acting on set X . Define a relation $\sim$ on X as : $x \sim x'$ if and only if $x = hx'$ for some $h \in H$. Then this relation is an equivalence relation on X .*

The equivalence class $[x]_\sim$ of this relation are called as **orbit** of x under the action of H . From Theorems 1.1, 1.2 we know that these equivalence classes will partition X .

Proof. We use Definition 4.1 to prove that $\sim$ is indeed reflexive, symmetric and transitive relation on X .

- Since for each $x \in X$, $e_H \cdot x = x$, action on this equation by inverse of e_H , which means by e_H itself, implies that relation $\sim$ is reflexive on X .
- Let $x \sim x'$. This means $x = hx'$ for some $h \in H$. Since H is a group, so, $h^{-1} \in H$. By first axiom of group action, action by h^{-1} on both side of $x = hx'$ gives $h^{-1}x = (h^{-1} * h) \cdot x' = e_H \cdot x' = x'$. Hence, $x' \sim x$. Hence $\sim$ is a symmetric relation on X .
- The transitivity is obvious by axioms of group action and set theoretical axiom of substitution.

□

Lemma 4.2 (Precursor to Lagrange's Theorem). *Let $H \leq G$ of a finite group G . Let H acts on G by left multiplication. Here set $X = G$. Let $x \in G$. Let $\mathcal{O} = [x]_\sim$ be the orbit of x , in sense of Lemma 4.1, under the action of H on G . Then the map $H \rightarrow \mathcal{O}$ defined by $h \mapsto hx$ is a bijection. Thus, $|H| = |\mathcal{O}|$.*

Proof. We prove this theorem by using definition of injection and surjection given in Section 2.

- **Injective.** Let $h_1x = h_2x$. Since, $x \in \mathcal{O} \subset G$, so, we can do right multiplication to previous relation on by x^{-1} . Then, by associativity of binary operation on G we get $h_1(x * x^{-1}) = h_2(x * x^{-1})$. This gives, $h_1 = h_2$.
- **Surjective.** Let $x_0 \in \mathcal{O}$. We have to find an element $h_0 \in H$ such that $h_0 \mapsto x_0$. Since, $x_0 \in \mathcal{O} = [x]_\sim$ so, $x_0 \sim x$. Therefore, by definition of $\sim$ on $X = G$, as defined in Lemma 4.1, there exist at least one element $h' \in H$ such that $x_0 = h'x$. Set $h_0 = h'$. This closes the proof.

This proves that $|H| = |\mathcal{O}|$. Therefore, for finite group we have the first combinatorial results of group theory - Lagrange's Theorem as stated below- □

Theorem 4.1 (Lagrange's theorem for finite group). *If H is a subgroup of finite group G , then order of H divides the order of G .*

Proof. Equivalence classes do the partition of G . Lemma 4.2, proves that each equivalence class $\mathcal{O}$ has same size as $|H|$. Now, let G be a finite group. Let k is number of equivalence classes of equivalence relation $\sim$ as defined in Lemma 4.1 and induced by action of H on G . Then $|G| = k|H|$. Thus, $k = \frac{|G|}{|H|}$ is a finite positive integer. That is, order of the subgroup divides the order of the group.

Is converse³ of Lagrange's theorem true? □

³No. However, historically, Lagrange and Cauchy often appear together in mathematics. So, we expect Cauchy to appear here and indeed, he appears. Cauchy Said, that not every divisor of order of

Corollary 4.1 (Order of element is divisor of order of group). *Let G be a finite group with $|G| = n$. Let $g \in G$. Let $|g| = m$. Then m divides n .*

Proof. Let $H = \{g^i | 1 \leq i \leq m\}$ be the cyclic group generated by g . Obviously, $H \leq G$. Hence, by Lagrange's Theorem 4.1, m divides n . As a consequence of this result, let us make a concluding remark that in a finite group G , $g^{|G|} = e_G$ for all $g \in G$. $\square$

Theorem 4.2 (Fermat's little theorem - FLT). *Let p be a prime integer and let a be any integer. Then $a^p \equiv a \pmod{p}$.*

Proof. If a is multiple of p , then claim of the theorem is obviously true. So, let us assume that a is not a multiple of p . In this case, we work with finite multiplicative group introduced in example 3.4. $(\mathbb{Z}/p\mathbb{Z})^\times$ is a group of order $p - 1$. Consider the equivalence class $[a]_p \in (\mathbb{Z}/p\mathbb{Z})^\times$. So, by last concluding remark of Corollary 4.1, we know that $[a]_p^{p-1} = [1]_p$. Hence, by multiplication of equivalence classes we get $[a]_p^p = [a]_p \rightarrow a^p \equiv a \pmod{p}$. This closes the proof. $\square$

Definition 4.2 (Automorphism of a group). *An isomorphism $f : G \rightarrow G$ is called as automorphism of the group G . Collection $\text{Aut}(G)$ is collection of all automorphism of group G . Under composition of function as binary operation, $\text{Aut}(G)$ form of a group.*

Proposition 4.1. *Let G be a group. Prove that function $g \mapsto g^{-1}$ is a homomorphism if and only if G is abelian.*

Proof. Assume that G is abelian. Since, $(ab)^{-1} = b^{-1}a^{-1}$ and that G is abelian so $(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$. This implies that map $g \mapsto g^{-1}$ is indeed an homomorphism. Now assume that $g \mapsto g^{-1}$ is an homomorphism. let $a, b \in G$. We need to show that $ab = ba$. We know that $ab = ba \iff a^{-1}b^{-1}ab = 1$. let us name $g \mapsto g^{-1}$ to be f . Then $f(ab) = (ab)^{-1} = b^{-1}a^{-1} = f(a)f(b) = a^{-1}b^{-1}$. That is $(ab)^{-1} = b^{-1}a^{-1} = a^{-1}b^{-1}$. Act first by right multiplication by a and then by b in last identity, we get $1 = a^{-1}b^{-1}ab$. Which proves that G is abelian group. $\square$

Theorem 4.3 (Automorphism of cyclic group). *Order of the group of automorphisms of a finite cyclic group, C_n , of order n is number of positive integers which are co-prime with n .*

Proof. From Theorem 3.8, total number of generators of any cyclic group, of order n , is $\varphi(n)$, the Euler's φ function. Therefore, in particular, know that order of $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times$ is $\varphi(n)$. In order to prove claim of Theorem 4.3, it is enough to show that $\text{Aut}(G) \cong \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times$. Let x be generator of cyclic group, say C_n , of order n . Let $f \in \text{Aut}(C_n)$, then, $f(x) = x^i$ for some $i \in \mathbb{Z}$ because every homomorphism of C_n into itself will have only this possibility. Moreover, i , when taken $\pmod{n}$, will uniquely determine definition

finite group G corresponds to a subgroup of G , however, if p is a prime number dividing the order of G , then G contains an element, say g_0 , of order p . Hence, G would contain the cyclic group, of order p , generated by this element g_0 .

of f . Let us denote this automorphism $f(x) = x^i$ as f_i , where i will be taken modulo n . Since, x is generator of C_n , therefore, order of x is n . By Theorem 3.7, Definition 3.7, for each j which is co-prime with n , map $x \mapsto x^j$ is an automorphism of C_n , Theorem 3.8. That is, given any element of $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times$, we have corresponding pre-image in $\text{Aut}(C_n)$. So, This map $\phi : \text{Aut}(C_n) \rightarrow \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times$ defined by $f_i \mapsto i \pmod n$ is indeed a surjection. It is obvious that ϕ is an injection by its definition. To see if this map is a group homomorphism - let $f_i, f_j \in \text{Aut}(C_n)$. $\phi(f_i \circ f_j)(x) = \phi(f_i(x^j)) = \phi(x^{ji}) = \phi(f_{ji}(x))$. So, $\phi(f_i \circ f_j) = \phi(f_{ji}) = ji \pmod n = \phi(f_i)\phi(f_j)$. Hence, ϕ is indeed a group homomorphism. Conclusively, $\text{Aut}(G) \cong \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^\times$ $\square$

Remark 4.1. *Note that one can not conclude from Fermat's little theorem that $a^n \equiv a \pmod n$ is true for all a, n . However, a certain version of this conjecture is true - This version is called as Euler's theorem of finite group. As this work expands, I will discuss, in greater details, the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$ and Euler's totient function. I will use last two results and Lagrange's theorem to prove the Euler's theorems of finite group.*

5. FUTURE WORK

Due to crisis of time I am not able to spare much time to write documentation of my understanding of abstract algebra that I studied in past one year. However, I plan to write more and expand this document regularly, though slowly, with following two objectives

- To write my understanding of standard theorems of quotient groups, group action, ring of polynomial over fields, field extension and cyclotomic polynomials. Study of integers and cyclotomic polynomials have been very fascinating subject for me especially for its strong usage in algebra problems of various mathematical Olympiads that I wrote and qualified.
- To write solutions to some mathematical competitions' problems from number theory, complex numbers where we generally used concepts of elementary abstract algebra. I also plan to type solutions to some select exercises of abstract algebra which I have solved while I was learning this course.

6. ACKNOWLEDGEMENT

I am thankful to my mentor **Yaashaa Golovanov** for teaching me, this early, an introductory course on abstract algebra. This learning and understanding of abstract algebra gave me lot of happiness and opened the path of new opportunities for me like currently I am doing a reading project in number theory.