# Groups, Subgroups and Isomorphisms 

Luqman Mahmood Yaseen<br>University of Duhok college of education Akre mathematics department, luqmanzebari20@gmail.com

Zebari
University of Duhok college of education Akre mathematics department


#### Abstract

We have now looked rather extensively at rings and fields and in this subject we consider the basic concepts of group theory. Groups arise in many different areas of mathematics. For example they arise in geometry as groups of congruence motions and in topology as groups of various types of continuous functions. Later in this subject they will appear in Galois Theory as groups of automorphisms of Fields.


## INTRODUCTION

2. Definition : A group G is a set with one binary operation which we will denote by multiplication, such that
(1) The operation is associative, that is, $\left(g_{1} g_{2}\right) g_{3}=g_{1}\left(g_{2} g_{3}\right) \quad$ for $\quad$ all $\boldsymbol{g}_{1}, \boldsymbol{g}_{2}, \boldsymbol{g}_{3} \in \boldsymbol{G}$.
(2) There exists an identity for this operation, that is, an element 1 such that $\mathbf{1} \boldsymbol{g}=\boldsymbol{g}$ and $\boldsymbol{g} \mathbf{1}=\boldsymbol{g}$ for each $\boldsymbol{g} \in \boldsymbol{G}$.
(3) Each $\boldsymbol{g} \in \boldsymbol{G}$ has an inverse for this operation, that is, for each $\boldsymbol{g}$ there exists a $\boldsymbol{g}^{\mathbf{- 1}}$ with the property that $\boldsymbol{g} \boldsymbol{g}^{\mathbf{1}}=\mathbf{1}$ an $\boldsymbol{g}^{\mathbf{- 1}} \boldsymbol{g}=$ 1.

If in addition the operation is commutative, that is $\boldsymbol{g}_{\boldsymbol{1}} \boldsymbol{g}_{\mathbf{2}}=\boldsymbol{g}_{\mathbf{2}} \boldsymbol{g}_{\boldsymbol{1}}$ for all $\boldsymbol{g}_{\mathbf{1}} \boldsymbol{g}_{\mathbf{2}} \in \boldsymbol{G}$, the group $\boldsymbol{G}$ is called an abelian group.
The order of $\boldsymbol{G}$, denoted $|\boldsymbol{G}|$, is the number of elements in the group $\boldsymbol{G}$. If $|\boldsymbol{G}|<\infty, \boldsymbol{G}$ is a finite group otherwise it is an infinite group.
It follows easily from the definition that the identity is unique and that each element has a unique inverse.

## Lemma (1):

If $\boldsymbol{G}$ is a group then there is a unique identity.
Further if $\boldsymbol{g} \in \boldsymbol{G}$ its inverse is unique. Finally
if $\boldsymbol{g}_{\boldsymbol{1}} \boldsymbol{g}_{\mathbf{2}} \in \boldsymbol{G}$ then $\left(g_{1} g_{2}\right)^{-1}=g_{2}^{-1} g_{1}^{-1}$.

Proof. Suppose that $\mathbf{1}$ and $\boldsymbol{e}$ are both identities for $\boldsymbol{G}$. Then $\boldsymbol{1} \boldsymbol{e}=\boldsymbol{e}$ since $\boldsymbol{e}$ is an identity and $\mathbf{1} e=\mathbf{1}$ since $\mathbf{1}$ is an identity. Therefore $\mathbf{1}=\boldsymbol{e}$ and there is only one Identity.
Next suppose that $\boldsymbol{g} \in \boldsymbol{G}$ and $\boldsymbol{g}_{\mathbf{1}}$ and $\boldsymbol{g}_{\boldsymbol{2}}$ are inverses for $\boldsymbol{g}$. Then

$$
g_{1} g g_{2}=\left(g_{1} g\right) g_{2}=1 g_{2}=g_{2}
$$

since $\boldsymbol{g}_{\mathbf{1}} \boldsymbol{g}=\mathbf{1}$. On the other hand

$$
g_{1} g g_{2}=g_{1}\left(g g_{2}\right)=g_{1} 1=g_{1}
$$

since $\boldsymbol{g} \boldsymbol{g}_{\mathbf{2}}=\mathbf{1}$. It follows that $\boldsymbol{g}_{\boldsymbol{1}}=\boldsymbol{g}_{\mathbf{2}}$ and
$\boldsymbol{g}$ has a unique inverse.
Finally consider

$$
\begin{gathered}
\left(g_{1} g_{2}\right)\left(g_{2}^{-1} g_{1}^{-1}\right)=g_{1}\left(g_{2} g_{2}^{-1}\right) g_{1}^{-1}= \\
g_{1} 1 g_{1}^{-1}=g_{1} g_{1}^{-1}=1
\end{gathered}
$$

Therefore $\boldsymbol{g}_{\mathbf{2}}^{\mathbf{- 1}} \boldsymbol{g}_{\mathbf{1}}^{-\mathbf{1}}$ is an inverse for $\boldsymbol{g}_{1} \boldsymbol{g}_{\mathbf{2}}$ and since inverses are unique it is the inverse of the product.

Groups most often arise as permutations on a set. We will see this, as well as other Specific examples of groups, in the next sections.

Finite groups can be completely described by their group tables or multiplication tables. These are sometimes called Cayley tables. In general, let $\boldsymbol{G}=\left\{\boldsymbol{g}_{\mathbf{1}} \ldots . . \boldsymbol{g}_{\boldsymbol{n}}\right\}$ be a group, then the multiplication table of $\boldsymbol{G}$ is:

|  | $g_{1}$ | $g_{2}$ | $\cdots$ | $g_{j}$ | $\cdots$ | $g_{n}$ |
| :---: | :--- | :--- | :--- | :--- | :--- | :--- |
| $g_{1}$ | $\cdots$ |  |  |  |  |  |
| $g_{2}$ | $\cdots$ |  |  |  |  |  |
| $\vdots$ |  |  |  |  |  |  |
| $g_{i}$ | $\cdots$ | $\cdots$ | $\cdots$ | $g_{i} g_{j}$ |  |  |
| $\vdots$ |  |  |  |  |  |  |
| $g_{n}$ | $\cdots$ |  |  |  |  |  |

The entry in the row of $\boldsymbol{g}_{\boldsymbol{i}} \in \boldsymbol{G}$ and column of $\boldsymbol{g}_{\boldsymbol{j}} \in \boldsymbol{G}$ is the product (in that order) $\boldsymbol{g}_{\boldsymbol{i}} \boldsymbol{g}_{\boldsymbol{j}}$ in G.

Groups satisfy the cancellation law for multiplication.

## (t) Abelian_Group _or commutative

Group:
2. Definition :A Group $\{\boldsymbol{G}, *\}$ is said to be abelian or commutative if in addition to the above four postulate is also satisfied.

- commutativity $a o b=b o a \forall a, b \in$ G


## Notes:

1. In our definition of a group we have denoted the composition in $\boldsymbol{G}$ by multiplicative notation. However we can use any symbol like $*, \mathbf{0},+$ ect. to denote the composition. If we use the additive notation ' + ' to denote the composition in $\boldsymbol{G}$, then the inverse of an element $\boldsymbol{a} \in \boldsymbol{G}$ is denoted by the symbol - a i.e., we have $(-a)+a=e=$ $\boldsymbol{a}+(-\boldsymbol{a})$
2. A group is not simply a set but it is an algebraic structure i e., a set equipped with a binary composition provided the composition satisfies certain postulates. If a group consists of a non-empty set $\boldsymbol{G}$ and a binary composition in $\boldsymbol{G}$, then we shall often use the same symbol $\boldsymbol{G}$ to denote the group and the underlined set.
3. In additive notation the element $\boldsymbol{a}+$ $(-\boldsymbol{b}) \in \boldsymbol{G}$ is denoted by $\boldsymbol{a}-\boldsymbol{b}$.
in multiplicative notation the element $\boldsymbol{a} \boldsymbol{b}^{-\mathbf{1}} \in$ $\boldsymbol{G}$ is denoted by $\boldsymbol{a} / \boldsymbol{b}$.
4. If we use multiplicative notation to denote the composition in $\boldsymbol{G}$, then often we denote the identity by the symbol ' $\mathbf{I}$ ' thus $\mathbf{I}$ is an element of $\boldsymbol{G}$ such that $\boldsymbol{l} \boldsymbol{a}=\boldsymbol{a}=\boldsymbol{a l} \forall \boldsymbol{a} \in$ G .
Also in multiplicative notation we often denote the inverse of a by $1 / a$. Thus $1 / a$ is an element of $\boldsymbol{G}$ such that $\frac{\mathbf{1}}{\boldsymbol{a}} \boldsymbol{a}=\mathbf{1}=\boldsymbol{a} \frac{\mathbf{1}}{\boldsymbol{a}}$.
In additive notation, we often denote the identity by the symbol ' 0 '.
Thus, 0 is an element of $\boldsymbol{G}$ such that $\mathbf{0}+\boldsymbol{a}=$ $\boldsymbol{a}+\mathbf{0}$.
5. According to our definition of a binary operation if '.' is a binary operation on $\boldsymbol{G}$, then we must have $\boldsymbol{a} . \boldsymbol{b} \in \boldsymbol{G}, \forall \boldsymbol{a}, \boldsymbol{b} \in \boldsymbol{G}$. Therefore in our definition of a group there is no necessity of mentioning the closure axiom. It
is superfluous there. We have mentioned it there to simply lay emphasis upon the fact that while showing the group postulates in a problem the students should not forget to show the closure axiom.

## Lemma (2):

If $\boldsymbol{G}$ is a group and $\boldsymbol{g} \in \boldsymbol{G}$ then $\langle\boldsymbol{g}\rangle$ forms a subgroup of $\boldsymbol{G}$ called the cyclic subgroup generated by $\boldsymbol{g} \cdot\langle\boldsymbol{g}\rangle$ is abelian even if $\boldsymbol{G}$ is not.

## Proof.

If $\boldsymbol{g} \in \boldsymbol{G}$ then $\boldsymbol{g} \in\langle\boldsymbol{g}\rangle$ and hence $\langle\boldsymbol{g}\rangle$ is nonempty. Suppose then that $\boldsymbol{a}=\boldsymbol{g}^{\boldsymbol{n}}, \boldsymbol{b}=$ $\boldsymbol{g}^{\boldsymbol{m}}$ are elements of $\langle\boldsymbol{g}\rangle$. Then $\boldsymbol{a} \boldsymbol{b}=\boldsymbol{g}^{\boldsymbol{n}} \boldsymbol{g}^{\boldsymbol{m}}=$ $\boldsymbol{g}^{\boldsymbol{n}+\boldsymbol{m}} \in\langle\boldsymbol{g}\rangle$ so $\langle\boldsymbol{g}\rangle$ is closed under the group operation. Further $\boldsymbol{a}^{\mathbf{- 1}}=\left(\boldsymbol{g}^{\boldsymbol{n}}\right)^{\mathbf{- 1}}=\boldsymbol{g}^{-\boldsymbol{n}} \in$ $\langle\boldsymbol{g}\rangle$ so $\langle\boldsymbol{g}\rangle$ is closed under inverses. Therefore $\langle\boldsymbol{g}\rangle$ is a subgroup.
Finally $\quad a b=\boldsymbol{g}^{\boldsymbol{n}} \boldsymbol{g}^{\boldsymbol{m}}=\boldsymbol{g}^{\boldsymbol{n + m}}=\boldsymbol{g}^{\boldsymbol{m}+\boldsymbol{n}}=$ $\boldsymbol{g}^{\boldsymbol{m}} \boldsymbol{g}^{\boldsymbol{n}}=\boldsymbol{b} \boldsymbol{a}$ and hence $\langle\boldsymbol{g}\rangle$ is abelian.

## 2. Definition :

If $\boldsymbol{G}$ and $\boldsymbol{H}$ are groups then a mapping $\boldsymbol{f}: \boldsymbol{G} \rightarrow$ $\boldsymbol{H}$ is a (group) homomorphism if $\boldsymbol{f}\left(\boldsymbol{g}_{\boldsymbol{1}} \boldsymbol{g}_{2}\right)=$ $\boldsymbol{f}\left(\boldsymbol{g}_{\mathbf{1}}\right) \boldsymbol{f}\left(\boldsymbol{g}_{\boldsymbol{2}}\right)$ for any $\boldsymbol{g}_{\mathbf{1}} \boldsymbol{g}_{\mathbf{2}} \in \boldsymbol{G}$. If $\boldsymbol{f}$ is also a bisection then it is an isomorphism.
As with rings and fields we say that two groups $\boldsymbol{G}$ and $\boldsymbol{H}$ are isomorphic, denoted
by $\boldsymbol{G} \cong \boldsymbol{H}$, if there exists an isomorphism $\boldsymbol{F}$ : $\boldsymbol{G} \rightarrow \boldsymbol{H}$. This means that abstractly $\boldsymbol{G}$ and $\boldsymbol{H}$ have exactly the same algebraic structure.


## Example (1):

Show that the set of vectors defined as directed line segments does not form a group
(i) with respect to secular (dot) product (ii) with respect to vector (cross) product.

## Solution:

Let $\boldsymbol{V}$ denote the set of all vectors defined as directed line segments.

1. If $\boldsymbol{a}, \boldsymbol{b} \in \boldsymbol{V}$, then $\boldsymbol{a}, \boldsymbol{b}$ is a scalar quantity and so $\boldsymbol{a}, \boldsymbol{b} \notin \boldsymbol{V}$. Thus dot product of vectors is not a binary operation on the set $\boldsymbol{V}$ .Hence $\boldsymbol{V}$ cannot be a group with respect to dot product.
2. If $\boldsymbol{a}, \boldsymbol{b} \in \boldsymbol{V}$, then the cross product $\boldsymbol{a} \times \boldsymbol{b}$ is also a vector and so $\boldsymbol{a} \times \boldsymbol{b} \in \boldsymbol{V}$. thus, cross product of two vectors is a binary operation on the set $\boldsymbol{V}$. But the cross product of vectors is not an associative operation. If $\boldsymbol{a}, \boldsymbol{b}, \boldsymbol{c} \in \boldsymbol{V}$, then in general $\boldsymbol{a} \times(\boldsymbol{b} \times \boldsymbol{c}) \neq$ $(\boldsymbol{a} \times \boldsymbol{b}) \times \boldsymbol{c}$.
Hence $\boldsymbol{V}$ is not a group with respect to cross product.

## Example (2):

As already mentioned groups arise in many diverse areas of mathematics. In this section and the next we present specific examples of groups.

## Solution:

First of all any ring or field under addition forms an abelian group. Hence, for example $(\mathbb{Z},+),(\mathbb{Q},+),(\mathbb{R},+),(\mathbb{C},+) \quad$ where $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ are respectively the integers, the rational, the reels and the complex numbers, all are infinite abelian groups. If $\mathbb{Z}_{\boldsymbol{n}}$ is the modular ring $\mathbb{Z} / \boldsymbol{n} \mathbb{Z}$ then for any natural number $\mathrm{n},\left(\mathbb{Z}_{\boldsymbol{n}},+\right)$ forms a finite abelian
group. In abelian groups the group operation is often denoted by C and the identity element by 0 (zero).

In a field $\boldsymbol{F}$, the nonzero elements are all invertible and form a group under multiplication. This is called the multiplicative group of the field $\boldsymbol{F}$ and is usually denoted by $\boldsymbol{F} *$ since multiplication in a field is commutative the multiplicative group of a field is an abelian group. Hence $\mathbb{Q}^{*} \mathbb{R}^{*} \mathbb{C}^{*}$ are all infinite abelian groups while if p is a prime $\mathbb{Z}_{\boldsymbol{p}}^{*}$ forms a finite abelian group. Recall that if p is a prime then the modular ring $\mathbb{Z}_{\boldsymbol{p}}$ is a field.

Within $\mathbb{Q}^{*} \mathbb{R}^{*} \mathbb{C}^{*}$ there are certain multiplicative subgroups. Since the positive rationals $\mathbb{Q}_{+}$and the positive reals $\mathbb{R}_{+}$are closed under multiplication and inverse they form subgroups of $\mathbb{Q}^{*}$ and $\mathbb{R}^{*}$ respectively. In $\mathbb{C}$ if we consider the set of all complex numbers $\boldsymbol{Z}$ with $|\boldsymbol{Z}|=\mathbf{1}$ then these form a multiplicative subgroup. Further within this subgroup if we consider the set of $n$-the roots of unity $\boldsymbol{Z}\left(\right.$ that $\left.\boldsymbol{i} \boldsymbol{Z}^{\boldsymbol{n}}=\mathbf{1}\right)$ for a fixed $\mathbf{n}$ this forms a subgroup, this time of finite order.

The multiplicative group of a field is a special case of the unit group of a ring. If $\boldsymbol{R}$ is a ring with identity, recall that a unit is an element of $\boldsymbol{R}$ with a multiplicative inverse. Hence in $\mathbb{Z}$ the only units are $\pm \mathbf{1}$ while in any field every nonzero element is a unit.


1. Is $\left(\mathcal{S},{ }^{\circ}\right)$ a group if
(i) $\quad \boldsymbol{S}=\boldsymbol{Z}$ and ${ }^{\circ}$ is the usual multiplication of integers?
(ii) $\boldsymbol{S}=\boldsymbol{Q}$ and $^{\circ}$ is the usual multiplication in $\boldsymbol{Q}$ ?
(iii) $\boldsymbol{S}=\{\boldsymbol{q} \mid \boldsymbol{q} \in \boldsymbol{Q}$ and $\boldsymbol{q}>\boldsymbol{0}\}$ and $■$ is the usual multiplication of rational numbers?
(iv) $S=\{Z \mid z \in \mathcal{Z}$ and $z>\sqrt{2}\}$ and ${ }^{\circ}$ is the usual multiplication in $\boldsymbol{Z}$ ?
(v) $\boldsymbol{S}=\boldsymbol{\mathcal { R }}$ and ${ }^{\circ}$ is the usual addition of real numbers?
(vi) $\boldsymbol{S}=\boldsymbol{Z}^{\circ}$ is defined by $\boldsymbol{a}^{\circ} \boldsymbol{b}=\mathbf{0}$ for all

## a,b in Z?

solutions:
(i) The identity element is the integer 1 . ( $\boldsymbol{S}{ }^{\circ}$ ) is not a group because $\mathbf{5} \notin \boldsymbol{Z}$ but there is no integer $\boldsymbol{z}$ in $\boldsymbol{Z}$ such that $\boldsymbol{z}^{\circ} \mathbf{5}=\mathbf{5}^{\circ} \boldsymbol{z}=\mathbf{1}$.
(ii) Again the identity is the number 1 . There is no $\boldsymbol{q} \in \boldsymbol{Q}$ such that $\boldsymbol{q}^{\circ} \mathbf{0}=\mathbf{1}$. Hence $\left(\boldsymbol{S},{ }^{\circ}\right)$ is not a group.
(iii) $\quad(\boldsymbol{S}, \boldsymbol{\square})$ is a group. Clearly $\boldsymbol{\mathcal { S }} \neq \boldsymbol{\phi}$ and is a binary operation on $\boldsymbol{S}$. $q \boxminus 1=1 ■ q=q$ for all $\boldsymbol{q} \in \mathcal{S}$, is an identity. Multiplication of rational numbers is associative and every element in $\boldsymbol{\mathcal { S }}$ has an
inverse; for if $\boldsymbol{q} \in \mathcal{S}$, then $\frac{\mathbf{1}}{\boldsymbol{q}} \in \mathcal{S}$ and $\frac{\mathbf{1}}{\boldsymbol{q}} \llbracket \boldsymbol{q}=$ $1=q ■ \frac{1}{q}$.
(iv) $\quad \boldsymbol{S}=\boldsymbol{\phi}$ since $\sqrt{\mathbf{2}} \notin \boldsymbol{Z}$. Therefore $\left(\mathcal{S},{ }^{\circ}\right)$ is not a group.
(v) $\quad\left(\boldsymbol{S},{ }^{\circ}\right)$ is a group. $\boldsymbol{S} \neq \boldsymbol{\phi}$ and addition is an associative binary operation on $\boldsymbol{S} . \boldsymbol{r}+\mathbf{0}=$ $0+r=r$ and $r+(-r)=0=(-r)+r$ for all $\in \boldsymbol{S}$.
(vi) $\left(\boldsymbol{S},{ }^{\circ}\right)$ is not a group because there is no identity element in $\boldsymbol{S}$.
2. let $m$ be any fixed positive integer and let $\mathcal{S}=\{0,1,2, \ldots, m-1\}$. Define a binary operation in $\mathcal{S}$ by $\quad a^{\circ} \mathfrak{b}=a+b$ if $a+$ $\mathrm{b}<m$

$$
a^{\circ} b=r \quad \text { if } \quad a+b=m+
$$

$r, 0 \leq r<m$
Prove that $\left(\mathcal{S},{ }^{\circ}\right)$ is a group of order $m$. (Hard.)

## Solutions:

If $\boldsymbol{a}, \boldsymbol{b} \in \boldsymbol{\mathcal { S }}$, then $\boldsymbol{a}^{\circ} \mathbf{b}$ is uniquely defined and belongs to $\boldsymbol{S}$. $\boldsymbol{a}^{\circ} \mathbf{0}=\mathbf{0}^{\circ} \boldsymbol{a}=\boldsymbol{a}$ so 0 is an identity.Note that $\boldsymbol{a}^{\circ} \mathbf{b}=\boldsymbol{a}+\boldsymbol{b}-\boldsymbol{\delta} \boldsymbol{m}$ where $\boldsymbol{\delta}$ is 0 or 1 , for any $\boldsymbol{a}, \boldsymbol{b} \in \boldsymbol{\mathcal { S }}, \mathrm{So}^{\circ} \boldsymbol{c}=\boldsymbol{b}+\boldsymbol{c}-$ $\boldsymbol{\delta}_{\mathbf{1}} \boldsymbol{m}$ where $\boldsymbol{\delta}_{\mathbf{1}}$ is $\mathbf{0}$ or $\mathbf{1}$. Hence
$a^{\circ}\left(\mathbf{b}^{\circ} c\right)=a+\mathfrak{b}+\boldsymbol{c}-\boldsymbol{\eta}_{1} m \quad$ Where $\quad \boldsymbol{\eta}_{1}$ is $\mathbf{0}$ or $\mathbf{1}$ or $\mathbf{2}$.

Similarly

$$
\left(\boldsymbol{a}^{\circ} \mathbf{b}\right)^{\circ} c=a+\mathbf{b}+
$$

$\boldsymbol{c}-\boldsymbol{\eta}_{\mathbf{2}} \boldsymbol{m}$ Where $\boldsymbol{\eta}_{\mathbf{2}}$ is $\mathbf{0}$ or $\mathbf{1}$ or $\mathbf{2}$.

Now $\quad \mathbf{0} \leq \boldsymbol{a}^{\circ}\left(\boldsymbol{b}^{\circ} \boldsymbol{c}\right)<\boldsymbol{m} \quad$ and $0 \leq\left(\boldsymbol{a}^{\circ} \mathbf{b}\right)^{\circ} \boldsymbol{c}<\boldsymbol{m}$ Suppose $\boldsymbol{\eta}_{\boldsymbol{1}}>\boldsymbol{\eta}_{\mathbf{2}}$
$a^{\circ}\left(\mathbf{b}^{\circ} c\right)=a+b+c-\left(\eta_{2}+1\right) m=a+$ $\mathrm{b}+c-\eta_{2} m-m$
because $\boldsymbol{\eta}_{\boldsymbol{1}}$ is at least $\boldsymbol{\eta}_{\boldsymbol{2}}+\mathbf{1}$ But $\mathbf{0} \leq \boldsymbol{a}+$ $\mathbf{b}+\boldsymbol{c}-\boldsymbol{\eta}_{\mathbf{2}} \boldsymbol{m}<\boldsymbol{m}$ and the above equation implies that $\boldsymbol{a}^{\circ}\left(\mathbf{b}^{\circ} \boldsymbol{c}\right)<\mathbf{0}$; this contradicts $\mathbf{0} \leq \boldsymbol{a}^{\circ}\left(\boldsymbol{b}^{\circ} \boldsymbol{c}\right)$. Hence $\boldsymbol{\eta}_{\mathbf{1}} \leq \boldsymbol{\eta}_{\mathbf{2}} \quad \boldsymbol{\eta}_{\mathbf{2}}>\boldsymbol{\eta}_{\mathbf{1}}$ leads in a similar way to a contradiction. Thus $\boldsymbol{\eta}_{\boldsymbol{1}}=$ $\boldsymbol{\eta}_{2}$ and
$\boldsymbol{a}^{\circ}\left(\mathbf{b}^{\circ} \boldsymbol{c}\right)=\left(\boldsymbol{a}^{\circ} \mathbf{b}\right)^{\circ} \boldsymbol{c}$ If $\boldsymbol{a} \in \mathcal{S}$ then $\boldsymbol{m}-\boldsymbol{a} \in \mathcal{S}$ and
$a^{\circ}(m-a)=(m-a)^{\circ} a=0$ hence $m-a$ is an inverse to $\boldsymbol{a}$ Thus $\boldsymbol{S}$ is a group.

## $\Rightarrow$ 2-subgroups :

In this chapter, we'll continue to utilize our intuitive definition of a group. That is, a group $G$ is a set of actions that satisfies the following rules.

Rule 1. There is a predefined list of actions that never changes.

Rule 2. Every action is reversible.

Rule 3. Every action is deterministic.

Rule 4. Any sequence of consecutive actions is also an action.

In the previous chapter, we constructed lots of Clayey diagrams for various groups. To construct a Clayey diagram for a group G, we need to first identify a set of generators, say $S$. Recall that our choice of generators is
important as changing the generators can result in a deferent Clayey diagram.

In the Clayey diagram for $G$ using $S$, all the actions of $G$ are represented by the vertices of the graph. Each vertex corresponds to a unique action. This does not imply that there is a unique way to obtain a given action from the generators. Each of the generators determines an arrow type in the diagram. One way to distinguish the deferent arrow types is by using deferent colors. An arrow of a particular color always represents the same generator.

One of the vertices in the diagram is labeled by the do-nothing action, often denoted by e. Each of the other vertices are labeled by words that correspond to following arrows (forwards or backwards) from e to a given vertex. There may be many ways to do this as each sequence of arrows corresponds to a unique word. So, a vertex could be potentially labeled by many words. Also, one potentially confusing item is that we read our words from right to left. That is, the first arrow we follow out of e is the rightmost generator in the word.
2. Definition : Let ( $\boldsymbol{G}, \cdot$ ) be a group with binary operation. and let $\mathcal{H}$ be a non-empty subset of $\boldsymbol{G}$.

Then we say $\mathcal{H}$ is a subgroup of $\boldsymbol{G}$ if the operation. restricted to $\mathcal{H}$ is a binary operation in $\mathcal{H}$ which makes $\boldsymbol{H}$ into a group.

For example, if $\boldsymbol{G}$ is the group with $\boldsymbol{m}=\mathbf{4}$, then the subset $\mathcal{H}=\{\mathbf{0}, \mathbf{2}\}$ is a subgroup of $\boldsymbol{G}$. For when the operation ${ }^{\circ}$ in $\boldsymbol{G}$, as defined in the multiplication table
for $\boldsymbol{G}$, is restrict to $\mathcal{H}$, it is a binary operation in $\mathcal{H}$, i.e.
$\mathbf{0}^{\circ} \mathbf{0}=\mathbf{0} \in \mathcal{H}, \quad \mathbf{0}^{\circ} \mathbf{2}=\mathbf{0} \in \mathcal{H}, \mathbf{2}^{\circ} \mathbf{0}=\mathbf{0} \in \mathcal{H}$ and $\mathbf{2}^{\circ} \mathbf{2}=\mathbf{0} \in \mathcal{H}$.
$\mathcal{H}$ is a group because: $\mathcal{H} \neq \emptyset ; \mathbf{0}$, the identity, is in $\mathcal{H}$; the operation $\mathbf{0}$ restricted to $\mathcal{H}$ is an associative binary operation (since the operation in $\boldsymbol{G}$ is associative); and every element in $\mathcal{H}$ has an inverse in $\mathcal{H}$.

奉 Lemma:
Let $(\boldsymbol{G}, \cdot)$ be a group. Then a subset $\mathcal{H}$ of G is a subgroup of $\boldsymbol{G}$ iff
(i) $\boldsymbol{\mathcal { H }} \neq \varnothing \quad$ and $\quad$ (ii) if $\boldsymbol{a}, \boldsymbol{b} \in$
$\mathcal{H}, \quad$ then $\quad \boldsymbol{a b}^{\mathbf{- 1}} \in \mathcal{H}$

## Proof.

If $\mathcal{H}$ satisfies these conditions, then $\mathcal{H}$ is a group with respect to the binary operation. For if $\mathcal{H} \neq \emptyset$, then there exists $\boldsymbol{a} \in \mathcal{H}$. Hence $a a^{-1}=\mathbf{1} \in \mathcal{H}$. Also, if $\mathbf{b} \in \mathcal{H}$ then $\mathbf{1 b}^{\mathbf{- 1}}=$ $\mathbf{b}^{-1} \in \mathcal{H}$. Hence $\boldsymbol{a}, \mathbf{b} \in \mathcal{H}$ implies $\boldsymbol{a}\left(\mathbf{b}^{-\mathbf{1}}\right)^{-\mathbf{1}}=\boldsymbol{a b} \in \mathcal{H}$. Associativity is true in $\mathcal{H}$, as it is true in $\boldsymbol{G}$. Thus' is an associative binary operation on $\mathcal{H}, \mathbf{1} \in \mathcal{H}$ and the inverse of every element of $\mathcal{H}$ is an element of $\mathcal{H}$. Therefore $(\mathcal{H}, \cdot)$ is a subgroup.
2. Definition : Let $\boldsymbol{G}$ be an arbitrary group. A subgroup $\mathcal{H}$ is a normal subgroup of $\boldsymbol{G}$, which we denote by $\mathcal{H} \triangleleft \boldsymbol{G}$, if


Since the conjugation map is an isomorphism it follows that if $\boldsymbol{g}^{\mathbf{- 1} \boldsymbol{H}} \boldsymbol{g} \subset \mathcal{H}$ then $\boldsymbol{g}^{\mathbf{1} \boldsymbol{H}} \boldsymbol{g}=\mathcal{H}$. Hence in order to show that a
subgroup is normal we need only show inclusion.

## Lemma:

Every subgroup of an abelian group is normal.

## Proof.

Let $\boldsymbol{G}$ be abelian and $\mathcal{H}$ a subgroup of $\boldsymbol{G}$.
Suppose $\boldsymbol{g} \in \boldsymbol{G}$ then $\mathbf{g} \boldsymbol{h}=\boldsymbol{k} \boldsymbol{g}$ for
all $\boldsymbol{h} \in \mathcal{H}$ since $\boldsymbol{G}$ is abelian. It follows that
$\mathbf{g} \mathcal{H}=\mathcal{H} \boldsymbol{g}$. Since this is true for every
$\boldsymbol{g} \in \boldsymbol{G}$ it follows that $\mathcal{H}$ is normal.

## 2

efinition : Let $\boldsymbol{G}$ be an arbitrary group and $\boldsymbol{\mathcal { H }}$ a normal subgroup of $\boldsymbol{G}$. Let $\boldsymbol{G} / \mathcal{H}$ denote the set of distinct left (and hence also right) cossets of $\mathcal{H}$ in $\boldsymbol{G}$. On $\boldsymbol{G} / \mathcal{H}$ define the multiplication

$$
\left(\mathbf{g}_{1} \mathcal{H}\right)\left(\mathbf{g}_{2} \mathcal{H}\right)=\mathbf{g}_{1} \mathbf{g}_{2} \mathcal{H}
$$

for any elements $\mathbf{g}_{1} \mathcal{H}, \mathbf{g}_{2} \mathcal{H}$ in $\boldsymbol{G} / \mathcal{H}$.

Theorem: Let $\boldsymbol{G}$ be a group and $\mathcal{H}$ a normal subgroup of $\boldsymbol{G}$. Then $\boldsymbol{G} / \mathcal{H}$
under the operation defined above forms a group. This group is called the factor group or quotient group of $\boldsymbol{G}$ modulo $\boldsymbol{\mathcal { H }}$. The identity element is the cosset $\boldsymbol{1 \mathcal { H }}=\mathcal{H}$ and the inverse of a cosset $\boldsymbol{g} \mathcal{H}$ is $\boldsymbol{g}^{\mathbf{- 1}} \boldsymbol{\mathcal { H }}$.

## Proof.

We first show that the operation on $\boldsymbol{G} / \boldsymbol{\mathcal { N }}$ is well-defined. Suppose that $\boldsymbol{a}^{\prime} \boldsymbol{\mathcal { N }}=\boldsymbol{a} \mathcal{N}$ and
$\mathfrak{b}^{\prime} \mathcal{N}=\mathfrak{b} \mathcal{N}$, then $\mathfrak{b}^{\prime} \in \mathfrak{b} \mathcal{N}$ and so $\mathfrak{b}^{\prime}=\mathbf{b} \mathfrak{n}_{\mathbf{1}}$. Similarly $\boldsymbol{a}^{\prime}=\boldsymbol{a n}_{\mathbf{2}}$ where $\boldsymbol{n}_{\mathbf{1}}, \mathfrak{n}_{\mathbf{2}} \in \mathcal{N}$.

Therefore

$$
a^{\prime} \mathbf{b}^{\prime} \mathcal{N}=\boldsymbol{a} \mathfrak{n}_{2} \mathfrak{b} \mathfrak{n}_{1} \mathcal{N}=\boldsymbol{a} \mathfrak{n}_{2} \mathbf{b} \mathcal{N}
$$

Since $\mathbf{n}_{\mathbf{1}} \in \mathcal{N}$. But $\mathfrak{b}^{\mathbf{- 1}} \mathbf{n}_{\mathbf{2}} \mathbf{b}=\mathbf{n}_{\mathbf{3}} \in \mathcal{N}$, since $\mathcal{N}$ is normal, so the right-hand side of The equation can be written as

$$
\boldsymbol{a n}_{2} \mathbf{b} \mathcal{N}=\boldsymbol{a} \mathbf{b} \mathcal{N}
$$

Thus we have shown that if $\boldsymbol{\mathcal { N }} \triangleleft \boldsymbol{G}$ then $\boldsymbol{a}^{\prime} \mathbf{b}^{\prime} \mathcal{N}=\boldsymbol{a} \mathbf{b} \mathcal{N}$, and the operation on $\boldsymbol{G} / \mathcal{N}$ is indeed, well-defined.
The associative law is $\mathbf{D}$ true because cosset multiplication as defined above uses the
Ordinary group operation which is by definition associative.

The cosset $\mathcal{N}$ serves as the identity element of $\boldsymbol{G} / \mathcal{N}$. Notice that

$$
a \mathcal{N} . \mathcal{N}=a \mathcal{N}^{2}=a \mathcal{N}
$$

and

$$
\mathcal{N} \cdot a \mathcal{N}=a \mathcal{N}^{2}=a \mathcal{N}
$$

The inverse of $\boldsymbol{a} \mathcal{N}$ is $\boldsymbol{a}^{\mathbf{- 1}} \mathcal{N}$ since

$$
a \mathcal{N} a^{-1} \mathcal{N}=a a^{-1} \mathcal{N}^{2}=\mathcal{N} .
$$

We emphasize that the elements of $\boldsymbol{G} / \mathcal{N}$ are cosets and thus subsets of $\boldsymbol{G}$. If $|\boldsymbol{G}|<\infty$ then $|\boldsymbol{G} / \mathcal{N}|=[\boldsymbol{G}: \mathcal{N}]$, the member of cossets of $\mathcal{N}$ in $\boldsymbol{G}$. It is also to be emphasized that in order for $\boldsymbol{G} / \mathcal{N}$ to be a group $\mathcal{N}$ must be a normal subgroup of $\boldsymbol{G}$.

In some cases properties of $\boldsymbol{G}$ are preserved in factor groups.

2 Definition : A group $\boldsymbol{G} \neq\{\mathbf{1}\}$ is simple provided that $\mathcal{N} \triangleleft \boldsymbol{G}$ implies $\boldsymbol{\mathcal { N }}=\boldsymbol{G}$ or $\boldsymbol{\mathcal { N }}=$ \{1\}.

One of the most outstanding problems in group theory has been to give a complete classification of all finite simple groups. In other words, this is the program to discover all finite simple groups and to prove that there are no more to be found. This was accomplished through the efforts of many mathematicians. The proof of this magnificent result took thousands of pages. We refer the reader to [18] for a complete discussion of this. We give one elementary example.

## Lemma:

Any finite group of prime order is simple and cyclic.

## Proof.

Suppose that $\boldsymbol{G}$ is a finite group and $|\boldsymbol{G}|=\mathcal{P}$ where $\mathcal{P}$ is a prime. Let $\boldsymbol{g} \in \boldsymbol{G}$ with $\boldsymbol{g} \neq \mathbf{1}$. Then $\langle\boldsymbol{g}\rangle$ is a nontrivial subgroup of $\boldsymbol{G}$ so its order divides the order of $\boldsymbol{G}$ by Lagrange's theorem. Since $\boldsymbol{g} \neq \mathbf{1}$ and $\mathcal{P}$ is a prime we must have $|\langle\boldsymbol{g}\rangle|=\mathcal{P}$.

Therefore $\langle\boldsymbol{g}\rangle$ is all of $\boldsymbol{G}$, that is $\boldsymbol{G}=\langle\boldsymbol{g}\rangle$ and hence $\boldsymbol{G}$ is cyclic.
The argument above shows that $\boldsymbol{G}$ has no nontrivial proper subgroups and therefore no nontrivial normal subgroups. Therefore $\boldsymbol{G}$ is simple.

## $\Rightarrow 3$-Isomorphisms:

We saw that there was a close relationship between ring homomorphisms and factor rings. In particular to each ideal, and consequently to each factor ring, there is a ring homomorphism that has that ideal as its kernel. Conversely to each ring homomorphism its kernel is an ideal and the corresponding factor ring is isomorphic to the image of the homomorphism. This was formalized in Theorem 1.5.7 which we called the ring isomorphism theorem. We now look at the group theoretical analog of this result, called the group isomorphism theorem. We will then examine some consequences of this result that will be crucial in the Galois theory of fields.
2. Definition : If $\boldsymbol{G}_{\boldsymbol{1}}$ and $\boldsymbol{G}_{\mathbf{2}}$ are groups and $\boldsymbol{f}: \boldsymbol{G}_{\mathbf{1}} \rightarrow \boldsymbol{G}_{\mathbf{2}}$ is a group homomorphism then the kernel of $\boldsymbol{f}$, denoted $\boldsymbol{\operatorname { k e r }}(\boldsymbol{f})$, is defined as

$$
\operatorname{ker}(f)=\left\{g \in G_{1}: f(g)=1\right\}
$$

That is the kernel is the set of the elements of $\boldsymbol{G}_{\boldsymbol{1}}$ that map onto the identity of $\boldsymbol{G}_{\mathbf{2}}$.
The image of $\boldsymbol{f}$, denoted $\boldsymbol{\operatorname { i m }}(\boldsymbol{f})$, is the set of elements of $\boldsymbol{G}_{\mathbf{2}}$. mapped onto by $\boldsymbol{f}$ from elements of $\boldsymbol{G}_{\mathbf{1}}$. That is

$$
\begin{aligned}
\operatorname{im}(f)=\{g & \in G_{2}: f\left(g_{1}\right) \\
& \left.=\mathfrak{g}_{2} \text { for some } \mathfrak{g}_{1} \in G_{1}\right\}
\end{aligned}
$$

Note that if $\boldsymbol{f}$ is a surjection then $\boldsymbol{\operatorname { i m }}(\boldsymbol{f})=\boldsymbol{G}_{\mathbf{2}}$

As with ring homomorphisms the kernel measures how far a homomorphism is from being an injection, that is, a one-to-one mapping.

## Lemma:

Let $\boldsymbol{G}_{\mathbf{1}}$ and $\boldsymbol{G}_{\mathbf{2}}$ are groups and $\boldsymbol{f}: \boldsymbol{G}_{\mathbf{1}} \boldsymbol{\rightarrow} \boldsymbol{G}_{\mathbf{2}}$ a group homomorphism.
Then $\boldsymbol{f}$ is injective if and only if $\boldsymbol{\operatorname { k e r }}(\boldsymbol{f})=$ \{1\}.

## Proof.

Suppose that $\boldsymbol{f}$ is injective. Since $\boldsymbol{f}(\mathbf{1})=\mathbf{1}$ we always have $\mathbf{1} \in \operatorname{ker}(f)$.
Suppose that $\mathbf{g} \in \boldsymbol{\operatorname { k e r }}(\boldsymbol{f})$. Then $\boldsymbol{f}(\mathbf{g})=\boldsymbol{f}(\mathbf{1})$. Since $\boldsymbol{f}$ is injective this implies that $\mathbf{g}=\mathbf{1}$ and hence $\boldsymbol{\operatorname { k e r }}(\boldsymbol{f})=\{\mathbf{1}\}$.
Conversely suppose that $\boldsymbol{\operatorname { k e r }}(\boldsymbol{f})=\{\mathbf{1}\}$ and $\boldsymbol{f}\left(\mathbf{g}_{1}\right)=\boldsymbol{f}\left(\mathbf{g}_{2}\right)$. Then
$f\left(\mathfrak{g}_{1}\right)\left(f\left(\mathbf{g}_{2}\right)\right)^{-1}=1 \Rightarrow f\left(\mathfrak{g}_{1} \mathfrak{g}_{2}{ }^{-1}\right)=1 \Rightarrow$ $\mathbf{g}_{1} \mathrm{~g}_{2}{ }^{-1} \in \operatorname{ker}(f)$.
Then since $\boldsymbol{\operatorname { k e r }}(\boldsymbol{f})=\{\mathbf{1}\}$ we have $\boldsymbol{g}_{\mathbf{1}} \mathbf{g}_{2}{ }^{\mathbf{1}}=$ 1 and hence $\boldsymbol{g}_{\mathbf{1}}=\mathbf{g}_{\mathbf{2}}$. Therefore $\boldsymbol{f}$ is
injective.
We now state the group isomorphism theorem.
This is entirely analogous to the ring isomorphism theorem replacing ideals by normal subgroups. We note that this theorem is sometimes called the first group isomorphism theorem.

Theorem: (group isomorphism theorem)
(a) Let $\boldsymbol{G}_{\mathbf{1}}$ and $\boldsymbol{G}_{\mathbf{2}}$ be groups and $\boldsymbol{f}: \boldsymbol{G}_{\mathbf{1}} \rightarrow$ $\boldsymbol{G}_{\mathbf{2}}$ a group homomorphism. Then $\boldsymbol{\operatorname { k e r }}(\boldsymbol{f})$ is a normal subgroup of $\boldsymbol{G}_{\mathbf{1}}, \boldsymbol{\operatorname { i m }}(\boldsymbol{f})$ is a subgroup of $\boldsymbol{G}_{\mathbf{2}}$ and

$$
G / \operatorname{ker}(f) \cong \operatorname{im}(f)
$$

(b) Conversely suppose that $\mathcal{N}$ is a normal subgroup of a group $\boldsymbol{G}$. Then there exists a group $\mathcal{H}$ and a homomorphism $\boldsymbol{f}: \boldsymbol{G} \rightarrow \boldsymbol{\mathcal { H }}$ such that $\boldsymbol{\operatorname { k e r }}(\boldsymbol{f})=\mathcal{N}$ and $\boldsymbol{\operatorname { i m }}(\boldsymbol{f})=\mathcal{H}$.

## Proof.

(a) Since $\mathbf{1} \in \boldsymbol{\operatorname { k e r }}(\boldsymbol{f})$ the kernel is nonempty. Suppose that $\mathbf{g}_{1}, \mathbf{g}_{2} \in \boldsymbol{\operatorname { k e r }}(\boldsymbol{f})$.
Then $\boldsymbol{f}\left(\mathbf{g}_{1}\right)=\boldsymbol{f}\left(\mathbf{g}_{2}\right)=\mathbf{1}$. It follows that $f\left(\boldsymbol{g}_{1} \mathfrak{g}_{2}{ }^{-1}\right)=f\left(g_{1}\right)\left(f\left(g_{2}\right)\right)^{-1}=1$.
Hence $\mathbf{g}_{\mathbf{1}} \mathbf{g}_{\mathbf{2}}{ }^{-\mathbf{1}} \in \boldsymbol{\operatorname { k e r }}(\boldsymbol{f})$ and therefore $\boldsymbol{\operatorname { k e r }}(\boldsymbol{f})$ is a subgroup of $\boldsymbol{G}_{\boldsymbol{1}}$. Further for any $\boldsymbol{g} \in \boldsymbol{G}_{\boldsymbol{1}}$ we have

$$
f\left(g^{-1} \mathfrak{g}_{1} g\right)=(f(g))^{-1} f\left(g_{1}\right) f(g)=
$$

$(f(g))^{-1} .1 . f(g)=f\left(g^{-1} g\right)=f(1)=1$. Hence $\boldsymbol{g}^{-\mathbf{1}} \mathfrak{g}_{\mathbf{1}} \boldsymbol{g} \in \boldsymbol{\operatorname { k e r }}(\boldsymbol{f})$ an $\boldsymbol{\operatorname { k e r }}(\boldsymbol{f}) \mathrm{d}$ is a normal subgroup.
It is straightforward to show that $\boldsymbol{\operatorname { i m }}(\boldsymbol{f})$ is a subgroup of $\boldsymbol{G}_{\mathbf{2}}$.
Consider the map $\hat{\boldsymbol{f}}: \boldsymbol{G} / \boldsymbol{\operatorname { k e r }}(\boldsymbol{f}) \rightarrow \boldsymbol{\operatorname { i m }}(\boldsymbol{f})$ defined by

$$
\hat{\boldsymbol{f}}(\boldsymbol{g} \operatorname{ker}(f))=f(\mathbf{g})
$$

We show that this is an isomorphism.
Suppose that $\boldsymbol{g}_{\mathbf{1}} \boldsymbol{\operatorname { k e r }}(\boldsymbol{f})=\boldsymbol{g}_{\mathbf{2}} \boldsymbol{\operatorname { k e r }}(\boldsymbol{f})$ then $\mathbf{g}_{1} \mathbf{g}_{2}{ }^{\mathbf{1}} \in \boldsymbol{\operatorname { k e r }}(\boldsymbol{f})$ so that $\boldsymbol{f}\left(\mathbf{g}_{1} \mathbf{g}_{2}{ }^{\mathbf{- 1}}\right)=1$
This implies that $\boldsymbol{f}\left(\mathbf{g}_{1}\right)=\boldsymbol{f}\left(\mathbf{g}_{2}\right)$ and hence the map $\hat{\boldsymbol{f}}$ is well-defined. Now

$$
\begin{aligned}
& \hat{f}\left(g_{1} \operatorname{ker}(f) g_{2} \operatorname{ker}(f)\right)=\hat{f}\left(g_{1} \mathbf{g}_{2} \operatorname{ker}(f)\right) \\
&=f\left(\mathbf{g}_{1} \mathfrak{g}_{2}\right)=f\left(\mathfrak{g}_{1}\right) f\left(\mathbf{g}_{2}\right) \\
&=\widehat{\boldsymbol{f}}\left(\mathbf{g}_{1} \operatorname{ker}(f)\right) \hat{\boldsymbol{f}}\left(\mathbf{g}_{2} \operatorname{ker}(f)\right)
\end{aligned}
$$

and therefore $\hat{\boldsymbol{f}}$ is a homomorphism.
Suppose that $\hat{\boldsymbol{f}}\left(\mathbf{g}_{1} \boldsymbol{\operatorname { k e r }}(\boldsymbol{f})\right)=\hat{\boldsymbol{f}}\left(\mathbf{g}_{2} \boldsymbol{\operatorname { k e r }}(\boldsymbol{f})\right)$ then $\boldsymbol{f}\left(\mathfrak{g}_{1}\right)=\boldsymbol{f}\left(\mathbf{g}_{2}\right)$ and hence $\mathbf{g}_{1} \operatorname{ker}(\boldsymbol{f})=$ $\mathbf{g}_{2} \boldsymbol{\operatorname { k e r }}(\boldsymbol{f})$. It follows that $\hat{\boldsymbol{f}}$ is injective.
Finally suppose that $\boldsymbol{h} \in \boldsymbol{\operatorname { i m }}(\boldsymbol{f})$. Then there exists a $\boldsymbol{g} \in \boldsymbol{G}_{\mathbf{1}}$ with $\boldsymbol{f}(\boldsymbol{g})=h$.

Then $\hat{\boldsymbol{f}}(\boldsymbol{g} \boldsymbol{\operatorname { k e r }}(\boldsymbol{f}))=\boldsymbol{h}$ and $\hat{\boldsymbol{f}}$ is a surjection onto $\boldsymbol{\operatorname { i m }}(\boldsymbol{f})$. Therefore $\hat{\boldsymbol{f}}$ is an isomorphism completing the proof of part (a).
(b) Conversely suppose that $\mathcal{N}$ is a normal subgroup of $\boldsymbol{G}$. Define the map $\boldsymbol{f}: \boldsymbol{G} \rightarrow \boldsymbol{G} / \mathcal{N}$ by $\boldsymbol{f}(\mathbf{g})=\boldsymbol{g} \mathcal{N}$ for $\in \boldsymbol{G}$. By the definition of the product in the quotient group $\boldsymbol{G} / \mathcal{N}$ it is clear that $\boldsymbol{f}$ is a homomorphism with $\boldsymbol{\operatorname { i m }}(\boldsymbol{f})=\boldsymbol{G} / \mathcal{N}$. if $\boldsymbol{g} \in$ $\boldsymbol{\operatorname { k e r }}(\boldsymbol{f})$ then $\boldsymbol{f}(\mathbf{g})=\boldsymbol{g} \mathcal{N}=\mathcal{N}$ since $\mathcal{N}$ is the identity in $\boldsymbol{G} / \boldsymbol{\mathcal { N }}$
However this implies that $\mathfrak{g} \in \mathcal{N}$ and hence it follows that $\boldsymbol{\operatorname { k e r }}(\boldsymbol{f})=\mathcal{N}$ completing the proof.
There are two related theorems that are called the second isomorphism theorem and the third isomorphism theorem.

## Reference

1. De Gruyter Graduate - Heldermann Verlage - Abstract Algebra (Applications to Galois Theory, Algebraic Geometry and Cryptography)- " 2011Walter de Gruyter GmbH \& Co. KG, Berlin/New York- Library of Congress Cataloging-inPublication Data.
2. BENJAMIN BAUMSLAG, Ph.D., BRUCE CHANDLER, Ph.D. (Department of Mathematics) - New York University - SCHAUM'S OUTLINE OF THEORY AND PROBLEMS OF GROUP THEORY- Copyright © 1968 by McGraw-Hill, Inc. All Rights Reserved. Printed in the United States of America. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of the publisher. (04124).
3. C. Curtis and I. Reiner, Representation Theory of Finite Groups and Associative Algebras, Wiley Interscience, 1966.
4. T. Camps, S. Künling and G. Rosenberger, Einführung in die mengenteoretische und die algebraische Topologie, Heldermann Verlag, 2006.
