Important Result: The converse of Lagrange's theorem is false...

A group A_4 of order 12 has no subgroup of order 6

Imp To verify this we see A_4 has 8 elements of order 3

$\alpha_1 = (1)$ $\alpha_2 = (1,2)(3,4)$ $\alpha_3 = (1,3)(2,4)$

$\alpha_4 = (1,4)(2,3)$ $\alpha_5 = (1,2,3)$ $\alpha_6 = (2,3,4)$

$\alpha_7 = (1,4,2)$ $\alpha_8 = (1,3,4)$ $\alpha_9 = (1,3,2)$

$\alpha_{10} = (1,4,3)$ $\alpha_{11} = (2,4,3)$ $\alpha_{12} = (1,2,4)$

Suppose that H is a subgroup of order 6

Let a be any element of order 3 in A_4

Since H has index 2 in A_4 atmost two of the cosets H, aH, a^2H are distinct.

But equality of any pair of these three implies

$aH = H \Rightarrow a \in H$ & if $H = a^2H$

$\& aH = a^3H = H$

$a \in H$

Thus a subgroup of A_4 of order 6 would have to contain eight elements of order 3 which is absurd

$\therefore$ There is no subgroup of order 6

Normal Subgroups & factor groups

Def": A subgroup H of a group G is called a normal subgroup of G if $aH = Ha$ for all a in G. We denote this by $H \triangleleft G$

Remark: Many people make the mistake of thinking that "H is normal in G means $ah = ha$ $\forall$ $a \in G$ & $h \in H$
This is not what normality of H means; rather it means that if $a \in G$ & $h \in H$ then there exists some $h' \in H$ such that $ah = h'a$

Normal Subgroup Test: A subgroup H of G is normal in G if and only if
$xHx^{-1} \subseteq H$ $\forall$ x in G

Example 1: Every subgroup of an abelian group is normal

Example 2: The center $Z(G)$ of a group G is the subset of elements in G that commute with every element of G.
$$Z(G) = \{a \in G \mid ax = xa \ \forall \ x \text{ in } G\}$$
The center of a group G is a subgroup of G. It is always normal because $aH = Ha$ for $a \in G$ & $h \in Z(G)$.

Example 3: The alternating group A_n of even permutations is a normal subgroup of S_n.
Note that for $(1,2) \in S_n$, $(1,2,3) \in A_n$ we have
$$(1,2)(1,2,3) \neq (1,2,3)(1,2)$$
but
$$(1,2)(1,2,3) = (1,3,2)(1,2)$$

Factor Group

When the subgroup H of G is normal the set of left (or right) cosets of H in G is itself a group called the factor group of G by H or the quotient group of G by H.

Theorem: Let G be a group & H be a normal subgroup of G. The set $G/H = \{aH \mid a \in G\}$ is a group under the operation $(aH)(bH) = abH$

Proof:

Our first task is to that the operation is well defined that is we must show that the correspondence defined from $G/H \times G/H$ into G/H is actually a function

Assume $aH = a'H$, $bH = b'H$ $\left[aH = a'H \Leftrightarrow a^{-1}a' \in H \Leftrightarrow a'\in aH\right]$

$\therefore a' = ah_1$ & $b' = bh_2$ for $h_1, h_2 \in H$

$\therefore a'b'H = ah_1 bh_2 H = ah_1 bH$ $[\because aH = H \Leftrightarrow a\in H]$

$= ah_1 Hb$ $[\because H \lhd G]$

$= aHb = abH = aHbH$

Now $eH = H$ is the identity element

Since $(aH) = (eH) = aeH = ah$

Also $a^{-1}H$ is the inverse of aH

$(aH)(a^{-1}H) = aa^{-1}H = eH = H$

$(a^{-1}H)(aH) = a^{-1}aH = eH = H$

[where $aH \in G/H$, $a^{-1}H \in G/H$]

For associativity

$(aHbH)cH = (ab)HcH = (ab)cH = a(bc)H = aH(bHcH)$

The operation $(aH)(bH) = abH$ implies that closure holds

$\therefore G/H$ is a group.

Example: Let $4\mathbb{Z} = \{0, \pm 4, \pm 8 \ldots\}$. To construct $\mathbb{Z}/4\mathbb{Z}$ we just determine the left cosets of $4\mathbb{Z}$ in $\mathbb{Z}$. Consider the following four cosets

$0 + 4\mathbb{Z} = 4\mathbb{Z} = \{0, \pm 4, \pm 8 \ldots\}$

$1 + 4\mathbb{Z} = \{1, 5, 9 \ldots ; -3, -7, -11 \ldots\}$

$2 + 4\mathbb{Z} = \{2, 6, 10 \ldots ; -2, -6, -10 \ldots\}$

$3 + 4\mathbb{Z} = \{3, 7, 11 \ldots ; -1, -5, -9 \ldots\}$

We claim that there are no others. For if $k \in \mathbb{Z}$ then $k = 4q + r$ where $0 \le r < 4$ & so $k + 4\mathbb{Z} = r + 4q + 4\mathbb{Z} = r + 4\mathbb{Z}$

We form a Cayley Table for $\mathbb{Z}/4\mathbb{Z}$.

	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$0+4\mathbb{Z}$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$
$1+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$	$0+4\mathbb{Z}$
$2+4\mathbb{Z}$	$2+4\mathbb{Z}$	$3+4\mathbb{Z}$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$
$3+4\mathbb{Z}$	$3+4\mathbb{Z}$	$0+4\mathbb{Z}$	$1+4\mathbb{Z}$	$2+4\mathbb{Z}$

Symmetries of Square

Consider a square with corners insulated on one side with colours blue, white, pink & green. Any motion will be equivalent to one of the eight listed below. The final position determined by location & orientation of any particular corner.

R_0 = Rotation of 0° (no change in position)

P	W
G	B

R_0 → | P | W | / | G | B |

R_{90} = Rotation of 90° (counter clockwise clockwise (anticlockwise)

P	W
G	B

$\xrightarrow{90^\circ}$ | W | P | / | G | B |

R_{180} = Rotation of 180

P	W
G	B

$\xrightarrow{R_{180}}$

B	G
W	P

R_{270} = Rotation of 270

P	W
G	B

$\xrightarrow{R_{270}}$

G	P
B	W

H = Rotation of 180° about horizontal axis

P	W
G	B

$\xrightarrow{H}$

G	B
P	W

V = Rotation of 180° about vertical axis

P	W
G	B

$\longrightarrow$

W	P
B	G

D = Rotation of 180° about main diagonal

P	W
G	B

$\xrightarrow{D}$

P	G
W	S

D' = Rotation of 180° about other diagonal

P	W
G	B

$\xrightarrow{D'}$

B	W
G	P

It can be seen that every motion is equal to one of the eight listed above. Suppose a square is repositioned by a rotation of 90° followed by a rotation of 180° about the horizontal axis of symmetry.

P	W
G	B

$\xrightarrow{R_{90}}$

W	B
P	G

$\xrightarrow{H}$

P	G
W	B

Thus we see that this pair of motions - taken together - is equal to the single motion D. Thus we can compose two motion to obtain a single motion. We write $HR_{90} = D$

The eight motions R_0, R_{90}, R_{180}, R_{270}, H, V, D & D' together with the operation composition form a mathematical system called the Dihedral group of order 8 (the order of group is the no of elements it contains) & it is denoted by D_4.

We now construct the Cayley Table.

	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_0	R_0	R_{90}	R_{180}	R_{270}	H	V	D	D'
R_{90}	R_{90}	R_{180}	R_{270}	R_0	D'	D	H	V
R_{180}	R_{180}	R_{270}	R_0	R_{90}	V	H	D'	D
R_{270}	R_{270}	R_0	R_{90}	R_{180}	D	D'	V	H
H	H	D	V	D'	R_0	R_{180}	R_{90}	R_{270}
V	V	D'	H	D	R_{180}	R_0	R_{270}	R_{90}
D	D	V	D'	H	R_{270}	R_{90}	R_0	R_{180}
D'	D'	H	D'	V	R_{90}	R_{270}	R_{180}	R_0

* We noticed that - the table is completely filled in written any two motions. Algebraically this means that if A & B are in D_4 then so is AB. This property is called Closure.

* Next we noticed that if a is any element of D_4 then $AR_0 = R_0A = A$ combining any element A on either side with R_0 yields A back when R_0 with this property is called an identity. Every group must have one.

* We see that for each element A in D_4 there is exactly one element R_θ in D_4 so that $AB = BA = R_\theta$. In this case B is said to be inverse of A & vice versa. For ex. R_{90} & R_{270} are inverse of each other. H is its own inverse.

* We noticed that $HD \neq DH$ but $R_{90} R_{180} = R_{180} R_{90}$ In a group AB may or may not be same as BA. If it happens that $AB = BA$ for all elements A & B say group is commutative (or abelian). Otherwise we say group is non abelian

* Thus, closure, existence of identity, existence of inverse - the three conditions are satisfied. The remaining cond" required for group is associativity that is $(ab)c = a(bc)$ $\forall$ a, b, c in the set
It may be observed that eight motions are functions & operation is function composition
We know that composition of functions is always associative.
∴ collection of these eight elements is a group.

Group Homomorphism

Def": A homomorphism ϕ from a group G to a group $\bar{G}$ is a mapping from G into $\bar{G}$ that preserves the group operation that is $\phi(a)\,\phi(b) = \phi(ab)$ $\forall$ a, b ∈ G

G operation	$\bar{G}$ operation	Operation preservation
·	·	$\phi(a \cdot b) = \phi(a) \cdot \phi(b)$
·	+	$\phi(a \cdot b) = \phi(a) + \phi(b)$
+	·	$\phi(a+b) = \phi(a) \cdot \phi(b)$
+	+	$\phi(a+b) = \phi(a) + \phi(b)$

Def": Kernel of a homomorphism
The kernel of a homomorphism ϕ from a group G to a group with identity e is the set $\{x \in G \mid \phi(x) = e\}$. The kernel of ϕ is denoted by $\ker \phi$

Remark: A homomorphism that is also one-one & onto is isomorphism

eg. The mapping ϕ from $\mathbb{R}$ to $\mathbb{R}^*$ where $\mathbb{R}^*$ is the group of non-zero real no. under mul. defined by $\phi(x) = |x|$ is a homomorphism with kernel $\phi = \{1, -1\}$

$\phi(xy) = |xy| = |x||y| = \phi(x)\,\phi(y)$

Properties of Homomorphism

Let ϕ be a homomorphism from a group G to a group $\bar{G}$ & let g be an element of G. Then

1. ϕ carries identity of G to identity of $\bar{G}$
2. $\phi(g^n) = [\phi(g)]^n$ for all integers n
3. If $g = |n|$ then $|\phi(g)|$ divides n
4. If $\phi(g) = g'$ then $\phi^{-1}(g') = \{x \in G \mid \phi(x) = g'\} = gk$

Proof

1. ϕ carries identity of G to identity of $\bar{G}$

→ For convenience let us denote the identity of G by e_G & identity of $\bar{G}$ by $e_{\bar{G}}$

Then $e_G = e_G e_G$

$$\phi(e_G) = \phi(e_G e_G)$$
$$= \phi(e_G)\,\phi(e_G) \quad -(1)$$

[ϕ is a homomorphism]

But $\phi(e_G) \in \bar{G}$

$$\therefore \phi(e_G) = e_{\bar{G}}\,\phi(e_G) \quad -(2)$$

From (1) & (2)

$$\phi(e_G)\phi(e_G) = e_{\bar{G}}\,\phi(e_G)$$

By cancellation law

$$\phi(e_G) = e_{\bar{G}}$$

2. For every integer n & for every group element g in G:

$$\phi(g^n) = [\phi(g)]^n$$

For positive integers we apply principle of induction

Let $n = 1$, $\phi(a^1) = [\phi(a)]^1$

So result is true for $n = 1$

Let $n = k$

Let the result be true for $n = k$

Then $\phi(a^k) = [\phi(a)]^k$

Let $n = k+1$

$$\phi(a^{k+1}) = \phi(\underbrace{a \cdots a}_{k+1 \text{ times}}) = \phi(a^k a)$$
$$= \phi(a^k)\,\phi(a) \quad [\phi \text{ is homomorphism}]$$
$$= [\phi(a)]^k \phi(a) \quad [\text{Result for } n = k]$$
$$= [\phi(a)]^{k+1}$$

Here result is true for $n = k+1$

∴ Result is true for all +ve integer

If n is 0 then

$$\phi(g^0) = \phi(e_G) = e_{\bar{G}}$$

Further $[\phi(g)]^0 = e_{\bar{G}}$

∴ Result is true for $n = 0$

If n is -ve then $-n$ is +ve

So, $e_{\bar{G}} = \phi(e_G) = \phi(g^n g^{-n})$

$$= \phi(g^n)\cdot\phi(g^{-n})$$
$$= \phi(g^n)[\phi(g)]^{-n}$$

Multiplying on right by $[\phi(g)]^n$

$$[\phi(g)]^n = \phi(g^n)$$

Result is true for -ve integers also

3. If $|g| = n$ then $|\phi(g)|$ divides n

Now $e_{\bar{G}} = \phi(e_G) = \phi(g^n)$

$$= [\phi(g)]^n$$

[ϕ carries identity of G to identity of $\bar{G}$
$|g| = n \Rightarrow g^n = e$
Also $\phi(g^n) = [\phi(g)]^n$

We have the result

"Let G be a group & a be an element of order n in G. If $a^k = e$ then n divides k"

Hence $[\phi(g)]^n = e_{\bar{G}}$

$\Rightarrow$ $|\phi(g)|$ divides n

4. If $\phi(g) = g'$ then $\phi^{-1}(g') = \{x \in G \mid \phi(x) = g'\} = g \ker \phi$

We must show that $\phi^{-1}(g') \subseteq g \ker \phi$

& $g \ker \phi \subseteq \phi^{-1}(g')$

For just inclusion let $x \in \phi^{-1}(g')$

so that $\phi(x) = g'$

Then $\phi(x) = \phi(g)$

$\Rightarrow [\phi(g)]^{-1} \phi(x) = e$

$\Rightarrow e = [\phi(g)]^{-1} \phi(x) = \phi(g^{-1}) \phi(x) = \phi(g^{-1}x)$

[$\because \phi$ is homomorphism]

$\therefore \phi(g^{-1}x) = e$.

$g^{-1}x \in \ker \phi$

$x \in g \ker \phi$

$\therefore \phi^{-1}(g') \subseteq g \ker \phi$ — (1)

To prove $g \ker \phi \subseteq \phi^{-1}(g')$

Suppose that $k \in \ker \phi$

Then $\phi(gk) = \phi(g)\phi(k) = g'e = g'$

$\therefore gk \in \phi^{-1}(g')$

& $g \ker \phi \in \phi^{-1}(g')$ — (2)

From (1) & (2)

$\phi^{-1}(g') = g \ker \phi$

Theorem: Let ϕ be a homomorphism from a group G to a group $\bar{G}$ & let H be a subgroup of G. Then

1. $\phi(H) = \{\phi(h) \mid h \in H\}$ is a subgroup of $\bar{G}$

Since $e_{\bar{G}} = \phi(e_G) \in \phi(H)$ we know that $\phi(H)$ is not empty

If $\phi(h_1), \phi(h_2) \in \phi(H)$ then

$\phi(h_1)\phi(h_2)^{-1} = \phi(h_1)\phi(h_2^{-1})$

$= \phi(h_1 h_2^{-1}) \in \phi(H)$

[$\because h_1 h_2^{-1} \in H$]

$\therefore$ By one step subgroup test $\phi(H)$ is a subgroup of $\bar{G}$

2. Let H be cyclic. Then $\phi(H)$ is cyclic

Let H be cyclic. Let $h' \in \phi(H)$ then

$\exists\, h \in H$ s.t $\phi(h) = h'$

Now, $h \in H = \langle a \rangle$ [$\because H$ is cyclic]

$\Rightarrow h = a^m$ for some integer m

$\therefore h' = \phi(h) = \phi(a^m) = \phi(\underbrace{a \cdots a}_{m \text{ times}})$

$h' = [\phi(a)]^m$

Now, $\phi(h) = [\phi(a)]^n$

$\Rightarrow \phi(H) = \langle \phi(a) \rangle \Rightarrow \phi(H)$ is cyclic

3. If H is abelian then $\phi(H)$ is abelian

Let $\alpha, \beta \in \phi(H)$

$\Rightarrow \exists\, x, y \in H$ such that

$\phi(x) = \alpha$ & $\phi(y) = \beta$

$\Rightarrow \alpha\beta = \phi(x)\phi(y) = \phi(xy)$ [$\because \phi$ is a homomorphism]

$\Rightarrow \alpha\beta = \phi(yx)$ [$\because H$ is abelian]

$\Rightarrow \alpha\beta = \phi(y)\phi(x)$ [$\because \phi$ is homomorphism]

$= \beta\alpha$

$\Rightarrow \alpha\beta = \beta\alpha$ $\forall\, \alpha, \beta \in \phi(H)$

$\phi(H)$ is abelian

4. If H is normal in G then $\phi(H)$ is normal in $\phi(G)$

To prove this property let $\phi(h) \in \phi(H)$ & $\phi(g) \in \phi(G)$. Then

$\phi(g)\phi(h)[\phi(g)]^{-1} = \phi(g)\phi(h)\phi(g^{-1})$ [$\because [\phi(a)]^n = \phi(a^n)$]

$= \phi(ghg^{-1})$ [ϕ is homo.]

$\in \phi(H)$ [$\because ghg^{-1} \in H$ as H is normal]

$\therefore \phi(H)$ is normal in $\phi(G)$

5. If $|\ker \phi| = n$ then ϕ is n to 1 mapping from G onto $\phi(G)$

This property follows from the following result:

[If $\phi(g) = g'$ then $\phi^{-1}(g') = \{x \in G \mid \phi(x) = g'\} = g\ker\phi$]

$\therefore$ Order of $\phi^{-1}(g') = |g.\ker\phi| = |g| n$

$\therefore \phi^{-1}$ is a 1 to n mapping $\Rightarrow \phi$ is n to 1 mapping from G onto $\phi(G)$

6. If $|H| = n$ then $|\phi(H)|$ divides n

To prove this property let ϕ_H denote the restriction of ϕ to elements of H. Thus ϕ_H is a homomorphism from H to $\phi(H)$

Suppose $|\ker\phi| = t$ then by the prop.

[If $|\ker\phi| = n$ then ϕ is n to 1 mapping from G onto $\phi(G)$]

ϕ_H is a t to 1 mapping.

So $|\phi(H)|t = |H|$

So $t = \dfrac{|H|}{|\phi(H)|}$

So $|\phi(H)|$ divides $|H|$ which is n.

7. If $\bar{K}$ is a subgroup of $\bar{G}$ then $\phi^{-1}(\bar{K}) = \{k \in G \mid \phi(k) \in \bar{K}\}$ is a subgroup of G

To prove this property we see $e \in \phi^{-1}(\bar{K})$ $\phi^{-1}(\bar{K})$ is non-empty. Let $k_1, k_2 \in \phi^{-1}(\bar{K})$ Then by def^n of $\phi^{-1}(\bar{K})$ we know $\phi(k_1), \phi(k_2) \in \bar{K}$ Thus $[\phi(k_2)]^{-1} \in \bar{K}$

So we have

$\phi(k_1 k_2^{-1}) = \phi(k_1)\phi(k_2^{-1}) = \phi(k_1)\phi(k_2)^{-1} \in \bar{K}$

[$\because \bar{K}$ is subgroup of $\bar{G}$]

Now since $\phi(k_1 k_2^{-1}) \in \bar{K}$ by def^n of $\phi^{-1}(\bar{K})$ we have $k_1 k_2^{-1} \in \phi^{-1}(\bar{K})$

$\therefore$ By one step subgroup test $\phi^{-1}(\bar{K})$ is subgroup

8. If $\bar{K}$ is a normal subgroup of $\bar{G}$ then $\phi^{-1}(\bar{K}) = \{k \in G \mid \phi(k) \in \bar{K}\}$ is a normal subgroup of G

Let k be a normal subgroup of $\bar{G}$. For any elements $k \in K$ & $g \in G$

$\phi(g^{-1}kg) = [\phi(g)]^{-1}\phi(k)\phi(g) \in \bar{K}$

[$\because \phi(k) \in \bar{K}$, $\phi(g) \in \bar{G}$ & $\bar{K}$ is a normal subgroup of $\bar{G}$]

$\phi(g^{-1}kg) \in \bar{K}$

$\Rightarrow g^{-1}kg \in K$

$\Rightarrow K$ is normal subgroup of G

9. If ϕ is onto & $\ker\phi = \{e\}$ then ϕ is one-one mapping from G to $\bar{G}$ (isomorphism)

Let $\phi: G \to \bar{G}$ be a homomorphism

Let $\phi(x) = \phi(y)$

$\Rightarrow \phi(x)\phi(y)^{-1} = e'$

$\phi(x)\phi(y^{-1}) = e'$

$\phi(xy^{-1}) = e$

$xy^{-1} \in \ker\phi = \{e\}$

$xy^{-1} = e \Rightarrow x = y$

$\therefore \phi$ is one-one

* **Theorem:** Let ϕ be a group homomorphism from G to $\bar{G}$. Then $\ker\phi$ is normal subgroup of G

Proof:

Since $\phi(e) = e' \Rightarrow e \in \ker\phi$

$\ker\phi$ is non empty

Let $x, y \in \ker\phi$

$\Rightarrow \phi(x) = e' \qquad \phi(y) = e'$

$\phi(xy^{-1}) = \phi(x)\,\phi(y^{-1}) = \phi(x)[\phi(y)]^{-1} = ee'^{-1} = e'$

$\Rightarrow xy^{-1} \in \ker\phi$

Hence it is subgroup of G

Again for $g \in G \quad x \in \ker\phi$

$\phi(g^{-1}xg) = \phi(g^{-1})\,\phi(x)\,\phi(g) = [\phi(g)]^{-1}\phi(x)\phi(g)$

$= [\phi(g)]^{-1} e' \phi(g)$

$= e'$

$\Rightarrow g^{-1}xg \in \ker\phi$

$\therefore$ It is normal subgroup of G

Ex: Consider the mapping ϕ from C^* to C^* given by $\phi(x) = x^4$

$\phi(xy) = (xy)^4 = x^4y^4 = \phi(x)\,\phi(y)$

$\therefore$ It is homomorphism

$\ker\phi = \{x \mid \phi(x) = x^4 = 1\} = \{1, -1, i, -i\}$

By prop of homomorphism we know that ϕ is 4 to 1 mapping

Now let us find all elements mapped to 2

$\phi(2^{1/4}) = 2$

since $\phi^{-1}(g') = g\ker\phi$

$\therefore \sqrt{2}\ker\phi = \{\sqrt{2}, -\sqrt{2}, \sqrt{2}i, -\sqrt{2}i\}$

Ring

Def": A ring R is a set with two binary operations addition (denoted by $a+b$) & multiplication (denoted by ab) such that for all a, b, c in R

1. $a + b = b + a$
2. $(a + b) + c = a + (b + c)$
3. There is an element 0 in R s.t. $a + 0 = a$.
4. There is an element $-a$ in R st. $a + (-a) = 0$
5. $a(bc) = (ab)c$
6. $a(b + c) = ab + ac$

Remarks:

1. A ring is an abelian group under addition also having an associative multiplication that is left & right distributive over addition
2. In a ring multiplication need not to be commutative when it is, we say that ring is commutative.
3. A ring need not to have an identity element under multiplication. When ring other than $\{0\}$ has an identity under multiplication we say the ring has unity (identity)

4. A non zero element of a commutative ring with unity need not have a multiplicative inverse. When it does we say that it is a unit of the ring. Thus a is a unit if a^{-1} exist.

Example1: The set $\mathbb{Z}$ of integers under ordinary add^n is a commutative ring with with unity 1. The units of $\mathbb{Z}$ are 1 & -1.

Example2: The set $\mathbb{Z}_n = \{0, 1, \ldots n-1\}$ under add^n & mul^n modulo n is a commutative ring with unity 1. The set of units is $U(n)$.

Example3: The set $2\mathbb{Z}$ of even integers under ordinary add^n & mul^n is a commutative ring without unit.

Theorem: In a ring R the following results hold

1. $a.0 = 0.a = 0 \quad \forall a \in R$
2. $a(-b) = (-a)b = -ab \quad \forall a, b \in R$
3. $(-a)(-b) = ab \quad \forall a, b \in R$
4. $a.(b-c) = ab - ac \quad \forall a, b, c \in R$

Proof:

1. $a.0 = 0.a = 0$

i) $a.0 = a.(0+0)$

$a.0 = a.0 + a.0$

$a.0 + 0 = a.0 + a.0$

$0 = a.0$ [using cancellation wrt + in $\langle R, + \rangle$]

$\therefore a.0 = 0$

2. $a(-b) = (-a)b = -ab$

$a.0 = 0$

$a(-b+b) = 0$

$a(-b) + ab = a$

$a(-b) = -(ab)$

Similarly, $(-a).b = -ab$

3. $(-a)(-b) = ab$

ii) $(-a)(-b) = -(a(-b)) = -[-ab] = ab$

4. $a.(b-c) = ab - ac$

$a(b-c) = a[b + (-c)]$

$= ab + a(-c)$

$= ab - ac$

Remark: If R has a unity element 1 then i) $(-1)a = -a$ ii) $(-1)(-1) = 1$

i) We know $(-a)b = -(ab)$

$(-1)a = -(1a) = -a$

ii) $(-1)(-1) = 1$

We know $(-a)(-b) = ab$

$\therefore (-1)(-1) = 1.1 = 1$

Theorem: If a ring has unity it is unique. If a ring element has an inverse it is unique.

Proof: Same as groups.

Subrings: A subset S of a ring R is a subring of R if S itself is a ring with operations in R

Subring Test: A non-empty subset of a ring R is a subring if S is closed under subtraction & multiplication - that is if a-b & ab are in S whenever a & b are in S

Proof: Since addition in R is commutative & S is closed under subtraction & multiplication we know by one-step subgroup test that S is an abelian group under "add".
Now multiplication in R is associative as well as distributive over add", the same is true for multiplication in S.
Thus the only cond" remaining to be checked is that mul" is a binary operation on S.
But this is exactly what closure means
[It is given that S is closed under mul"]

Remark: If R is a ring then {0} & R are always subrings of R called subrings of R

* Def": (Zero Divisors): A non zero element a in a commutative ring R is called a zero divisor, if there is a non-zero element b in R such that ab=0

Def" Integral Domain: A commutative ring with unity is said to be an Integral domain if it has no zero divisors.

Remark: In an Integral domain, a product is 0 only when one of the factors is 0 that is ab=0 only when a=0 or b=0

Ex1 The ring of integers is an Integral domain

Ex2 The ring of Gaussian Integers Z[i]={a+bi | a,b∈Z} is an integral domain.

Ex3 The set Z[x] of polynomials with integer coefficients is an Integral domain.

Theorem: Let a,b,c belong to Integral domain. If a≠0 & ab=ac then b=c

Proof: From ab=ac we have a(b-c)=0
Since a≠0 & a,b,c are in Integral domain have b-c=0
& b=c

Field: A commutative ring with unity is called a field if every non-zero element is unit.

Theorem: Every field is an integral domain.

Proof: If a & b belong to a field with $a \neq 0$ & $ab = 0$ we can multiply both sides of last expression by a^{-1}

$a^{-1}ab = a^{-1}0$

$\Rightarrow b = 0$

Theorem: A finite integral domain is a field.

Proof: Let D be a finite integral domain with unity 1.

Let a be any non-zero element of D.

We must show that a is a unit. If $a = 1$ a is its own inverse. So we assumes $a \neq 1$

Now consider the following sequence of element of D $a, a^2, a^3 \ldots$

Since D is finite there must be two +ve integer i & j such that $i > j$ & $a^i = a^j$. Then by cancellation $a^{i-j} = 1$. Since $a \neq 1$ we know $i - j > 1$ & so a^{i-j-1} is inverse of a

Corollary: Z_p is a field.

For every prime p, Z_p the ring of integers modulo p is a field.

Proof: Acc. to theorem [A finite integral domain is a field] we only need to show that Z_p has no zero divisor.

So suppose $a, b \in Z_p$ & $ab = 0$

Then $ab = pk$ for some integer k. Then p divides ab i.e. p divides b. Thus in Z_p $a = 0$ or $b = 0$

Ideal Def^n: A subring A of a ring R is called a (two sided) ideal of R if for every $r \in R$ & every $a \in A$ both ra & ar are in a.

Remark: 1. A subring A of a ring R is called an ideal of R if A absorbs elements from R that is $rA \subseteq A$ & $Ar \subseteq A$ $\forall r \in R$

2. An ideal A of R is called a proper ideal of R if A is a proper subset of R

Ideal Test

1. A non empty subset A of a ring R is an ideal of R if
   i) $a - b \in A$ whenever $a, b \in A$
   ii) ra & ar are in A whenever $a \in A$ & $r \in R$

Ex1. For any ring R, $\{0\}$ & R are ideals of R. The ideal $\{0\}$ is called trivial ideal.

Ex2. For any +ve integer n, $n\mathbb{Z} = \{0, \pm n, \pm 2n, \ldots\}$ is ideal of $\mathbb{Z}$

Def^n: Let R be a commutative ring with unity & $a \in R$

The set $\langle a \rangle = \{ra \mid r \in R\}$ is an ideal of R called principal ideal generated by a

Note: $\langle a \rangle$ notation is also used for cyclic group generated by a. However meaning is clear from context.

Characteristic of a Ring:

The characteristic of a ring R is the least positive integer n such that $nx = 0$ $\forall x$ in R. If no such integer exists we say that R has characteristic 0

Remark: The ring of integers has characteristic 0. & $\mathbb{Z}_n$ has characteristic n.

Theorem: Characteristic of a ring with unity
Let R be a ring with unity 1. If 1 has infinite order under add" then characteristic of R is 0. If 1 has order n under add" then characteristic of R is n.

Proof: If 1 has infinite order then there is no +ve integer n such that $n.1 = 0$.
So characteristic of R is 0.
Now suppose 1 has additive order n then $n.1 = 0$. Now suppose that 1 has additive & n is the least +ve integer with this prop. So for any x in R,
$nx = n(1.x) = (n.1)x = 0.x = 0$
Thus R has characteristic n.

Characteristic of an Integral Domain
Theorem: The characteristic of an integral domain is 0 or prime

Proof: By theorem proved above it suffices to show that if the additive order of 1 is finite it must be prime. Suppose that 1 has order n and $n = s.t$ where $1 \le s, t \le n$. Then
$0 = n.1 = (st).1 = (s.1)(t.1)$
so $s.1 = 0$ or $t.1 = 0$ [since an integral domain]
Since n is the least +ve integer with the property that $n.1 = 0$ we must have $s = n$ or $t = n$
Thus n is prime.

Factor Ring

Let R be a ring & let A be an ideal of R. Since R is a group under add" & A is a normal subgroup of R we may form the factor group
$R/A = \{x + A \mid x \in R\}$
We define the product of two cosets of $S + A$ & $t + A$ as $st + A$

Existence of factor ring
Let R be a ring & let A be a subring of R. The set of cosets $\{x + A \mid x \in R\}$ is a ring under the operation $(s + A) + (t + A) = (s + t) + A$ & $(s + A)(t + A) = st + A$ iff A is ideal of R

Ring Homomorphism

A ring homomorphism ϕ from a ring R to a ring S is a mapping from R to S that preserves the two ring operations i.e $\forall a, b \in R$
$\phi(a + b) = \phi(a) + \phi(b)$, $\phi(ab) = \phi(a).\phi(b)$

A ring homomorphism that is both one-one & onto is called ring isomorphism.

Kernel of Ring homomorphism

Let ϕ be a homomorphism from a ring R to a ring S. Then $\ker \phi = \{x \in R \mid \phi(x) = 0\}$ is an ideal of R.

Properties

Let ϕ be a homomorphism from a ring R to a ring S. Let A & B be subrings of R & let B be an ideal of S.

1. For every $x \in R$ & any +ve integer n
$\phi(nx) = n\phi(x)$
& $\phi(x^n) = [\phi(x)]^n$

Now $\phi(ix) = \phi(x)$ is true

Proof

Let $\phi(nx) = \phi(x + x + \dots x) = n\phi(x)$ be true

$\phi((n+1)x) = \phi(\underbrace{x + x + \dots x}_{(n+1) \text{ times}}) = \phi(\underbrace{x + x + \dots x}_{n \text{ times}} + x)$

$= \phi(nx) + \phi(x)$

$= n\phi(x) + \phi(x) = (n+1)\phi(x)$

$\therefore$ Result is true

Similarly $\phi(x^n) = (\phi(x))^n$

2. $\phi(A) = \{\phi(a) \mid a \in A\}$ is a subring of R

Let $\phi(a), \phi(b) \in \phi(A)$

$\phi(a) - \phi(b) = \phi(a) + (-\phi(b))$

$= \phi(a) + \phi(-b)$ [by result on group]

$= \phi(a - b) \in \phi(A)$ [$\because \phi$ is homomorphism]

$\phi(a)\phi(b) = \phi(ab) \in \phi(A)$ [$\because \phi$ is homomorphism]

$\therefore \phi(A)$ is a subring

3. If A is an ideal & ϕ is onto S then $\phi(A)$ is an ideal.

To show $\phi(A)$ is an ideal let $a, b \in \phi(A)$

then $a = \phi(a')$ & $b = \phi(b')$

$a - b = \phi(a') - \phi(b') = \phi(a' - b') \in \phi(A)$

[since A is an ideal $a' - b' \in A$]

$\boxed{a - b \in \phi(A)}$

Since, $\phi: R \to S$ is onto $\forall\, x \in R$ s.t $\phi(x) = s$

it follows

$sa = \phi(x)\phi(a) = \phi(xa') \in \phi(A)$

$as = \phi(a')\phi(x) = \phi(a'x) \in \phi(A)$

$\therefore \phi(A)$ is an ideal

4. $\phi^{-1}(B) = \{x \in R \mid \phi(x) \in B\}$ is an ideal of R

If $a, b \in \phi^{-1}(B)$

then $\phi(a) \in B$ & $\phi(b) \in B$

& $\phi(a) - \phi(b) \in B$ [$\because B$ is ideal of S]

& $\phi(a - b) \in B$ [$\because \phi$ is homomorphism]

$\Rightarrow a - b \in \phi^{-1}(B)$ — (1)

Let $x \in R$ & $x_1 \in \phi^{-1}(B)$

Consider $\phi(xx_1) = \phi(x)\phi(x_1) = \phi(x)j \in B$ [$\because x_1 \in A$, $\forall \phi(x_1) = j$]

& $\phi(x_1 x) = \phi(x_1)\phi(x) = j\phi(x) \in B$ [B is an ideal]

$xx_1, x_1 x \in \phi^{-1}(B)$ & $x_1, x \in \phi^{-1}(B)$

$\therefore \phi^{-1}(B)$ is ideal of R

5. If R is commutative, $\phi(R)$ is commutative

Let $\alpha, \beta \in R$

Then $\alpha\beta = \beta\alpha$

$\phi(\alpha)\phi(\beta) = \phi(\alpha\beta) = \phi(\beta\alpha) = \phi(\beta)\phi(\alpha)$

Hence the result

A ring homomorphism that is both one-one & onto is called ring isomorphism.

Kernel of Ring homomorphism
Let ϕ be a homomorphism from a ring R to a ring S. Then $\ker \phi = \{x \in R \mid \phi(x) = 0\}$ is an ideal of R.

Properties
Let ϕ be a homomorphism from a ring R to a ring S. Let A & B be subrings of R & let B be an ideal of S.

1. For every $x \in R$ & any +ve integer n
$\phi(nx) = n\phi(x)$
& $\phi(x^n) = [\phi(x)]^n$
Now $\phi(ix) = i\phi(x)$ is true
Proof
Let $\phi(nx) = \phi(x + x + \dots x) = n\phi(x)$ be true
$\phi((n+1)x) = \phi(\underbrace{x + x + \dots x}_{(n+1) \text{ times}}) = \phi(\underbrace{x + x + \dots x}_{n \text{ times}} + x)$
$= \phi(nx) + \phi(x)$
$= n\phi(x) + \phi(x) = (n+1)\phi(x)$
$\therefore$ Result is true
Similarly $\phi(x^n) = (\phi(x))^n$

2. $\phi(A) = \{\phi(a) \mid a \in A\}$ is a subring of R
Let $\phi(a), \phi(b) \in \phi(A)$
$\phi(a) - \phi(b) = \phi(a) + (-\phi(b))$
$= \phi(a) + \phi(-b)$ [by result on group]
$= \phi(a - b) \in \phi(A)$ [$\because \phi$ is homomorphism]
$\phi(a)\phi(b) = \phi(ab) \in \phi(A)$ [$\because \phi$ is homomorphism]
$\therefore \phi(A)$ is a subring

3. If A is an ideal & ϕ is onto S then $\phi(A)$ is an ideal.
To show $\phi(A)$ is an ideal let $a, b \in \phi(A)$
then $a = \phi(a')$ & $b = \phi(b')$
$a - b = \phi(a') - \phi(b') = \phi(a' - b') \in \phi(A)$
[since A is an ideal $a' - b' \in A$]
$\boxed{a - b \in \phi(A)}$

Since, $\phi: R \to S$ is onto $\exists\ x \in R$ s.t $\phi(x) = s$
It follows
$sa = \phi(x)\phi(a) = \phi(xa') \in \phi(A)$
$as = \phi(a')\phi(x) = \phi(a'x) \in \phi(A)$
$\therefore \phi(A)$ is an ideal

4. $\phi^{-1}(B) = \{x \in R \mid \phi(x) \in B\}$ is an ideal of R
If $a, b \in \phi^{-1}(B)$
then $\phi(a) \in B$ & $\phi(b) \in B$
$\Rightarrow \phi(a) - \phi(b) \in B$ [$\because B$ is ideal of S]
$\Rightarrow \phi(a - b) \in B$ [$\because \phi$ is homomorphism]
$\Rightarrow a - b \in \phi^{-1}(B)$ — (1)
Let $x \in R$ & $x_1 \in \phi^{-1}(B)$
Consider $\phi(xx_1) = \phi(x)\phi(x_1) = \phi(x)j \in B$ [$\because x_1 \in A$, $\phi(x_1) = j$]
& $\phi(x_1 x) = \phi(x_1)\phi(x) = j\phi(x) \in B$ [B is ideal]
$xx_1, x_1x \in \phi^{-1}(B)$ & $x_1, x \in \phi^{-1}(B)$
$\therefore \phi^{-1}(B)$ is ideal of R

5. If R is commutative, $\phi(R)$ is commutative
Let $\alpha, \beta \in R$
Then $\alpha\beta = \beta\alpha$
$\phi(\alpha)\phi(\beta) = \phi(\alpha\beta) = \phi(\beta\alpha) = \phi(\beta)\phi(\alpha)$
Hence the result

6. If R has unity 1, $S \neq \{0\}$ & ϕ is onto then $\phi(1)$ is unity of S

Let $a' \in S$ be any element

Since ϕ is onto $\exists\ a \in R$ s.t $\phi(a) = a'$

$a'\phi(1) = \phi(a)\phi(1) = \phi(a \cdot 1) = \phi(a) = a'$

Sim. $\phi(1)\, a' = a'$

$\phi(1)$ is unity of S

Theorem: The kernel of any ring homomorphism $\phi : R \to S$ is an ideal of R

Proof:

We know from group theory that $\ker(\phi)$ is an additive subgroup of R.

Suppose $r \in R$ & $a \in \ker\phi$

Then we must show ar & ra are in $\ker\phi$

$\phi(ar) = \phi(a)\,\phi(r) = 0\,\phi(r) = 0$

$\phi(ra) = \phi(r)\,\phi(a) = \phi(r).\,0 = 0$

$\therefore ar$ & ra are in $\ker\phi$

Homomorphism from $\mathbb{Z}$ to a ring with unity

Let R be a ring with unity e

The mapping $\phi : \mathbb{Z} \to R$ given by $n \to ne$ is a ring homomorphism

Proof:

Let $m, n \in \mathbb{Z}$

$\phi(m+n) = (m+n)e$

$= e + \cdots + e$ ($m+n$ times)

$= (e + \cdots + e) + (e + \cdots + e)$ (m times, n times)

$= me + ne$

$= \phi(m) + \phi(n)$

Now suppose both m & n are negative

$\phi(m+n) = (m+n)e$

$= (-m-n)(-e)$

$= (-m)(-e) + (-n)(-e)$

$= me + ne$

$= \phi(m) + \phi(n)$

Suppose one of m & n is non-ve. $m \geq 0$, $n < 0$

$\phi(m+n) = (m+n)e$

$= (e + \cdots + e) - (e + \cdots + e)$ (m times, $-n$ summands)

$= me + ne$

$= \phi(m) + \phi(n)$

ϕ preserves add^n

The mult^n case

$(ma)(nb) = (mn)(ab)$ + integers m & n

$\phi(mn) = (mn)e = (mn)(ee) = (me)(ne)$

$= \phi(m)\,\phi(n)$

Fundamental Theorem for Ring Homomorphism

OR

First Isomorphism Theorem for Rings

Let ϕ be a ring homomorphism from R onto $\phi(R)$

Then the mapping from $R/\ker\phi$ to $\phi(R)$ given by

$r + \ker\phi \to \phi(r)$ is an isomorphism

In symbols $R/\ker\phi \cong \phi(R)$

Proof:

Let $\phi : R \to S$ be onto homomorphism

Define $f : R/\ker\phi \to \phi(R)$

by $f(r+k) = \phi(r)$ $\forall\ r \in R$ & $k = \ker\phi$

f is well defined as $r + k = t + k$

$\Rightarrow (x-t) \in K = \ker \phi$

$\phi(x-t) = 0$

$\Rightarrow \phi(x) - \phi(t) = 0$

$\Rightarrow \phi(x) = \phi(t)$

$\Rightarrow f(x+k) = f(t+k)$

f is one one

Let $f(x+k) = f(t+k)$

$\Rightarrow \phi(x) = \phi(t)$

$\Rightarrow \phi(x-t) = 0$

$\Rightarrow x - t \in K = \ker \phi$

$\Rightarrow x+k = t+k$

$\therefore x+k = t+k$

$x - t + k = k$

$x - t \in k$

Again $f(x+k) + (t+k) = \phi[(x+t)+k]$

$= \phi(x+t) = \phi(x) + \phi(t)$ $\because \phi$ is homo

$= f(x+k) + f(t+k)$

$f(x+k)(t+k) = f(xt+k) = \phi(xt) = \phi(x)\phi(t)$

$= f(x+k) f(t+k)$

$\therefore f$ is homomorphism.

If $x' = \phi(x) \in \phi(R)$ be any element then for $x \in R$

$f(x+k) = \phi(x) = x$

$x+k$ is preimage of x'

$\therefore f$ is onto

$\therefore R/\ker\phi \cong \phi(R)$

Theorem: Every ideal of a ring R is the kernel of a ring homomorphism of R. In particular an ideal A is kernel of the mapping $x \to x+A$ from R to R/A. The homomorphism from R to R/A is called natural homomorphism from R to R/A

Proof:

Define $f: R \to R/A$

as $f(x) = x + A \quad \forall x \in R$

f is well defined

Let $x = y \quad x, y \in R$

$\Rightarrow x + A = y + A$

$\Rightarrow f(x) = f(y)$

$f(x+y) = x+y+A = (x+A)+(y+A)$

$= f(x) + f(y)$

$f(xy) = (xy) + A = (x+A)(y+A)$

$\therefore f$ is a homomorphism

To show $\ker f = A$

$\ker f = \{x \in R : f(x) = 0+A\}$

$= \{x \in R \mid x+A = 0+A\}$

$= \{x \in R \mid x+A = A\}$

$= \{x \in R \mid x \in A\}$

$\therefore \ker f = A$