Rings and Modules
Chapter 5

Dr. Md. Masum Murshed
Department of Mathematics
University of Rajshahi

Additive Abelion Group

(i) $a + b \in G, \forall\ a,\ b \in G.$
(ii) $a + (b + c) = (a + b) + c\ \forall\ a,\ b,\ c \in G.$
(iii) There exists $0 \in G$ such that $a + 0 = 0 + a = a\ \forall\ a \in G.$
(iv) For every $a \in G$ there exists, $-a \in G$ such that $a + (-a) = (-a) + a = 0.$
(v) $a + b = b + a\ \forall\ a,\ b \in G.$

Ring: $(R, +, *)$

(i) R is an additive abelion group.
(ii) $a * b \in R\ \forall\ a,\ b \in R.$
(iii) $a * (b * c) = (a * b) * c\ \forall\ a,\ b,\ c \in R.$
(iv) $a * (b + c) = a * b + a * c\ \forall\ a,\ b,\ c \in R.$
(v) $(a + b) * c = (a * c) + (b * c)\ \forall\ a,\ b,\ c \in R.$

If $ab = ba$, then $(R, +, *)$ is a commutative ring.

Left R-module: Let R be a ring (not necessarily commutative). Let M be an additive abelian group then M is called a $left$ *R-module* if M is closed under scalar multiplication and satisfies the following conditions:
(i) $r(x + y) = rx + ry$
(ii) $(r_1r_2)(x) = r_1(r_2x)$
(iii) $(r_1 + r_2)(x) = r_1x + r_2x$
(iv) if $1 \in R$ then $1.x = x$,

where, $r_1, r_2, r \in R$ and $x,\ y \in M$; and $r \in R,\ x \in M$ implies rx is the unique element in M. The *left R-module* M is denoted by $_RM$.

Right R-module: Let R be a ring (not necessarily commutative). Let M be an additive abelian group then M is called a *right R-module* if M is closed under scalar multiplication and satisfies the following conditions:
(i) $(x + y)r = xr + yr$
(ii) $x(r_1r_2) = (xr_1)r_2$
(iii) $x(r_1 + r_2) = xr_1 + xr_2$
(iv) if $1 \in R$ then $x.1 = x$,

where, $r_1, r_2, r \in R$ and $x,\ y \in M$; and $r \in R,\ x \in M$ implies xr is the unique element in M. The *right R-module* M is denoted by M_R.

R-Module: An additive abelian group M is called an *R-Module* if it is both a *left R-Module* and a *right R-Module.* If R is a commutative ring then M is both a $left$ and a $right$ *R-Module*.

Examples:

(i) Any ring R is an *R-module* (either *left* or *right R-module*).

(ii) If R is a field then every vactor space V over R is an *R-module*.

(iii) $2\mathbb{Z}$ is a *$\mathbb{Z}$-module*.

(iv) Every abelian group is a *$\mathbb{Z}$-module*.

(v) Every ideal I of a ring R is an *R-module*.

Bi-Module: Let R and S be two rings each with identity element. Then the additive abelian group M is called a *Bi-module* if M is a left *R-Module* and a *right S-module* and it is denoted by $_RM_S$.

Sub-Module: Let R be a ring with 1 and M be a *left R-module*, then a subset N of M is said to be a *sub-module* of M if,

(i) N is a *sub-group* of M,

(ii) for each $r \in R$ and $n \in N$ implies $rn \in N$.

Theorem: Let N_i; $i \in I$ be a fimily of *sub-modules* of a *left R-module* M then $\bigcap_{i\in I} N_i$ is a *sub-module* of M.

Proof: Clearly, $\bigcap_{i\in I} N_i$ is a *sub-group* of M. Let $r \in R$ and $n \in \bigcap N_i$. This implies that $n \in N_i$ for each i. Since, each N_i is a submodule of M, $rn \in N_i$ for each i. Therefore, $rn \in \bigcap_{i\in I} N_i$. Hence, $\bigcap_{i\in I} N_i$ is a *sub-module* of M.

Factor module: Let M be a *left R-module* and N be a *sub-module* of M. We define $r(m+N) = rm + N$, then the factor group $\frac{M}{N}$ becomes a *left R-module*. This *left R-module* $\frac{M}{N}$ is called a *factor module* of M by N, where $m \in M$ and $r \in R$.

Note:

If $\overline{x+y} \in \frac{M}{N}$ then $\overline{x+y} = \overline{x} + \overline{y}$.

If $\overline{ax} \in \frac{M}{N}$ then $\overline{ax} = a\overline{x} = a(x+N)$.

If $x \in \frac{M}{N}$ then $x = m + N$, where $m \in M$.

Homomorplism: Let M and M' are *left R-modules*. A mapping $f : M \to M'$ is called an *R-hmomorplism* or a *linear mapping* or *linear homomorphism*, if the following conditions are satisfied:

(i) $f(x+y) = f(x) + f(y)$, $\forall\ x, y \in M$,

(ii) $f(rx) = rf(x)\ \forall\ x \in M$ and $r \in R$.

Example:

Let M be a *left R-module* and S be an *R-sub module* of M. A mapping $\phi : M \to \frac{M}{S}$ define by $\phi(m) = m + S$ is an *R-homomorphism*.

Proof : Here given that, $\phi(m) = m + S$, where $m \in M$.

Now, let $m_1,\, m_2 \in M$ then we have,

$$\begin{aligned} \phi(m_1 + m_2) &= m_1 + m_2 + S \\ &= m_1 + S + m_2 + S \\ &= \phi(m_1) + \phi(m_2). \end{aligned}$$

Again let, $r \in R$ and $m \in M$, then $rm \in M$. Now, we have,

$$\begin{aligned} \phi(rm) &= rm + S \\ &= r(m + S) \\ &= r\phi(m). \end{aligned}$$

Hence, ϕ is an *R-homomorphism*.

Problem: Let M and M' be two *left R-modules*. Show that the mapping $\phi : M \to M'$ defined by $\phi(x) = x^2$ is not an *R-homomorphism*.

Proof : Given that, $\phi : x \to x^2$.

Let $x,\, y \in M$ then $\phi(x) = x^2$ and $\phi(y) = y^2$.

$$\begin{aligned} \therefore \phi(x + y) &= (x + y)^2 \\ &= x^2 + y^2 + 2xy \\ &= \phi(x) + \phi(y) + 2xy. \end{aligned}$$

Thus, $\phi(x + y) \neq \phi(x) + \phi(y)$.

Again, if $r \in R$, then $\phi(rx) = r^2x^2 = r^2\phi(x)$.

Which implies that, $\phi(rx) \neq r\phi(x)$.

Hence, ϕ is not an *R-homomorphism*.

Problem: Let $M,\, N,\, Q$ be three *R-modules* and let $T : M \to N$ and $S : N \to Q$ be *R-homomorphisms*. Let $ST : M \to Q$ define by $(ST)(m) = ST(m)$ for $m \in M$. Prove that ST is an *R-homomorphism*.

Proof: Let $m,\, m_1,\, m_2 \in M$; $n,\, n_1,\, n_2 \in N$ and $r \in R$.

Since, T and S are both *R-homomorphism* then we have,

$T(m_1 + m_2) = T(m_1) + T(m_2)$, $T(rm) = rT(m)$

and $S(n_1 + n_2) = S(n_1) + S(n_2)$, $S(rn) = rS(n)$.

$$\begin{aligned} \text{Now, } (ST)(m_1 + m_2) &= ST(m_1 + m_2) \\ &= S(T(m_1) + T(m_2)) \\ &= S(T(m_1)) + S(T(m_2)) \\ &= ST(m_1) + ST(m_2) \\ &= (ST)(m_1) + (ST)(m_2). \end{aligned}$$

$$\begin{aligned} \text{And, } (ST)(rm) &= ST(rm) \\ &= S(rT(m)) \\ &= rS(T(m)) \\ &= rST(m) \\ &= r(ST)(m). \end{aligned}$$

Hence. $ST : M \to Q$ is an *R-homomorphism.*

Problem: Let M and Q be two *R-modules* and let $S : M \to Q$ and $T : M \to Q$ be *R-homomorphisms*. Then show that $(S + T) : M \to Q$ is an *R-homomorphism.*

Proof: Since, S and T are two *R-homomorphism* from M to Q, then for m_1, $m_2 \in M$ and $r \in R$, we have,

$$\begin{aligned} (S + T)(m_1 + m_2) &= S(m_1 + m_2) + T(m_1 + m_2) \\ &= S(m_1) + S(m_2) + T(m_1) + T(m_2) \\ &= S(m_1) + T(m_1) + S(m_2) + T(m_2) \\ &= (S + T)(m_1) + (S + T)(m_2). \end{aligned}$$

$$\begin{aligned} \text{And, } \quad (S + T)(rm) &= S(rm) + T(rm) \\ &= rS(m) + rT(m) \\ &= r(S(m) + T(m)) \\ &= r(S + T)(m). \end{aligned}$$

Hence, $(S + T)$ is an *R-homomorphism.*

Problem: If $f : M \to T$ be an *R-homomorphism* and X, Y being *R-submodules* of M and T, respectively, with the property that $f(X) = \{f(x) : x \in X\} \subseteq T$. Then show that $f' : \dfrac{M}{X} \to \dfrac{T}{Y}$ defined by $f'(m + X) = f(m) + Y$ is an *R-homomorphism*.

Proof: Let $m_1 + X$, $m_2 + X \in \dfrac{M}{X}$, where m_1, $m_2 \in M$ and $r \in R$, then,

$(m_1 + X) + (m_2 + X) = (m_1 + m_2) + X \in \dfrac{M}{X}$

$$\begin{aligned}
\text{Now, } f'((m_1 + X) + (m_2 + X)) &= f'((m_1 + m_2) + X) \\
&= f(m_1 + m_2) + Y \\
&= f(m_1) + f(m_2) + Y \\
&= f(m_1) + Y + f(m_2) + Y \\
&= f'(m_1 + X) + f'(m_2 + X).
\end{aligned}$$

$$\begin{aligned}
\text{Again, } f'(r(m + X)) &= f'(rm + X) \\
&= f(rm) + Y \\
&= rf(m) + Y \\
&= r(f(m) + Y) \\
&= rf'(m + X)
\end{aligned}$$

Hence, f' is an *R-homomorphism*.

Theorem: Let $\phi : M \to M'$ be an *R-homomorphism*, then show that,

(i) $\phi(0) = \bar{0}$, where $0 \in M$ and $\bar{0} \in M'$

(ii) $\phi(-m) = -\phi(m)$, where $m \in M$.

Proof (i): We have,

$\phi(m) + \bar{0} = \phi(m) = \phi(m + 0) = \phi(m) + \phi(0)$

i.e., $\phi(m) + \bar{0} = \phi(m) + \phi(0)$

Now, adding $-\phi(m)$ on both sides, we have, $\phi(0) = \bar{0}$.

Proof (ii): We have, from (i),

$$\begin{aligned}
\bar{0} &= \phi(0) \\
&= \phi(m + (-m)) \\
&= \phi(m) + \phi(-m)
\end{aligned}$$

i.e., $\phi(m) + \phi(-m) = \bar{0}$

Adding $-\phi(m)$ on both sides, we get,

$$\begin{aligned} \phi(-m) &= -\phi(m) + \bar{0} \\ &= -\phi(m) \end{aligned}$$

$\therefore \phi(-m) = -\phi(m)$.

Kernel and Image of an R-homomorphism: Let $\phi : M \to M'$ be an *R-homomorphism*. Then the *kernel* of ϕ is defined by, $ker\phi = \{x \in M : \phi(x) = \bar{0}\}$ and the image of ϕ is written as $Im\phi$ and is defined by $Im\phi = \{\phi(x) : x \in M\}$.

Theorem: Let $\phi : M \to M'$ be an *R-homomorphism*, then show that,

(i) $ker\phi$ is a *sub-module* of M.

(ii) $Im\phi$ is a *sub-module* of M'.

Proof (i): Since $\phi(0) = \bar{0}$ implies $0 \in ker\phi$, therefore $ker\phi$ is nonempty.

Now, let m_1, $m_2 \in ker\phi$ then $\phi(m_1) = \bar{0}$ and $\phi(m_2) = \bar{0}$.

Now, $\phi(m_1 + m_2) = \phi(m_1) + \phi(m_2) = \bar{0} + \bar{0} = \bar{0}$

which implies that $m_1 + m_2 \in ker\phi$.

Again, let $r \in R$ and $m \in ker\phi$ then $\phi(m) = \bar{0}$.

Now, $\phi(rm) = r\phi(m) = r.\bar{0} = \bar{0}$

which implies that $rm \in ker\phi$.

Hence, $ker\phi$ is a *sub-module* of M.

Proof (ii): Since $\phi(0) = \bar{0}$ implies $\bar{0} \in M'$. Also $\bar{0} \in Im\phi$, therefore $Im\phi$ is nonempty.

let $\phi(m_1), \phi(m_2) \in Im\phi$ then,

$\phi(m_1) + \phi(m_2) = \phi(m_1 + m_2) = \phi(m_3)$ where $m_3 \in M$

which implies $\phi(m_1) + \phi(m_2) \in Im\phi$.

Finally, let $r \in R$ *and* $\phi(m) \in Im\phi$ then, $r\phi(m) = \phi(rm) \in Im\phi$.

Hence $r\phi(m) \in Im\phi$ and therefore $Im\phi$ is a sub-module of M'.

Epimorphism: A homomorphism $f : M \to M'$ is called an *epimorphism* when $f(M) = Imf = M'$.

Monomorphism: A homomorphism $f : M \to M'$ is called a *monomorphism* if $f(m_1) = f(m_2) \implies m_1 = m_2$ for every $m_1,\ m_2 \in M$.

Isomorphism: A homomorphism $f : M \to M'$ is called an *isomorphism* if f is an *epimorphism* and a *monomorphism*.

Note: If $f : M \to M'$ is an *isomorphism* and if $f^{-1} : M' \to M$ be a mapping defined by $f^{-1}(x') = x\ iff\ f(x) = x'$ then f^{-1} is also an *isomorphism*. Here $f^{-1} \circ f$ is the identity mapping of M and $f \circ f^{-1}$ is the identity of M'.

Canonical injection and projection: If N is a *submodule* M then the mapping $J : N \to M$ defined by $J(x) = x\ \forall\ x \in N$ is a *monomorphism* and is called the *natural* or *canonical injection* of N into M.

The mapping $\phi : M \to \dfrac{M}{N}$ defined by $\phi(m) = m + N$ is called the *natural* or *canonical projection*.

Note: The set of all *homomorphism* of M to M' is denoted by $Hom_R(M, M')$.

Endomorphism and Automorphism: A *homomorphism* of M to M itself is called an *endomorphism* and an *isomorphism* of M to M itself is called an *automorphism*.

Theorem: If R is a commutative ring and M, M' are *R-modules* then the set $Hom_R(M, M')$ is an *R-module*.

Proof: We define, $(f_1 + f_2)(m) = f_1(m) + f_2(m)$, where $f_1,\ f_2 \in Hom_R(M, M')$.

(i) Here we have,
$$\begin{aligned}(f_1 + f_2)(m_1 + m_2) &= f_1(m_1 + m_2) + f_2(m_1 + m_2)\\ &= f_1(m_1) + f_1(m_2) + f_2(m_1) + f_2(m_2)\\ &= f_1(m_1) + f_2(m_1) + f_1(m_2) + f_2(m_2)\\ &= (f_1 + f_2)(m_1) + (f_1 + f_2)(m_2)\end{aligned}$$

And,
$$\begin{aligned}(f_1 + f_2)(rm) &= f_1(rm) + f_2(rm)\\ &= rf_1(m) + rf_2(m)\\ &= r(f_1(m) + f_2(m))\\ &= r(f_1 + f_2)(m).\end{aligned}$$

Thus, $f_1 + f_2 \in Hom_R(M, M')$.

i.e., $Hom_R(M, M')$ is closed under addition.

(ii) For any $f_1, f_2, f_3 \in Hom_R(M, M')$ we have,

$$\begin{aligned}(f_1 + (f_2 + f_3))(m) &= f_1(m) + (f_2 + f_3)(m) \\ &= f_1(m) + f_2(m) + f_3(m) \\ &= (f_1(m) + f_2(m)) + f_3(m) \\ &= (f_1 + f_2)(m) + f_3(m) \\ &= ((f_1 + f_2) + f_3)(m)\end{aligned}$$

Hence, $f_1 + (f_2 + f_3) = (f_1 + f_2) + f_3$.

i.e., associative law for addition is satisfied in $Hom_R(M, M')$.

(iii) We define $f_0 : M \to M'$ by $f_0(m) = \bar{0}$ such that,

$$\begin{aligned}(f + f_0)(m) &= f(m) + f_0(m) \\ &= f(m) + \bar{0} \\ &= f(m)\end{aligned}$$

i.e., $f + f_0 = f$

Similarly, we have, $f_0 + f = f$

Hence, f_0 is the identity element of $Hom_R(M, M')$.

(iv) For every $f \in Hom_R(M, M')$ there exists $-f \in Hom_R(M, M')$ defined by

$$\begin{aligned}(-f)(m) = -f(m) \text{ such that } (f + (-f))(m) &= f(m) + (-f)(m) \\ &= f(m) - f(m) \\ &= \bar{0} \\ &= f_0(m)\end{aligned}$$

Which implies $f + (-f) = f_0$.

Similarly, we have, $(-f) + f = f_0$

Hence, inverse element exists in $Hom_R(M, M')$.

(v) For all $f_1, f_2 \in Hom_R(M, M')$ we have,

$$\begin{aligned}(f_1+f_2)(m) &= f_1(m)+f_2(m)\\ &= f_2(m)+f_1(m)\\ &= (f_1+f_2)(m)\end{aligned}$$

This implies $f_1+f_2 = f_2+f_1$

Hence $Hom_R(M, M')$ is an additive abelian group.

(vi) Now, for any $r \in R$ and $f \in Hom_R(M, M')$, define $(rf)(m) = rf(m)$ and $(fr)(m) = f(m)r$. We show that rf and fr are *R-homomorphisms*. i.e., $rf,\ fr \in Hom_R(M, M')$.

$$\begin{aligned}\text{We have, } (rf)(m_1+m_2) &= r(f(m_1+m_2))\\ &= r(f(m_1)+f(m_2))\\ &= rf(m_1)+rf(m_2)\\ &= (rf)(m_1)+(rf)(m_2)\end{aligned}$$

$$\begin{aligned}\text{Again, } (rf)(r'm) &= rf(r'm)\\ &= rr'f(m)\\ &= r'rf(m) \text{ (since } R \text{ is commutative)}\\ &= r'(rf)(m)\end{aligned}$$

Hence, $rf \in Hom_R(M, M')$.

Similarly, we can show that $fr \in Hom_R(M, M')$.

(vii) Now, for any $r \in R$ and $f_1,\ f_2 \in Hom_R(M, M')$, we have,

$$\begin{aligned}(r(f_1+f_2))(m) &= r(f_1+f_2)(m)\\ &= r(f_1(m)+f_2(m))\\ &= rf_1(m)+rf_2(m)\\ &= (rf_1+rf_2)(m)\end{aligned}$$

i.e., $r(f_1+f_2) = rf_1+rf_2$

Similarly, we can show that $(f_1+f_2)r = f_1r+f_2r$

(viii) Next, for any r_1, $r_2 \in R$ and $f \in Hom_R(M, M')$, we have,

$$\begin{aligned}((r_1 + r_2)f)(m) &= (r_1 + r_2)f(m) \\ &= r_1 f(m) + r_2 f(m) \\ &= (r_1 f)(m) + (r_2 f)(m) \\ &= (r_1 f + r_2 f)(m)\end{aligned}$$

i.e., $(r_1 + r_2)f = r_1 f + r_2 f$

Similarly, we can show that $f(r_1 + r_2) = fr_1 + fr_2$

(ix) Next, for any r_1, $r_2 \in R$ and $f \in Hom_R(M, M')$, we have,

$$\begin{aligned}((r_1 r_2)f)(m) &= (r_1 r_2)(f(m)) \\ &= r_1(r_2 f(m)) \\ &= r_1(r_2 f)(m)\end{aligned}$$

i.e., $((r_1 r_2)f) = r_1(r_2 f)$

Similarly, we can show that $(f(r_1 r_2)) = (fr_1)r_2$

(x) Finally, if $1 \in R$, then for any $f \in Hom_R(M, M')$, we have, $(1f)(m) = 1f(m) = f(m)$

i.e., $1f = f$

Similarly, $f1 = f$

Hence, $Hom_R(M, M')$ is an *R-module*.

Theorem: If M is an *R-module*, then show that $Hom_R(M, M)$ is a *ring*.

or, The set of all endomorphism is a ring.

Proof: We define, $(f_1 + f_2)(m) = f_1(m) + f_2(m)$, where f_1, $f_2 \in Hom_R(M, M)$.

(i) Here we have, $$\begin{aligned}(f_1 + f_2)(m_1 + m_2) &= f_1(m_1 + m_2) + f_2(m_1 + m_2) \\ &= f_1(m_1) + f_1(m_2) + f_2(m_1) + f_2(m_2) \\ &= f_1(m_1) + f_2(m_1) + f_1(m_2) + f_2(m_2) \\ &= (f_1 + f_2)(m_1) + (f_1 + f_2)(m_2)\end{aligned}$$

$$\begin{aligned} \text{And, } (f_1 + f_2)(rm) &= f_1(rm) + f_2(rm) \\ &= rf_1(m) + rf_2(m) \\ &= r(f_1(m) + f_2(m)) \\ &= r(f_1 + f_2)(m). \end{aligned}$$

Thus, $f_1 + f_2 \in Hom_R(M, M)$.

i.e., $Hom_R(M, M)$ is closed under addition.

(ii) For any $f_1, f_2, f_3 \in Hom_R(M, M)$ we have,

$$\begin{aligned} (f_1 + (f_2 + f_3))(m) &= f_1(m) + (f_2 + f_3)(m) \\ &= f_1(m) + f_2(m) + f_3(m) \\ &= (f_1(m) + f_2(m)) + f_3(m) \\ &= (f_1 + f_2)(m) + f_3(m) \\ &= ((f_1 + f_2) + f_3)(m) \end{aligned}$$

Hence, $f_1 + (f_2 + f_3) = (f_1 + f_2) + f_3$.

i.e., associative law for addition is satisfied in $Hom_R(M, M)$.

(iii) We define $f_0 : M \to M$ by $f_0(m) = \bar{0}$ such that,

$$\begin{aligned} (f + f_0)(m) &= f(m) + f_0(m) \\ &= f(m) + \bar{0} \\ &= f(m) \end{aligned}$$

i.e., $f + f_0 = f$

Similarly, we have, $f_0 + f = f$

Hence, f_0 is the identity element of $Hom_R(M, M)$.

(iv) For every $f \in Hom_R(M, M)$ there exists $-f \in Hom_R(M, M)$ defined by

$$\begin{aligned} (-f)(m) = -f(m) \text{ such that } (f + (-f))(m) &= f(m) + (-f)(m) \\ &= f(m) - f(m) \\ &= \bar{0} \\ &= f_0(m) \end{aligned}$$

Which implies $f + (-f) = f_0$.

Similarly, we have, $(-f)+f=f_0$

Hence, inverse element exists in $Hom_R(M,M)$.

(v) For all $f_1, f_2 \in Hom_R(M,M)$ we have,

$$\begin{aligned}(f_1+f_2)(m) &= f_1(m)+f_2(m)\\ &= f_2(m)+f_1(m)\\ &= (f_1+f_2)(m)\end{aligned}$$

This implies $f_1+f_2=f_2+f_1$

Hence $Hom_R(M,M)$ is an additive abelian group.

(vi) Let $f_1,\ f_2 \in Hom_R(M,M)$ and $m_1,\ m_2 \in M$, then

$$\begin{aligned}(f_1f_2)(m_1+m_2) &= f_1(f_2(m_1+m_2))\\ &= f_1(f_2(m_1)+f_2(m_2))\\ &= f_1(f_2(m_1))+f_1(f_2(m_2))\\ &= (f_1f_2)(m_1)+(f_1f_2)(m_2)\end{aligned}$$

Again, let $f_1,\ f_2 \in Hom_R(M,M)$, $m \in M$ and $r \in R$, then

$$\begin{aligned}(f_1f_2)(rm) &= f_1(f_2(rm))\\ &= f_1(rf_2(m))\\ &= rf_1(f_2(m))\\ &= r(f_1f_2)(m)\end{aligned}$$

This implies that, $f_1f_2 \in Hom_R(M,M)$.

(vii) Let $f_1,\ f_2,\ f_3 \in Hom_R(M,M)$ and $m \in M$, then

$$\begin{aligned}((f_1f_2)f_3)(m) &= (f_1f_2)(f_3(m))\\ &= f_1(f_2(f_3(m)))\\ &= f_1((f_2f_3)(m))\\ &= (f_1(f_2f_3))(m)\end{aligned}$$

Hence, $(f_1f_2)f_3=f_1(f_2f_3)$.

(viii) Let f_1, f_2, $f_3 \in Hom_R(M, M)$ and $m \in M$, then

$$\begin{aligned}((f_1 + f_2)f_3)(m) &= (f_1 + f_2)(f_3(m)) \\ &= f_1(f_3(m)) + f_2(f_3(m)) \\ &= (f_1f_3)(m) + (f_2f_3)(m) \\ &= (f_1f_3 + f_2f_3)(m)\end{aligned}$$

Hence, $(f_1 + f_2)f_3 = f_1f_3 + f_2f_3$.

Similarly, we can show that

(ix) $f_1(f_2 + f_2) = f_1f_2 + f_1f_3$.

Hence, $Hom_R(M, M)$ is a ring.

Problem: Let R be a ring and let M and N be two arbitary *R-modules*. Let $f : M \to N$ be an *R-homomorphism*, then f is a *monomorphism* (*one-one*) iff $kerf = \{0\}$.

Proof: First suppose that $f : M \to N$ be a *monomorphism*. We show that $kerf = \{0\}$.

Let $a \in kerf$, then we have $f(a) = 0$.

Also, since f is a *monomorphism*, then f is an *R-homomorphism* and *one-one*.

Therefore, $f(0) = 0$. So, we have $f(a) = 0 = f(0)$. Which implies that $a = 0$.

Since $a \in kerf$ implies $a = 0$.

Hence $kerf = \{0\}$.

Conversely, let $kerf = \{0\}$, we have to show that f is a *monomorphism*. i.e., f is *one-one*.

Let $f(a_1) = f(a_2)$, then we have,

$f(a_1) - f(a_2) = 0$

$\implies f(a_1 - a_2) = 0$

$\implies a_1 - a_2 \in kerf$.

Now, since $kerf = \{0\}$, then $a_1 - a_2 = 0$.

Which implies atat $a_1 = a_2$.

Hence, f is *one-one*.

Definition: let M, M', M'' be three left *R-modules* and let $f : M \to M'$ and $g : M' \to M''$, then the mapping $g \circ f : M \to M''$ defined by $(g \circ f)(m) = g(f(m))$ is a *homomorphism* of M into M'. If f and g are *monomorphism* or *epimorphism* or *isomorphism*, then $g \circ f$ is so.

Definition: let $f : N \to M$ be a *homomorphism* of two $left$ *R-modules* N and M, then we define *co-kernel* and *co-image* by *co-*$kerf$=$\dfrac{M}{Imf}$ and *co-*Imf =$\dfrac{N}{kerf}$.

Theorem: Let R be a ring with 1 and let A and B be two $left$ *R-modules.* Let $\phi : A \to B$ be an *R-homomorphism* then $\dfrac{A}{ker\phi} \cong Im\phi$.

or, State and prove the fundamental theorem of *R-homomorphism.*

Proof: Define a map $\psi : \dfrac{A}{ker\phi} \to Im\phi$ by

$\psi(a + ker\phi) = \phi(a)$ for $a \in A$.

Then, this map is well defined. For if,

$a + ker\phi = a' + ker\phi$ for a, $a' \in A$

$$\begin{aligned}
\text{Then, } a - a' \in ker\phi \quad &\Longrightarrow \phi(a - a') = 0 \\
&\Longrightarrow \phi(a) - \phi(a') = 0 \\
&\Longrightarrow \phi(a) = \phi(a') \\
&\Longrightarrow \psi(a + ker\phi) = \psi(a' + ker\phi)
\end{aligned}$$

Thus, ψ is well defined.

Let $a + ker\phi$, $a' + ker\phi \in \dfrac{A}{ker\phi}$, then

$$\begin{aligned}
\psi((a + ker\phi) + (a' + ker\phi)) &= \psi(a + a' + ker\phi) \\
&= \phi(a + a') \\
&= \phi(a) + \phi(a') \\
&= \psi(a + ker\phi) + \psi(a' + ker\phi)
\end{aligned}$$

Again, let $a + ker\phi \in \dfrac{A}{ker\phi}$ and $r \in R$, then

$$\begin{aligned}
\psi(r(a + ker\phi)) &= \psi(ra + ker\phi) \\
&= \phi(ra) \\
&= r\phi(a) \text{ (since } \phi \text{ is an } R\text{-}homomorphism) \\
&= r\psi(a + ker\phi)
\end{aligned}$$

Hence, ψ is an *R-homomorphism.*

Next, let $\psi(a + ker\phi) = \psi(a' + ker\phi)$ for $a,\, a' \in A$

$$\begin{aligned}
\text{Then,} \quad & \phi(a) = \phi(a') \\
\implies \quad & \phi(a) - \phi(a') = 0 \\
\implies \quad & \phi(a - a') = 0 \\
\implies \quad & a - a' \in ker\phi \\
\implies \quad & a + ker\phi = a' + ker\phi
\end{aligned}$$

Hence, ψ is a *monomorphism*.

Now for any, $a \in A$, $\phi(a) \in Im\phi$. And for any $\phi(a) \in Im\phi$ there exists an element $a + ker\phi \in \dfrac{A}{ker\phi}$ such that $\psi(a + ker\phi) = \phi(a)$. Thus, ψ is an *epimorphism*.

Therefore, ψ is an isomorphism.

Hence $\dfrac{A}{ker\phi} \cong Im\phi$

proved

Exact and Short Exact Sequence

Exact sequence: A sequence of *R-modules* and *R-homomorphism*,

$$M_0 \xrightarrow{f_0} M_1 \xrightarrow{f_1} M_2 \xrightarrow{f_2} M_3 \xrightarrow{f_3} \dots \xrightarrow{f_{n-2}} M_{n-1} \xrightarrow{f_{n-1}} M_n \xrightarrow{f_n} M_{n+1} \qquad (1)$$

is said to be exact at M_i if $ker(f_i) = Im(f_{i-1})$. The sequence (1) is called exact if it is exact at each M_i for all $1 \leq i \leq n$, i.e., if $ker(f_i) = Im(f_{i-1})$ for all $1 \leq i \leq n$. The sequence (1) of *R-modules* and *R-homomorphism* may be either finite or infinite.

Note

Consider the sequence $0 \longrightarrow A \xrightarrow{f} B$. The image of the leftmost map is $\{0\}$. Therefore the sequence is exact if and only if $kerf = \{0\}$; that is, if and only if f is a monomorphism (injective, or one-one).

Consider the sequence $B \xrightarrow{g} C \longrightarrow 0$. The kernel of the rightmost map is C. Therefore the sequence is exact if and only if $Img = C$; that is, if and only if g is an epimorphism (surjective, or onto).

Therefore, the sequence $0 \longrightarrow A \xrightarrow{f} B \longrightarrow 0$ is exact if and only if f is both a monomorphism and epimorphism, and thus, in many cases, an isomorphism from A to B.

Short exact sequence (SES): Let A, B, C be three *R-modules* and let $f : A \to B$ and $g : B \to C$ be *R-homomorphisms* then the following sequence

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0 \qquad (2)$$

is called a *short exact sequence* of *R-modules* and *R-homomorphism* if it is exact at each of A, B and C, i.e., f is a *monomorphism*, g is an *epimorphism* and $Imf = kerg$.

Theorem: Let $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ be a short exact sequence of *R-modules* and *R-homomorphisms* then $A \cong kerg = Imf$ and $C = Img$.
Proof: Since $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ is a short exact sequence of *R-modules* and *R-homomorphisms* then, we have f is *monomorphism*, g is an *epimorphism* and $Imf = kerg$.

Let $h : A \to Imf$ be defined by $h(a) = f(a)\ \forall\ a \in A$. Then clearly h is a *monomorphism* and an *epimorphism*. Thus h is an *isomorphism*, i.e., $A \cong Imf$. But $Imf = kerg$. Hence $A \cong kerg = Imf$.

Since g is an *epimorphism*, we have $Img = C$.

Hence $A \cong kerg = Imf$ and $C = Img$.

Theorem: Let $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ be a short exact sequence of *R-modules* and *R-homomorphisms* then *co-ker*$f = \dfrac{B}{Imf} = \dfrac{B}{kerg} \cong Img = C$.

Proof: Since $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ is a short exact sequence of *R-modules* and *R-homomorphisms* then, we have f is *monomorphism*, g is an *epimorphism* and $Imf = kerg$.

By definition we have, *co-ker*$f = \dfrac{B}{Imf}$. Since $Imf = kerg$, then we have *co-ker*$f = \dfrac{B}{Imf} = \dfrac{B}{kerg}$.

Since $g : B \to C$ is a homomorphism, then by the fundamental theorem we have, $\dfrac{B}{kerg} \cong Img$. Again since g is an *epimorphism*, we have $Img = C$.

Hence *co-ker*$f = \dfrac{B}{Imf} = \dfrac{B}{kerg} \cong Img = C$.

Split short exact sequence: A short exact sequence $0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$ of *R-modules* and *R-homomorphisms* is called a split short exact sequence if either

(i) there exists an *R-homomorphism* $\alpha' : B \to A$ such that $\alpha'\alpha = 1_A$, where 1_A is the identity mapping on A.

or, (ii) there exists an *R-homomorphism* $\beta' : C \to B$ such that $\beta\beta' = 1_C$, where 1_C is the identity map on C.

Theorem: Let $0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$ be a short exact sequence of *R-modules* and *R-homomorphism*, then show that the following conditions are equivalent.

(i) there exists an *R-homomorphism* $\alpha' : B \to A$ such that $\alpha'\alpha = 1_A$, where 1_A is the identity mapping on A.

(ii) there exists an *R-homomorphism* $\beta' : C \to B$ such that $\beta\beta' = 1_C$, where 1_C is the identity map on C.

Or, Prove that the conditions for split short exact sequence are equivalent.

Proof: Since $0 \longrightarrow A \xrightarrow{\alpha} B \xrightarrow{\beta} C \longrightarrow 0$ is a short exact sequence of *R-modules* and *R-homomorphisms* then, we have α is *monomorphism*, β is an *epimorphism* and $Im\alpha = ker\beta$.

Let (i) holds. Let $c \in C$ then since β is an *epimorphism*, so $\exists\ b \in B$ such that $\beta(b) = c$.

Now, define $\beta' : C \to B$ such that $\beta'(c) = b - \alpha\alpha'(b)$.

First we show that β' is well defined.

Let $c, c' \in C$ such that $c = c'$.

Since β is an *epimorphism* so $\exists\ b,\ b' \in B$ such that $\beta(b) = c$ and $\beta(b') = c'$.

Then, $\beta'(c) = b - \alpha\alpha'(b)$ and $\beta'(c') = b' - \alpha\alpha'(b')$.

$$\begin{aligned} \text{Now, } \beta(b - b') &= \beta(b) - \beta(b') \text{ (since } \beta \text{ is a homomorphism).} \\ &= c - c' \\ &= c - c \\ &= 0 \end{aligned}$$

$\implies b - b' \in ker\beta = Im\alpha.$

Thus, $b - b' = \alpha(a)$ for some $a \in A$.

$$\begin{aligned} \text{Now, } \alpha\alpha'(b - b') &= \alpha\alpha'(\alpha(a)) \\ &= \alpha(\alpha'(\alpha(a))) \\ &= \alpha(\alpha'\alpha(a)) \\ &= \alpha(1_A(a)) \\ &= \alpha(a) \\ &= b - b' \end{aligned}$$

$\implies \alpha\alpha'(b) - \alpha\alpha'(b') = b - b'$ (since $\alpha\alpha'$ is a homomorphism).

$\implies b - \alpha\alpha'(b) = b' - \alpha\alpha'(b').$

$\implies \beta'(c) = \beta'(c')$

Hence β' is well defined.

Also we have, for each $c \in C$, $c = \beta(b)$ and $\beta'(c) = b - \alpha\alpha'(b)$.

$$\begin{aligned} \text{Now, } \beta\beta'(c) &= \beta(b - \alpha\alpha'(b)) \\ &= \beta(b) - \beta(\alpha\alpha'(b)) \\ &= \beta(b) - \beta\alpha(\alpha'(b)) \\ &= c - 0 \text{ as } Im\alpha = ker\beta \text{ so } \beta\alpha = 0 \\ &= c. \end{aligned}$$

i.e., $\beta\beta'(c) = c.$

Hence, $\beta\beta' = 1_C$ which is (ii).

2nd part

Conversely, suppose (ii) holds. Let $b \in B$ then

$\beta(b - \beta'\beta(b)) = \beta(b) - \beta\beta'\beta(b)$

$= \beta(b) - 1_C\beta(b)$, (since $\beta\beta' = 1_C$)

$= \beta(b) - \beta(b)$

$= 0.$

Therefore, $b - \beta'\beta(b) \in ker\beta = Im\alpha.$

Which implies $b - \beta'\beta(b) = \alpha(a)$ for some $a \in A$.

Now define $\alpha' : B \to A \; by \; \alpha'(b) = a.$

We show that α' is well defined.

Let b, $b' \in B$ such that $b = b'$.

Since $b - \beta'\beta(b)$, $b' - \beta'\beta(b') \in ker\beta = Im\alpha.$

Then $b - \beta'\beta(b) = \alpha(a)$ and $b' - \beta'\beta(b') = \alpha(a')$ for some $a, a' \in A$.

Thus $\alpha'(b) = a$ and $\alpha'(b') = a'$.

Now, $b - \beta'\beta(b) = b' - \beta'\beta(b')$ as $b = b'$.

$\implies \alpha(a) = \alpha(a')$.

$\implies a = a'$ (since α is a monomorphism).

$\implies \alpha'(b) = \alpha'(b')$.

Thus α' is well defined.

Also for each $a \in A$,

$\alpha'\alpha(a) = \alpha'(b - \beta'\beta(b))$

$= \alpha'(b) - \alpha'(\beta'\beta(b))$

$= a - 0 = a.$

(since $\beta'\beta(b) - \beta'\beta(\beta'\beta(b)) = \beta'\beta(b) - \beta' I_C(\beta(b)) = \beta'\beta(b) - \beta'\beta(b) = 0 = \alpha(0)$ so $\alpha'(\beta'\beta(b)) = 0$)

Which implies that $\alpha'\alpha = 1_A$.

Thus (i) holds.

Hence the theorem.

Theorem: Let $0 \longrightarrow A \underset{\alpha'}{\overset{\alpha}{\rightleftarrows}} B \underset{\beta'}{\overset{\beta}{\rightleftarrows}} C \longrightarrow 0$ be a split short exact sequence of R-*modules* and R-*homomorphism* with $\alpha'\alpha = 1_A$ and $\beta\beta' = 1_C$ then show that

$0 \longleftarrow A \underset{\alpha'}{\longleftarrow} B \underset{\beta'}{\longleftarrow} C \longleftarrow 0$ is an exact sequence.

Proof: Here we have to show that,

(i) β' is a monomorphism,

(ii) α' is an epimorphism,

and (iii) $ker\ \alpha' = Im\ \beta'$

(i) We show that β' is a monomorphism, i.e., $ker\beta' = \{0\}$. Let $c \in ker\beta'$ then $\beta'(c) = 0$.

Since $\beta\beta' = 1_C$ so we have $\beta\beta'(c) = 1_C(c) = c$.

Also, $\beta\beta'(c) = \beta(\beta'(c)) = \beta(0) = 0$.

Which implies $c = 0$.

Thus $ker\beta' = \{0\}$.

Hence β' is a monomorphism.

(ii) We show that α' is an epimorphism. Since $\alpha'\alpha = 1_A$, then for any $a \in A$ we have,

$a = 1_A(a) = \alpha'\alpha(a) = \alpha'(\alpha(a))$.

Since for every $a \in A$ there exists $\alpha(a) \in B$ such that $a = \alpha'(\alpha(a))$. Hence α' is an epimorphism.

(iii) Let $b \in ker\alpha' \subset B$ then $b \in B$ and $\alpha'(b) = 0$.

Also $\beta(b) = c$ for some $c \in C$.

Thus, $\beta'\beta(b) = \beta'(c)$

$= b - \alpha\alpha'(b)$ [By the def^n of β']

i.e., $\beta'\beta(b) = b - \alpha(0) = b - 0 = b$.

i.e., $\beta'(c) = b \implies b \in Im\beta'$

Therefore, $ker\alpha' \subseteq Im\beta' \cdots\cdots\cdots\cdots(1)$

Again, let $b \in Im\ \beta'$ then $\beta'(c) = b$ for some $c \in C$.

Now, $\alpha'(b) = \alpha'(\beta'(c))$

$= \alpha'(b - \alpha\alpha'(b))$ [from the definition of β' we have $\beta'(c) = b - \alpha\alpha'(b)$]

$= \alpha'(b) - \alpha'(\alpha\alpha'(b))$

$= \alpha'(b) - (\alpha'\alpha)(\alpha'(b))$

$= \alpha'(b) - 1_A(\alpha'(b))$

$= \alpha'(b) - \alpha'(b)$

$= 0$

Hence $b \in ker\alpha'$

Which implies that $Im\beta' \subseteq ker\alpha' \cdots\cdots\cdots\cdots(2)$

From (1) and (2), we have $Im\beta' = ker\alpha'$

Hence, the sequence is exact. [proved]

Internal and External Direct Sum

Internal Direct Sum: Let A and B be two sub-modules of a left R-module M. If $A \cap B = \{0\}$, zero sub-module, then the set $\{a + b : a \in A \text{ and } b \in B\}$ is called the internal direct sum of A and B.

Similarly, we can define the internal direct sum of a finite number of sub-modules of a left R-module. Thus if $A_1, A_2, \ldots, A_n$ are sub-modules of a left R-module M such that for each A_j, $A_j \cap (\cup_{i \neq j} A_i) = \{0\}$, then their internal direct sum is the set $\{\sum_{i=1}^{n} a_i : a_i \in A_i\}$.

External Direct Sum: The external direct sum $A_1 \oplus A_2$ of two R-modules A_1 and A_2 is the R-module consisting of all ordered pairs (a_1, a_2), for $a_i \in A_i$, with the module operations defined by

$$(a_1, a_2) + (a'_1, a'_2) = (a_1 + a'_1, a_2 + a'_2) \text{ and } r(a_1, a_2) = (ra_1, ra_2).$$

Theorem: Let M_1 and M_2 be two sub-modules of a left R-module M such that.

(i) $M_1 \cap M_2 = \{0\}$ and

(ii) if $m \in M$, $m_1 \in M_1$, $m_2 \in M_2$ such that $m = m_1 + m_2$,

then $M \cong M_1 \oplus M_2$.

Proof: Let us define a map $f : M \to M_1 \oplus M_2$ given by

$$f(m) = (m_1, m_2), \text{ where } m = m_1 + m_2.$$

We show that f is well defined.

Let $m, m' \in M$ such that $m = m'$. Then $m = m_1 + m_2$ and $m' = m'_1 + m'_2$ where $m_1, m'_1 \in M_1$; $m_2, m'_2 \in M_2$ and $f(m) = (m_1, m_2)$, $f(m') = (m'_1, m'_2)$.

Now, $m = m'$

$$\implies m_1 + m_2 = m'_1 + m'_2$$

$$\implies m_1 - m'_1 = m'_2 - m_2$$

But $m_1 - m'_1 \in M_1$ and $m'_2 - m_2 \in M_2$.

Since $M_1 \cap M_2 = \{0\}$ then we have,

$$m_1 - m'_1 = 0 = m_2 - m'_2$$

Which implies that, $m_1 = m'_1$ and $m_2 = m'_2$.

i.e., $(m_1, m_2) = (m_1', m_2')$

$$\implies f(m) = f(m').$$

Hence f is well defined.

Now, we show that f is a homomorphism.

Let $m, m' \in M$, then $m = m_1 + m_2$ and $m' = m_1' + m_2'$ where $m_1, m_1' \in M_1$; $m_2, m_2' \in M_2$ and $f(m) = (m_1, m_2)$, $f(m') = (m_1', m_2')$.

Now, $m + m' = (m_1 + m_2) + (m_1' + m_2') = (m_1 + m_1') + (m_2 + m_2')$ where $(m_1 + m_1') \in M_1$ and $(m_2 + m_2') \in M_2$.

Therefore, $f(m + m') = (m_1 + m_1', m_2 + m_2') = (m_1, m_2) + (m_1', m_2') = f(m) + f(m')$.

Also, for any $r \in R$, $rm = rm_1 + rm_2$ where $rm_{\in} M_1$ and $rm_2 \in M_2$.

Therefore, $f(rm) = (rm_1, rm_2) = r(m_1, m_2) = rf(m)$.

Thus f is an R-homomorphism.

Next, we show that f is a monomorphism.

Let $m, m' \in M$, then $m = m_1 + m_2$ and $m' = m_1' + m_2'$ where $m_1, m_1' \in M_1$; $m_2, m_2' \in M_2$ and $f(m) = (m_1, m_2)$, $f(m') = (m_1', m_2')$.

Let $f(m) = f(m')$, then we have,

$$(m_1, m_2) = (m_1', m_2')$$

$$\implies m_1 = m_1' \text{ and } m_2 = m_2'$$

Thus $m = m_1 + m_2 = m_1' + m_2' = m'$.

Hence f is a monomorphism.

Finally, we show that f is an epimorphism.

For any $(m_1, m_2) \in M_1 \oplus M_2$ there exist an element $m \in M$ such that $(m_1, m_2) = f(m)$, where $m_1 + m_2 = m$.

Thus f is an epimorphism.

Hence f is an isomorphism.

i.e., $M \cong M_1 \oplus M_2$ [**proved**]

Theorem: Let A and B are sub-modules of an R-module with $A \cap B = \{0\}$ then there is a split short exact sequence $0 \longrightarrow A \underset{\pi_2}{\overset{i_1}{\rightleftarrows}} A \oplus B \underset{i_2}{\overset{\pi_1}{\rightleftarrows}} B \longrightarrow 0.$

Proof: Let $a \in A$ and $b \in B$, then we define $i_1(a) = (a, 0)$ and $i_2(b) = (0, b)$. Also define π_1 and π_2 by $\pi_1(a, b) = b$ and $\pi_2(a, b) = a$. Then clearly i_1, i_2, π_1, π_2 are well defined and are all R-homomorphism.

Here we have to show that,

(i) i_1 is a monomorphism,

(ii) π_1 is an epimorphism,

(iii) $ker\ \pi_1 = Im\ i_1$

(iv) $\pi_2 i_1 = 1_A$

and (v) $\pi_1 i_2 = 1_B$.

(i) Let $i_1(a_1) = i_1(a_2)$ for some $a_1, a_2 \in A$. Then

$(a_1, 0) = (a_2, 0)$

$\implies a_1 = a_2$.

Thus i_1 is a monomorphism.

(ii) Let $b \in B$ then $b = \pi_1(a, b)$ for some $(a, b) \in A \oplus B$.

Thus π_1 is an epimorphism.

(iii) Let $(a, b) \in ker\ \pi_1$, then

$\pi_1(a, b) = 0$

$\implies b = 0$

Therefore, $(a, b) = (a, 0) = i_1(a)$ for some $a \in A$.

$\implies (a, b) \in Im\ i_1$

Thus $ker\ \pi_1 \subseteq Im\ i_1 \cdots\cdots\cdots\cdots (1)$

Again, let $(a, b) \in Im\ i_1$, then there exists $a \in A$ such that

$i_1(a) = (a, b)$

$\implies (a, 0) = (a, b)$

$\implies b = 0$

Now, $\pi_1(a, b) = b = 0$

$\implies (a, b) \in ker\ \pi_1$
Thus $Im\ i_1 \subseteq ker\ \pi_1 \cdots\cdots\cdots\cdots(2)$

From (1) and (2) we have $ker\ \pi_1 = Im\ i_1$.

Hence the given sequence is a short exact sequence.

(iv) For any $a \in A$, $\pi_2 i_1(a) = \pi_2(a, 0) = a$

$\implies \pi_2 i_1 = 1_A$.

(v) For any $b \in B$, $\pi_1 i_2(b) = \pi_1(0, b) = b$

$\implies \pi_1 i_2 = 1_B$.

Thus the sequence is split shot exact sequence.

Hence proved.

Note: For the sequence $0 \longrightarrow A \underset{\pi_2}{\overset{i_1}{\rightleftarrows}} A \oplus B \underset{i_2}{\overset{\pi_1}{\rightleftarrows}} B \longrightarrow 0$, we have the following:

(i) $\pi_2 i_1 = 1_A$,

(ii) $\pi_1 i_2 = 1_B$,

(iii) $\pi_1 i_1 = 0$,

(iv) $\pi_2 i_2 = 0$,

(v) $i_1\pi_2 + i_2\pi_1 = 1_{A\oplus B}$.

Proof: (i) and (ii) is clear from the previous theorem.

(iii) For any $a \in A$, $\pi_1 i_1(a) = \pi_1(a, 0) = 0 = 0(a)$. Thus $\pi_1 i_1 = 0$.

(iv) For any $b \in B$, $\pi_2 i_2(b) = \pi_2(0, b) = 0 = 0(b)$. Thus $\pi_2 i_2 = 0$.

(v) For any $(a, b) \in A \oplus B$, $(i_1\pi_2 + i_2\pi_1)(a, b) = i_1\pi_2(a, b) + i_2\pi_1(a, b)$

$= i_1(a) + i_2(b)$.

$= (a, 0) + (0, b) = (a, b)$.

Hence $i_1\pi_2 + i_2\pi_1 = 1_{A\oplus B}$.

Theorem: Let $0 \longrightarrow A \underset{\alpha'}{\overset{\alpha}{\rightleftarrows}} B \underset{\beta'}{\overset{\beta}{\rightleftarrows}} C \longrightarrow 0$ be a split short exact sequence of *R-modules* and *R-homomorphisms*, then $B \cong A \oplus C$.

Proof: Since $0 \longrightarrow A \underset{\alpha'}{\overset{\alpha}{\rightleftarrows}} B \underset{\beta'}{\overset{\beta}{\rightleftarrows}} C \longrightarrow 0$ is a split short exact sequence of *R-modules* and *R-homomorphisms*, then there exist an R-homomorphism $\alpha' : B \to A$ such that $\alpha'\alpha = 1_A$.

If we define $\beta' : C \to B$ by $\beta'(c) = b - \alpha'\alpha(b)$, where $b \in B$ such that $\beta(b) = c$, then clearly β' is well defined and also β' is an R-homomorphism and $\beta\beta' = 1_C$.

Now, define $\phi : B \to A \oplus C$ by $\phi(b) = (\alpha'(b), \beta(b))$ and also define $\psi : A \oplus C \to B$ by $\psi(a, c) = \alpha(a) + \beta'(c)$.

Then clearly ϕ and ψ are both R-homomorphisms.

Now let $b \in B$ then $\psi\phi(b) = \psi(\alpha'(b), \beta(b))$

$= \alpha(\alpha'(b)) + \beta'(\beta(b))$

$= \alpha\alpha'(b) + \beta'\beta(b)$

$= \alpha\alpha'(b) + \beta'(c)$

$= \alpha\alpha'(b) + b - \alpha\alpha'(b) = b$

$\implies \psi\phi(b) = b$

$\implies \psi\phi = 1_B$.

Again, let $(a, c) \in A \oplus C$ then,

$\phi\psi(a, c) = \phi(\alpha(a) + \beta'(c))$

$= (\alpha'(\alpha(a) + \beta'(c)), \beta(\alpha(a) + \beta'(c))$

$= (\alpha'\alpha(a) + \alpha'\beta'(c), \beta\alpha(a) + \beta\beta'(c))$

$= (1_A(a) + 0, 0 + 1_C(c))$ [Since $Im\beta' = ker\alpha'$ so $\alpha'\beta' = 0$ and $Im\alpha = ker\beta$ So $\beta\alpha = 0$]

$= (a, c)$

$\implies \phi\psi = 1_{A\oplus C}$

Thus ϕ and ψ are inverse of each other. i.e., ϕ and ψ are one-one and onto.

Hence $B \cong A \oplus C$.

Commutative Diagram: The diagram of R-module and R-homomorphism of the form

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & A' & \xrightarrow{\alpha'} & B' & \xrightarrow{\beta'} & C' & \longrightarrow & 0 \end{array}$$

is said to be commutative if $\alpha' f = g\alpha : A \to B'$ and $\beta' g = h\beta : B \to C'$.

Theorem: State and prove the Short Five Lemma.

Statement: If the commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{\alpha} & B & \xrightarrow{\beta} & C & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle g} & & \downarrow{\scriptstyle h} & & \\ 0 & \longrightarrow & A' & \xrightarrow{\alpha'} & B' & \xrightarrow{\beta'} & C' & \longrightarrow & 0 \end{array}$$

of R-modules and R-homomorphism has both rows exact, then

(i) if f and h are isomorphisms then g is an isomorphism;

(ii) if f and h are monomorphisms then g is a monomorphism;

(iii) if f and h are epimorphisms then g is an epimorphism.

Proof:
It is clear that (ii) and (iii) implies (i). Thus we only prove (ii) and (iii).

(ii) Let f and h are monomorphisms. We have to show that g is a monomorphism. i.e., $ker g = \{0\}$.

So let $b \in ker g$ then $g(b) = 0$.

Now, $\beta' g(b) = \beta'(0) = 0$.

$\implies h\beta(b) = 0$ (by the commutativity of the diagram).

Since h is a monomorphism, so $\beta(b) = 0$.

$\implies b \in ker\beta = Im\alpha$ (by the exactness of the top row).

Which shows that $b = \alpha(a)$ for some $a \in A$.

Now, $g(b) = g\alpha(a) = \alpha' f(a)$ (by the commutativity of the diagram).

$\implies \alpha' f(a) = 0$ (since $g(b) = 0$).

Since α' is a monomorphism, so we have $f(a) = 0$.

Since f is a monomorphism, so $a = 0$.

Therefore $b = \alpha(0) = 0$ implies $ker g = \{0\}$.

Which shows that g is a monomorphism.

Which is (i).

(ii) Let f and h are epimorphisms.

Let $b' \in B'$. Now $\beta'(b') = h(c)$ for some $c \in C$.

Since h is an epimorphism and β is an epimorphism so $c = \beta(b)$ for some $b \in B$.

Hence $\beta'(b') = h\beta(b)$.

$= \beta' g(b)$ [By the commutativity of the diagram].

So we have, $\beta'(b' - g(b)) = 0$.

$\implies b' - g(b) \in ker\beta' = Im\alpha'$ [By the exactness of the botttom row]

$\implies b' - g(b) = \alpha'(a')$; for some $a' \in A'$.

$= \alpha' f(a)$; for some $a \in A$ (since f is an epimorphism).

$= g\alpha(a)$ [By the commutativity of the diagram].

$\implies b' = g(b) + g\alpha(a) = g(b + \alpha(a))$.

Which implies that $b' \in Img$ where $b + \alpha(a) \in B$.

Hence g is epimorphism.

Which proves (ii).

Hence the theorem.

Theorem: State and prove the Five Lemma.

Statement: If the commutative diagram

$$\begin{array}{ccccccccc} A_1 & \xrightarrow{\alpha_1} & A_2 & \xrightarrow{\alpha_2} & A_3 & \xrightarrow{\alpha_3} & A_4 & \xrightarrow{\alpha_4} & A_5 \\ \downarrow{\lambda_1} & & \downarrow{\lambda_2} & & \downarrow{\lambda_3} & & \downarrow{\lambda_4} & & \downarrow{\lambda_5} \\ B_1 & \xrightarrow{\beta_1} & B_2 & \xrightarrow{\beta_2} & B_3 & \xrightarrow{\beta_3} & B_4 & \xrightarrow{\beta_4} & B_5 \end{array}$$

of R-modules and R-homomorphism has both rows exact, then

(i) if λ_1 is an epimorphism and λ_2, λ_4 are monomorphisms then λ_3 is a monomorphism;

(ii) if λ_5 is a monomorphism and λ_2, λ_4 are epimorphisms then λ_3 is an epimorphism;

(iii) if λ_1,λ_2, λ_4, λ_5 are isomorphisms then λ_3 is an isomorphism.

Proof: (i) Here given that λ_1 is an epimorphism and λ_2, λ_4 are monomorphisms. Now, we show that λ_3 is a monomorphism or equivalently $ker\lambda_3 = \{0\}$.

So let $a_3 \in ker\lambda_3$, then $a_3 \in A_3$ such that

$\lambda_3(a_3) = 0 \cdots\cdots\cdots\cdots\cdots (1)$

Thus we have, $\beta_3\lambda_3(a_3) = \beta_3(0) = 0$

$\implies \lambda_4\alpha_3(a_3) = 0$ (by the commutativity of the diagram)

Since λ_4 is a monomorphism so $\alpha_3(a_3) = 0$

$\implies a_3 \in ker\alpha_3 = Im\alpha_2$ (by the exactness of the top row)

$\implies a_3 \in Im\alpha_2$

$\implies a_3 = \alpha_2(a_2)$ for some $a_2 \in A_2$

Now from (1), $\lambda_3(a_3) = 0$

$\implies \lambda_3(\alpha_2(a_2)) = 0$

$\implies \lambda_3\alpha_2(a_2) = 0$

$\implies \beta_2\lambda_2(a_2) = 0$ (by the commutativity of the diagram)

$\implies \lambda_2(a_2) \in ker\beta_2 = Im\beta_1$ (by the exactness of the bottom row)

$\implies \lambda_2(a_2) \in Im\beta_1$

$\implies \lambda_2(a_2) = \beta_1(b_1)$ for some $b_1 \in B_1$

Also since λ_1 is epimorphism so $b_1 = \lambda_1(a_1)$ for some $a_1 \in A_1$

i.e., $\lambda_2(a_2) = \beta_1\lambda_1(a_1) = \lambda_2\alpha_1(a_1)$ (by the commutativity of the diagram)

$\implies \lambda_2(a_2) - \lambda_2\alpha_1(a_1) = 0$

$\implies \lambda_2(a_2 - \alpha_1(a_1)) = 0$

Since λ_2 is a monomorphism, so we have , $a_2 - \alpha_1(a_1) = 0$

$\implies a_2 = \alpha_1(a_1)$

Now, $a_3 = \alpha_2(a_2) = \alpha_2(\alpha_1(a_1)) = \alpha_2\alpha_1(a_1) = 0$ (since $Im\alpha_1 = ker\alpha_2$, then $\alpha_2\alpha_1 = 0$)

$\implies a_3 = 0$

Thus we have, $a_3 \in ker\lambda_3 \implies a_3 = 0$

Thus $ker\lambda_3 = \{0\}$ and hence λ_3 is monomorphism.

This proves (i).

Proof: (ii): Let λ_5 be a monomorphism and λ_2, λ_4 are epimorphisms. We show that λ_3 is an epimorphism.

Let $b_3 \in B_3$ then $\beta_3(b_3) \in B_4$.

Since λ_4 is epimorphism, then $\beta_3(b_3) = \lambda_4(a_4)$ for some $a_4 \in A_4$.

$\implies \beta_4\beta_3(b_3) = \beta_4\lambda_4(a_4)$

But $\beta_4\beta_3(b_3) = 0$ as $ker\beta_4 = Im\beta_3$

Thus $\beta_4\lambda_4(a_4) = 0$

$\implies \lambda_5\alpha_4(a_4) = 0$ (by the commutativity of the diagram)

Since λ_5 is a monomorphism, we have $\alpha_4(a_4) = 0$

$\implies a_4 \in ker\ \alpha_4 = Im\alpha_3$ (by the exactness of the top row)

$\implies a_4 = \alpha_3(a_3)$ for some $a_3 \in A_3$

Now, we have $\beta_3(b_3) = \lambda_4(a_4) = \lambda_4(\alpha_3(a_3)) = \beta_3\lambda_3(a_3)$ (by the commutativity of the diagram)

$\implies \beta_3(b_3 - \lambda_3(a_3)) = 0$

$\implies b_3 - \lambda_3(a_3) \in ker\beta_3 = Im\beta_2$ (by the exactness of the bottom row)

Thus we have, $b_3 - \lambda_3(a_3) = \beta_2(b_2)$ for some $b_2 \in B_2$

Since λ_2 is an epimorphism, we have $b_2 = \lambda_2(a_2)$ for some $a_2 \in A_2$

Thus $b_3 - \lambda_3(a_3) = \beta_2\lambda_2(a_2) = \lambda_3\alpha_2(a_2)$ (by the exactness of the top row)

$\implies b_3 = \lambda_3(a_3 + \alpha_2(a_2))$.

Since $a_3 + \alpha_2(a_2) \in A_3$, therafore λ_3 is an epimorphism.
This proves (ii).

Proof: (iii) Since λ_1, λ_2, λ_4 and λ_5 are isomorphisms. So by (i) λ_3 is a monomorphism and by (ii) λ_3 is an epimorphism.

Hence λ_3 is an isomorphism.

This proves (ii).

Hence the theorem is proved.

Theorem: State and prove the Strong Four Lemma.

Statement: If the commutative diagram

$$\begin{array}{ccccccc} A_1 & \xrightarrow{\alpha_1} & A_2 & \xrightarrow{\alpha_2} & A_3 & \xrightarrow{\alpha_3} & A_4 \\ \downarrow{\scriptstyle \gamma_1} & & \downarrow{\scriptstyle \gamma_2} & & \downarrow{\scriptstyle \gamma_3} & & \downarrow{\scriptstyle \gamma_4} \\ B_1 & \xrightarrow{\beta_1} & B_2 & \xrightarrow{\beta_2} & B_3 & \xrightarrow{\beta_3} & B_4 \end{array}$$

of R-modules and R-homomorphism has both rows exact. And if γ_1 is an epimorphism and γ_4 is a monomorphisms, then

(i) $ker\gamma_3 = \alpha_2(ker\gamma_2)$

(ii) $Im\gamma_2 = \beta_2^{-1}(Im\gamma_3)$ or, $\beta_2(Im\gamma_2) = Im\gamma_3$.

Proof: (i): Let $a_3 \in ker\gamma_3$.
Then $\gamma_3(a_3) = 0$.
$\implies \beta_3\gamma_3(a_3) = \beta_3(0) = 0$.
$\implies \gamma_4\alpha_3(a_3) = 0$ (since $\beta_3\gamma_3 = \gamma_4\alpha_3$).
$\implies \alpha_3(a_3) = 0$ (ince γ_4 is a monomorphism).
$\implies a_3 \in ker\alpha_3 = Im\alpha_2$.
$\implies a_3 = \alpha_2(a_2)$, for some $a_2 \in A_2$.
Now, $\gamma_3(a_3) = 0$.
$\implies \gamma_3\alpha_2(a_2) = 0$.
$\implies \beta_2\gamma_2(a_2) = 0$ (since $\gamma_3\alpha_2 = \beta_2\gamma_2$).
$\implies \gamma_2(a_2) \in ker\beta_2 = Im\beta_1$.
$\implies \gamma_2(a_2) = \beta_1(b_1)$ for some $b_1 \in B_1$.
$\implies \gamma_2(a_2) = \beta_1\gamma_1(a_1)$ (since γ_1 is an epimorphism, $b_1 = \gamma_1(a_1)$ for some $a_1 \in A_1$).
$\implies \gamma_2(a_2) = \gamma_2\alpha_1(a_1)$ (since $\beta_1\gamma_1 = \gamma_2\alpha_1$).
$\implies \gamma_2(a_2 - \alpha_1(a_1)) = 0$.
$\implies a_2 - \alpha_1(a_1) \in ker\gamma_2$.
$\implies \alpha_2(a_2 - \alpha_1(a_1)) \in \alpha_2 ker\gamma_2$.
$\implies (\alpha_2(a_2) - \alpha_2\alpha_1(a_1)) \in \alpha_2 ker\gamma_2$.
$\implies (a_3 - 0) \in \alpha_2 ker\gamma_2$ (since $\alpha_2\alpha_1 = 0$ and $\alpha_2(a_2) = a_3$).
$\implies a_3 \in \alpha_2(ker\gamma_2)$.
Thus $ker\gamma_3 \subset \alpha_2(ker\gamma_2) \cdots\cdots\cdots (A)$

Conversely let $a_3 \in \alpha_2(ker\gamma_2)$, then $a_3 = \alpha_2(a_2)$ for some $a_2 \in ker\gamma_2$.
Now, $a_2 \in ker\gamma_2$ implies $\gamma_2(a_2) = 0$.
$\implies \beta_2\gamma_2(a_2) = \beta_2(0) = 0$.

$\implies \gamma_3\alpha_2(a_2) = 0$ (since $\beta_2\gamma_2 = \gamma_3\alpha_2$).
$\implies \alpha_2(a_2) \in ker\gamma_3$.
$\implies a_3 \in ker\gamma_3$ (since $a_3 = \alpha_2(a_2)$).

Thus $\alpha_2(ker\gamma_2) \subset ker\gamma_3 \cdots\cdots\cdots (B)$

Hence from (A) and (B) we have $ker\gamma_3 = \alpha_2(ker\gamma_2)$. Which proves (i).

Proof: (ii):
We show that $Im\gamma_2 = \beta_2^{-1}(Im\gamma_3)$ or, $\beta_2(Im\gamma_2) = Im\gamma_3$.

Let $b_3 \in \beta_2(Im\gamma_2)$, then $b_3 = \beta_2(b_2)$ for some $b_2 \in Im\gamma_2$.
Now, $b_2 \in Im\gamma_2$, implies $b_2 = \gamma_2(a_2)$ for some $a_2 \in A_2$.
Therefore, $b_3 = \beta_2(b_2) = \beta_2\gamma_2(a_2) = \gamma_3\alpha_2(a_2)$ (since $\beta_2\gamma_2 = \gamma_3\alpha_2$)
$\implies b_3 \in Im\gamma_3$.
Thus $\beta_2(Im\gamma_2) \subset Im\gamma_3$
$\implies Im\gamma_2 \subset {\beta_2}^{-1}(Im\gamma_3) \cdots\cdots\cdots (C)$

Conversely let $b_2 \in {\beta_2}^{-1}(Im\gamma_3)$.
$\implies \beta_2(b_2) \in Im\gamma_3$.
$\implies \beta_2(b_2) = \gamma_3(a_3)$ for some $a_3 \in A_3$.
$\implies \gamma_3(a_3) = \beta_2(b_2)$.
$\implies \beta_3\gamma_3(a_3) = \beta_3\beta_2(b_2)$.
$\implies \beta_3\gamma_3(a_3) = 0$ (since $\beta_3\beta_2 = 0$).
$\implies \gamma_4\alpha_3(a_3) = 0$ (since $\beta_3\gamma_3 = \gamma_4\alpha_3$).
$\implies \alpha_3(a_3) = 0$ (since γ_4 is a monomorphism).
$\implies a_3 \in ker\alpha_3 = Im\alpha_2$.
$\implies a_3 = \alpha_2(a_2)$ for some $a_2 \in A_2$.
Now, $\beta_2(b_2) = \gamma_3(a_3)$.
$\implies \beta_2(b_2) = \gamma_3\alpha_2(a_2)$ (since $a_3 = \alpha_2(a_2)$).
$\implies \beta_2(b_2) = \beta_2\gamma_2(a_2)$ (since $\gamma_3\alpha_2 = \beta_2\gamma_2$).
$\implies \beta_2(b_2 - \gamma_2(a_2)) = 0$.
$\implies (b_2 - \gamma_2(a_2)) \in ker\beta_2 = Im\beta_1$.
$\implies (b_2 - \gamma_2(a_2)) = \beta_1(b_1)$ for some $b_1 \in B_1$.
$\implies (b_2 - \gamma_2(a_2)) = \beta_1\gamma_1(a_1)$ (since γ_1 is an epimorphism $b_1 \in B_1 \implies b_1 = \gamma_1(a_1)$ for some $a_1 \in A_1$).
$\implies (b_2 - \gamma_2(a_2)) = \gamma_2\alpha_1(a_1)$ (since $\beta_1\gamma_1 = \gamma_2\alpha_1$).
$\implies b_2 = \gamma_2(a_2) + \gamma_2\alpha_1(a_1)$.
$\implies b_2 = \gamma_2(a_2 + \alpha_1(a_1))$.
$\implies b_2 \in Im\gamma_2$.
Thus ${\beta_2}^{-1}(Im\gamma_3) \subset Im\gamma_2 \cdots\cdots\cdots (D)$.
From (C) and (D) we have, ${\beta_2}^{-1}(Im\gamma_3) = Im\gamma_2$
or, $\beta_2(Im\gamma_2) = Im\gamma_3$. Which proves (ii).