Notes on Group Theory - II & Linear Algebra - II (Core Course - XII)

Books followed: 1. Higher Algebra (Abstract and Linear) - S. K. Mapa
2. Contemporary Abstract Algebra - Joseph Gallian
~~3. Topics Fundamentals of Abstract Algebra - D.S. Malik, Shamik Ghosh & Parthasarathi Mukhopadhyay~~
3. Fundamentals of Abstract Algebra - D.S. Malik, John M. Mordeson and M. K. Sen
4. Topics in Abstract Algebra - M.K. Sen, Shamik Ghosh & Parthasarathi Mukhopadhyay
5. A first course in Abstract Algebra - J. B. Fraleigh

Unit - 1 : Group theory :

1.1 Definition of Automorphism : An isomorphism of a group G onto itself is said to be an automorphism of G.

Examples 1.1.1 : 1. Let G be a group. The identity mapping on G is an automorphism of G. This is called the identity automorphism and is denoted by I_G.

2. Let G be an abelian group and the mapping $\phi: G \to G$ is defined by $\phi(a) = a^{-1}$, $a \in G$. Then ϕ is an automorphism.

3. Let $G = (\mathbb{C}, +)$ and the mapping $\phi: G \to G$ is defined by $\phi(z) = \bar{z}$, $z \in \mathbb{C}$ ($\mathbb{C}$ is the set of all complex numbers). Then ϕ is an automorphism.

Theorem 1.1.2 The set of all automorphisms of a group forms a group under the mapping composition.

Proof: Let G be a group and let $Aut(G)$ be the set of all automorphisms of G.

(i) Let $\alpha, \beta \in Aut(G)$. So, α and β are two automorphisms of G. As the mapping α, β are both bijective, $\alpha \circ \beta$ is also bijective. Again, since α, β are both isomorphisms, $\alpha \circ \beta$ is an isomorphism. So, $\alpha \circ \beta$ is an automorphism. So, $\alpha, \beta \in Aut(G) \Rightarrow \alpha \circ \beta \in Aut(G)$

(ii) The composition of mapping is associative

(iii) The identity automorphism I_G is the identity element.

(iv) Let $\alpha \in Aut(G)$. Then α is bijective. So, α^{-1} exists and α^{-1} is bijective. As α is isomorphism, so, α^{-1} is also an isomorphism. Hence $\alpha^{-1} \in Aut(G)$. So, $(Aut(G), \circ)$ is a group.

Theorem 1.1.3 Let G be a group and the mapping $\alpha : G \to G$ is defined by $\alpha(x) = x^{-1}$, $x \in G$. Then α is an automorphism if and only if G is abelian.

Proof: Let G be abelian. To prove that α is an automorphism, we have to prove that α is a bijection and α is a homomorphism.

α is injective as $\alpha(x_1) = \alpha(x_2) \Rightarrow x_1^{-1} = x_2^{-1} \Rightarrow x_1 = x_2$.

α is surjective as for each element $y \in G$, we have $y^{-1} \in G$ and $f(y^{-1}) = (y^{-1})^{-1} = y$

So, α is a bijective mapping.

Let $x, y \in G$. Then $\alpha(xy) = (xy)^{-1} = y^{-1}x^{-1} = x^{-1}y^{-1}$ (as G is abelian)

So, $\alpha(xy) = \alpha(x)\alpha(y)$. Hence α is a homomorphism

So, α is an automorphism.

Conversely, let α be an automorphism of G, and let $x, y \in G$

Then $\alpha(xy) = \alpha(x)\alpha(y)$. So, $(xy)^{-1} = x^{-1}y^{-1}$

or, $((xy)^{-1})^{-1} = (x^{-1}y^{-1})^{-1}$ or, $xy = (y^{-1})^{-1}(x^{-1})^{-1} = yx$

Hence $xy = y$ for all $x, y \in G$. So, G is abelian.

Theorem 1.1.4 Let G be a group and $g \in G$. Then the mapping $I_g : G \to G$ defined by $I_g(x) = gxg^{-1}$, $x \in G$ is an automorphism.

Proof: I_g is injective as $I_g(x_1) = I_g(x_2)$

$$\Rightarrow gx_1g^{-1} = gx_2g^{-1}$$

$$\Rightarrow x_1 = x_2 \quad \text{(by cancellation law}$$

I_g is surjective as for any element $y \in G$, we have $g^{-1}yg \in G$ such that $f(g^{-1}yg) = g(g^{-1}yg)g^{-1} = y$

Now let $x, y \in G$, then $I_g(xy) = gxyg^{-1} = (gxg^{-1})(gyg^{-1}) = I_g(x)I_g(y)$

So, I_g is a homomorphism. So, I_g is an automorphism of G.

Note 1.1.5 If $g \in Z(G)$ (the centre of the group G) then I_g is the identity automorphism as $I_g(x) = gxg^{-1} = xgg^{-1}$ (as $g \in Z(G)$ $gx = xg$ for $x \in G$)

$$= x \quad , \text{ for } x \in G.$$

Definition 1.1.6 The automorphism I_g defined by $I_g(x) = gxg^{-1}, x \in G$ is said to the inner automorphism determined by g.

The set of all inner automorphisms of G is denoted by $Inn(G)$

Theorem 1.1.7 G is a commutative group if and only if $I_g = I_G$ for $g \in G$

Proof: Let G be a commutative group and let $g \in G$.

Then $I_g(x) = gxg^{-1}$ for all $x \in G$

$= xgg^{-1}$ (As G is commutative) for all $x \in G$

$= x$ for all $x \in G$

This shows that $I_g = I_G$ for all $g \in G$.

Conversely, let $I_g = I_G$ for all $g \in G$

Then $I_g(x) = x$ for all $x \in G$ and for all $g \in G$.

or, $gxg^{-1} = x$ for all $x \in G$ and for all $g \in G$

or, $gx = xg$ for all $x \in G$ and for all $g \in G$.

So, G is commutative.

Corollary 1.1.8 If G be a non-commutative group then G has a non-trivial automorphism

Proof: Since G is non-commutative, $\exists$ distinct elements a, b in G such that $ab \neq ba$ and therefore $a \neq bab^{-1}$. This implies $I_b(a) \neq a$. That is, the inner automorphism I_b is distinct from the identity automorphism (the trivial automorphism)

Theorem 1.1.9 Let G be a group. Then $Inn(G)$ is a normal subgroup of $Aut(G)$.

Proof: The identity automorphism I_G is I_e (e is the identity element in G) as $I_e(x) = exe^{-1} = x$, for all $x \in G$. So, $I_G \in Inn(G)$ and $Inn(G)$ is non-empty. Let $I_{g_1}, I_{g_2} \in Inn(G)$

Then $(I_{g_1} \circ I_{g_2})(x) = I_{g_1}(I_{g_2}(x)) = I_{g_1}(g_2 x g_2^{-1})$

$= g_1(g_2 x g_2^{-1})g_1^{-1} = (g_1 g_2) x (g_1 g_2)^{-1}$, for all $x \in G$.

Hence $I_{g_1} \circ I_{g_2} \in Inn(G)$.

Now let $I_g \in Inn(G)$

$(I_g \circ I_{g^{-1}})(x) = (gg^{-1}) x (gg^{-1})^{-1} = exe^{-1} = x$

Also, $(I_{g^{-1}} \circ I_g)(x) = (g^{-1}g) x (g^{-1}g)^{-1} = exe^{-1} = x$

So, $I_g^{-1} = I_{g^{-1}} \in Inn(G)$

So, $Inn(G)$ is a subgroup of $Aut(G)$

To prove that $Inn(G)$ is normal in $Aut(G)$, let $\alpha \in Aut(G)$, $I_g \in Inn(G)$. Then

$$(\alpha \circ I_g \circ \alpha^{-1})(x) = \alpha(I_g(\alpha^{-1}(x))) = \alpha(g\alpha^{-1}(x)g^{-1}) = \alpha(g)\,\alpha(\alpha^{-1}(x))\,\alpha(g^{-1})$$

$$= \alpha(g)\, x\, (\alpha(g))^{-1} \quad [\text{As } \alpha(g^{-1}) = (\alpha(g))^{-1}]$$

$$= I_{\alpha(g)}(x) \quad \text{for all } x \in G.$$

Hence $\alpha \circ I_g \circ \alpha^{-1} = I_{\alpha(g)} \in Inn(G)$. So, $Inn(G)$ is a normal subgroup of $Aut(G)$.

<u>**Theorem 1.1.10**</u> Let G be a group and $Z(G)$ be the centre of the group. Then $Inn(G)$ is isomorphic to the quotient group $G/Z(G)$.