MAS 4301, Abstract Algebra I

Notes of Krishna Alladi's Lecture on Fri, Mar 13, 2020

Chapter 6: Isomorphisms Cont'd.

Theorem 1: Let G and $\bar{G}$ be groups and $\phi: G \to \bar{G}$ be an isomorphism. Then $\phi^{-1}: \bar{G} \to G$ is an isomorphism as well.

Proof: Since ϕ is an isomorphism, $\phi: G \to \bar{G}$ is one-to-one and onto. Thus $\phi^{-1}: G \to \bar{G}$ exists as a function and it is one-to-one and onto. So all we need to check is that ϕ^{-1} is operation preserving. To establish ~~Sn~~ this, consider an arbitrary pair $\bar{a}, \bar{b} \in \bar{G}$. Since ϕ is onto, $\exists\, a, b \in G$, such that $\phi(a) = \bar{a}$ & $\phi(b) = \bar{b}$. Consider ab and note that since ϕ is operation preserving, we have

$$\phi(ab) = \phi(a)\,\phi(b) = \bar{a}\,\bar{b}.$$

This means $\phi^{-1}(\bar{a}\bar{b}) = ab = \phi^{-1}(\bar{a})\,\phi^{-1}(\bar{b})$. Thus ϕ^{-1} is operation preserving and hence is an isomorphism.

(NOTE: Theorem 1 above is part 1 of Theorem 6.3 in the book)

Properties of isomorphisms on elements of a group.

Thm 6.2: Let $\phi: G \to \bar{G}$ be an isomorphism of groups.

(i) If $e, \bar{e}$ are identities of G & $\bar{G}$, then $\phi(e) = \bar{e}$ & $\phi^{-1}(\bar{e}) = e$.

(ii) Let $a \in G$. Then $\forall n \in \mathbb{Z}$, $\phi(a^n) = \phi(a)^n$

(iii) ~~If~~ Let $a, b \in G$. Then a & b commute if and only if $\phi(a)$ & $\phi(b)$ commute.

(iv) If $a \in G$, then $|a| = |\phi(a)|$ (isomorphisms preserve orders)

Proof: (i) Since ϕ and ϕ^{-1} are both homomorphisms ~~He~~ we know $\phi(e) = \bar{e}$ & $\phi^{-1}(\bar{e}) = e$. (already proved for homomorphisms in Ch. 10).

(ii) Already proved for homomorphisms, hence true for isomorphisms.

(iii) ($\Rightarrow$) Let $ab = ba$. Then $\phi(a \cdot b) = \phi(ba) \iff \phi(a)\phi(b) = \phi(b)\phi(a)$. Hence $\phi(a)$ & $\phi(b)$ commute. Conversely let $\bar{a} = \phi(a)$ & $\bar{b} = \phi(b)$ commute ie $\bar{a}\bar{b} = \bar{b}\bar{a}$.

($\Leftarrow$) Since ϕ^{-1} is an isomorphism, we ~~know~~ know that if $\bar{a} = \phi(a)$ & $\bar{b} = \phi(b)$ commute, then $\phi^{-1}(\bar{a})$ & $\phi^{-1}(\bar{b})$ commute $\iff$ a & b commute. Hence part (iii)

Case 1

(iv). Let $|a| < \infty$ (finite order). Since ϕ is a homomorphism, we know $|\phi(a)| < \infty$ and that $|\phi(a)| \,\big|\, |a|$. Now if $|\phi(a)| = |\bar{a}| < \infty$, then since ϕ^{-1} is an isomorphism, and hence a homomorphism, we know that $|\phi^{-1}(\bar{a})| \,\big|\, |\bar{a}| \iff |a| \,\big|\, \phi(a)$. Hence $|a| = |\phi(a)|$ in the finite case.

Case 2: $|a| = \infty$. In this case we must have $|\phi(a)| = \infty$, because $|\phi(a)| < \infty$ will force $|a| = |\phi^{-1}(\phi(a))| < \infty$. — contradiction. Similarly, $|\phi(a)| = \infty$ will yield $|a| = \infty$. Thus $|a| = |\phi(a)|$ in this case as well. Hence (iv) holds.

Properties of isomorphisms on subgroups.

Thm 6.3: Let $\phi: G \to \bar{G}$ be an isomorphism of groups, & $H \leq G$.

(i) ~~If H~~ H is Abelian if and only if $\phi(H) = \bar{H}$ is Abelian

(ii) H is cyclic if and only if $\phi(H) = \bar{H}$ is cyclic.

(iii) $\phi(Z(G)) = Z(\bar{G})$.

Proof: (i) Since ϕ is a homomorphism, we know that if H is Abelian, so is $\phi(H)$. Conversely if $\bar{H} = \phi(H)$ is Abelian, then since ϕ^{-1} is an isomorphism (and hence a homomorphism), we have $\phi^{-1}(\bar{H}) = H$ is Abelian. Hence (i) is proved.

(ii) Since ϕ is a homomorphism, and if $H = \langle a \rangle$ is cyclic, we know that $\phi(H) = \bar{H}$ is cyclic. Conversely, if $\phi(H) = \bar{H}$ is cyclic, then since ϕ^{-1} is an isomorphism and hence a homomorphism, we know $\phi^{-1}(\bar{H}) = H$ is cyclic. Hence part (ii).

Remark: In ~~part~~ part (ii), $H = \langle a \rangle \iff \bar{H} = \langle \phi(a) \rangle$ and $|a| = |\phi(a)|$.

(iii) We know from Theorem 6.2, (iii) above that $g \in Z(G) \iff gx = xg \ \forall x \in G$ $\iff \phi(g)\cdot\phi(x) = \phi(x)\phi(g) \ \forall x \in G$. But every $\bar{x} \in \bar{G}$ occurs as $\phi(x)$. Thus $g \in Z(G) \iff \phi(g) \in Z(\bar{G})$. This yields $\phi(Z(G)) = Z(\bar{G})$.

Theorem 6.1 (Cayley's Theorem)

Every group G is isomorphic to a group of permutations.

Remark: This is true for both finite and infinite groups.

Proof: Let G be a group. For each $g \in G$, consider the map L_g (left multiplication by ~~G~~ g) given by:

$$L_g : G \longrightarrow G \quad , \quad L_g(x) = g.x, \ \forall\, x \in G \qquad (1)$$
$$x \longrightarrow g.x$$

We know that L_g is a permutation of G (by the Latin-square property!)
Now consider the set

$$\overline{G} = \{ L_g \mid g \in G \} \qquad (2).$$

We claim that $\overline{G}$ is a group under composition. (a group of permutations).
To prove the claim, first note that L_e is the identity map, where e is the identity in G, because $L_e(x) = e.x = x \ \forall\, x \in G$. Next for any two elements $g, g' \in G$,

$$\cancel{L_g \circ L_{g'}(x)}$$

$$L_g \circ L_{g'}(x) = L_g(L_{g'}(x)) = L_g(g'.x) = g(g'.x) = g.g'.x \qquad (3)$$
$$= L_{g.g'}(x)$$

This means $L_g \circ L_{g'} = L_{g.g'} \in \overline{G}$, because $g.g' \in G$.

Finally for any $g \in G$ and the corresponding $L_g \in \overline{G}$, we have $\forall\, x \in G$

$$\left.\begin{aligned} &L_{g^{-1}} \circ L_g(x) = L_{g^{-1}}(g.x) = g^{-1}(g.x) = g^{-1}.g.x = e.x = L_e(x) \\ \text{and}\quad &L_g \circ L_{g^{-1}}(x) = L_g(g^{-1}.x) = g(g^{-1}.x) = g.g^{-1}.x = e.x = L_e(x) \end{aligned}\right\} (4)$$

which means

$$(L_g)^{-1} = L_{g^{-1}} \quad \text{in } \overline{G}.$$

Thus $\overline{G}$ is a group.

Now consider the map $\phi : G \longrightarrow \overline{G}$ defined by

$$\phi : G \to \overline{G} \quad , \quad \phi(g) = L_g \quad \forall\, g \in G \qquad (5)$$
$$g \longrightarrow L_g$$

By definition of $\overline{G}$ in (2), we see the ϕ is a bijection. To see that ϕ is operation preserving, use (3) to deduce that
$\phi(g.g') = L_{g.g'} = L_g \circ L_{g'} = \phi(g) \circ \phi(g')$. Thus ϕ is an isomorphism.