Group Theory

Week #3, Class #11 (first half)

I Automorphisms & inner automorphisms

$$\mathrm{Aut}(G) := \{ \varphi : G \longrightarrow G \ : \ \varphi \text{ is an automorphism} \}$$

automorphism $\Updownarrow$ bijective homomorphism

This is a group, with $* = \circ$ (composition)
$e = id_G$
φ^{-1} is the inverse function (also an auto)

eg: $\cdot \ \mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2 = \{ \pm id_{\mathbb{Z}} \}$
$\cdot \ \mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^{\times}$

Non-examples $\quad g \in G$: $\begin{cases} \rho_g : G \longrightarrow G & \rho_g(x) = xg \\ \lambda_g : G \longrightarrow G & \lambda_g(x) = gx \end{cases}$

These functions are bijections:

$\rho_g^{-1} = \rho_{g^{-1}}$ $\quad \begin{pmatrix} \rho_g \circ \rho_{g^{-1}} = \rho_g(xg^{-1}) = (xg^{-1})g = x \\ \rho_{g^{-1}} \circ \rho_g = \rho_{g^{-1}}(xg) = (xg)g^{-1} = x \end{pmatrix}$

$\lambda_g^{-1} = \lambda_{g^{-1}}$

But they are $\underline{\underline{\text{not}}}$ homomorphism (and, so, not autos), except when $g = e$ (the identity of G), since $\rho_e = \lambda_e = id_G$.

Reason: (for $g \neq e$) Let $x, y \in G$. Then

$$\rho_g(x \cdot y) = (x \cdot y) \cdot g = xyg$$
$$\rho_g(x) \cdot \rho_g(y) = (x \cdot g) \cdot (yg) = xgyg$$

ρ_g hom $\Rightarrow \rho_g(xy) = \rho_g(x)\rho_g(y) \Rightarrow \cancel{x}y\cancel{g} = \cancel{x}gy\cancel{g}$
$\underset{\text{cancellation law}}{\Longrightarrow} y = gy \underset{\text{cancel}}{\Longrightarrow} e = g$ $\divideontimes$

Easier proof : $\rho_g(e) = e \cdot g = g \neq e \Rightarrow \rho_g$ not hom

---

Inner automorphisms (or, conjugations)

Lemma For every $g \in G$, the function

$$z_g = \lambda_g \circ \rho_{g^{-1}} : G \longrightarrow G$$
$$= \rho_{g^{-1}} \circ \lambda_g$$
$$z_g(x) = g x g^{-1}$$

(Check: $\lambda_g \circ \rho_{g^{-1}}(x) = \lambda_g(xg^{-1}) = gxg^{-1}$)

is an automorphism of G.

Proof ∘ Clearly, z_g is a bijection (since it is the composite of two bijections), with inverse

$$z_g^{-1} = (\lambda_g \circ \rho_{g^{-1}})^{-1} = (\rho_{g^{-1}})^{-1} \circ \lambda_g^{-1} = \rho_{(g^{-1})^{-1}} \circ \lambda_{g^{-1}}$$
$$= \rho_g \circ \lambda_{g^{-1}} = z_{g^{-1}}$$

(check: $z_g \circ z_{g^{-1}}(x) = g(g^{-1}xg)g^{-1} = x$
$z_{g^{-1}} \circ z_g(x) = g^{-1}(gxg^{-1})g = x$ ✓)

∘ Check that z_g is a hom:

$$z_g(xy) = g(xy)g^{-1}$$
$$z_g(x)\, z_g(y) = (gxg^{-1})\cdot(gyg^{-1}) = gx(g^{-1}g)yg^{-1}$$
$$= gx \cdot e \cdot yg^{-1} = gxyg^{-1} \quad ✓$$

∎

Definition The autos $\{z_g\}_{g \in G}$ are called inner automorphisms (or, conjugations). They form a subgroup of $\mathrm{Aut}(G)$:

$$\boxed{\mathrm{Inn}(G) = \{ z_g : g \in G \}}$$ Inner auto. group

Check
$$z_g \circ z_{h^{-1}}(x) = z_g(h^{-1}xh) = g(h^{-1}xh)g^{-1} = (gh^{-1})x(hg^{-1})$$
$$= (gh^{-1})x(gh^{-1})^{-1} = z_{gh^{-1}}(x)$$ ∎

(in particular: $\tau_g \circ \tau_h = \tau_{gh}$ & $(\tau_g)^{-1} = \tau_{g^{-1}}$)

<u>Remark</u> If G is abelian, then $\tau_g(x) = gxg^{-1} = xgg^{-1} = xe = x$

so $\tau_g = id_G$, $\forall g \in G$, i.e.:

$$\mathrm{Inn}(G) = \{id_G\}$$

In general, though, $\mathrm{Inn}(G)$ is not trivial; for instance, when $G = S_3$.

II <u>Normal subgroups</u>

~~Def~~ A subgroup $H \leq G$ is a <u>normal subgroup</u> (written as $H \trianglelefteq G$) if

$$\boxed{ghg^{-1} \in H, \quad \forall h \in H \text{ and } g \in G}$$

<u>Lemma</u> $H \leq G$ is normal $\Longleftrightarrow \tau_g(H) = H$, $\forall g \in G$

(notation: $gHg^{-1} := \tau_g(H) = \{ghg^{-1} : h \in H\}$)

<u>Proof</u> ($\Longleftarrow$) $\tau_g(H) = H \Longrightarrow ghg^{-1} \in H$, $\forall h \in H, g \in G$ ✓

($\Longrightarrow$) Suppose $\boxed{ghg^{-1} \in H, \ \forall h \in H, \forall g \in G}$ $(*)$

then $gHg^{-1} \subseteq H$. We need to show $H \subseteq gHg^{-1}$

Indeed: Let $h \in H$. Then $g^{-1}hg \in H$
(take $g \to g^{-1}$ in $(*)$)

$\therefore$ $g^{-1}hg = k$, for some $k \in H$

$\therefore$ $h = gkg^{-1} \in gHg^{-1}$

$\therefore$ $H \subseteq gHg^{-1}$ $\blacksquare$