Recall

$G \circlearrowright A$, fix $g \in G$ get bijection

$\sigma_g : A \to A$
$a \mapsto g.a$

Do this $\forall g \in G$ get

$G \to S_A$ hom.
$g \mapsto \sigma_g$

called perm. rep.

What does the perm rep look like for conj $G \circlearrowright G$

fix $g \in G$

$\sigma_g : G \to G$
$a \mapsto g * a = gag^{-1}$

Lemma

σ_g is an isomorphism.

Pf/ $\sigma_g(a)\cdot\sigma_g(b) = (ga\cancel{g^{-1})(g}bg^{-1})$
$= gabg^{-1}$
$= \sigma_g(ab)$.

$\Rightarrow \sigma_g$ is homomorphism + bijective $\Rightarrow$ iso ⊘

$G \circlearrowright G$ by conj

$G \xrightarrow{\phi} S_G$

But $\operatorname{im}\phi$ consists of isomorphisms!!

Defn (Automorphism Group)

G a group.

$\operatorname{Aut}(G) = \{\phi : G \to G \mid \phi \text{ an iso}\}$

A group under comp.

Remark

set A — $\operatorname{Aut}(A) = \{\text{bij. } A \to A\} = S_A$ ← set

Vector Space — $\operatorname{Aut}(V) = \{\text{invertible linear } V \to V\} \cong GL_n$ ← VS

Groups — $\operatorname{Aut}(G)$ as above

Prop G group.

$\operatorname{Aut} G \leq S_G$

Pf/ $\phi, \psi \in \operatorname{Aut} G$
$\Rightarrow \phi \circ \psi^{-1}$

$G \circlearrowright G$ by conj.

$\Rightarrow G \xrightarrow{\phi} S_G$
$\quad \phi: G \to \operatorname{Aut}(G) \leq S_G$

Study
$\phi: G \to \operatorname{Aut} G$

$\ker\phi = \{g \in G \mid \sigma_g(a) = a \ \forall a\}$
$= \{g \in G \mid gag^{-1} = a \ \forall a\}$
$= \{g \in G \mid ga = ag \ \forall g\}$
$= Z(G)$

$G \to \operatorname{Aut}(G)$, $G \to G/Z(G) \to \operatorname{Aut}(G)$ — First iso thm

$\Rightarrow G/Z(G) \simeq K \leq \operatorname{Aut} G$

Remark $H \trianglelefteq G$ then $G \circlearrowright H$ via conjugation
$h \in H$
$g * h = ghg^{-1} \in H$

Prop
$\phi: G \to \operatorname{Aut}(H)$
$\ker\phi = C_G(H)$ — no ref to G
$G/C_G(H) \simeq K \leq \operatorname{Aut}(H)$ — Pf

Corollary 1

$|gag^{-1}| = |a|$ ← HW
$\quad |\sigma_g(a)|$

Corollary 2

$K \leq G$, then $gKg^{-1} \leq G$
& $K \simeq gKg^{-1}$

Ex/ $K = \langle (12) \rangle \leq S_3$
$g = (13)$

* $g(12)g^{-1} = (13)(12)(13) = (23)$
& $|(12)| = 2 = |(23)|$
* $gKg^{-1} = \langle (23) \rangle \simeq \mathbb{Z}_2 \simeq K$

Corollary 3 $H \leq G$

Then $N_G(H) \circlearrowright H$ via conj.

$N_G(H) \to \operatorname{Aut}(H)$, $N_G(H) \to N_G(H)/C_G(H) \to \operatorname{Aut}(H)$

Pf/ $H \trianglelefteq N_G(H) \leq G$
$N_G(H) = \{g \in G \mid gHg^{-1} = H\}$ ⊘

Prop w/ $G = N_G(H)$

Defn $G \circlearrowright G$ via conj

$\phi: G \to \operatorname{Aut} G$

$\operatorname{Inn}(G) := \operatorname{im}\phi \leq \operatorname{Aut} G$
↑ inner automorphisms

Prop $\Rightarrow \operatorname{Inn}(G) \simeq G/Z(G)$

Examples

1) G abelian $\Leftrightarrow \operatorname{Inn} G = 1$
2) $Z(D_8) = \langle r^2 \rangle$
$\Rightarrow \operatorname{Inn}(D_8) = D_8/\langle r^2 \rangle \simeq V_4$
$\sigma_r(s) = rsr^{-1} = sr^2$
$\sigma_r(r) = r$
3) $Z(S_n) = 1 \quad n \geq 3$
$\Rightarrow \operatorname{Inn}(S_n) \simeq S_n \leq \operatorname{Aut}(S_n)$
$n \neq 6$ this $=$
4) $H \leq G \quad H \simeq \mathbb{Z}_2$.
If $H \trianglelefteq G \Rightarrow H \leq Z(G)$.

Pf/ $\phi: H \to H = \langle x \mid x^2 = 1 \rangle$
$1 \mapsto 1$, $x \mapsto x$
$\Rightarrow \phi = id$
i.e. $\operatorname{Aut}(H) = 1$
$N_G(H)/C_G(H)$
$\quad = 1$

$C_G(H) = N_G(H) = G$
If $H \trianglelefteq G$
$\Rightarrow H \leq Z(G)$ ⊘

Applications

Prop

$\operatorname{Aut}(\mathbb{Z}_n) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$

Pf/ $\mathbb{Z}_n = \langle x \rangle \quad \phi \in \operatorname{Aut}(\mathbb{Z}_n)$

$\Rightarrow \phi(x) = x^a$ ← also a generator

$\Rightarrow \gcd(a, n) = 1$

Rmk $z \in \mathbb{Z}_n$: $\phi(z) = \phi(x^d) = \phi(x)^d$
$= (x^a)^d$
$= (x^d)^a$
$= z^a$

Call $\phi = \phi_a$

$\operatorname{Aut}(\mathbb{Z}_n) \xrightarrow{\Psi} (\mathbb{Z}/n\mathbb{Z})^\times$
$\phi_a \mapsto a$

Hom $\phi_a \phi_b(z) = \phi_a(z^b)$
$= z^{ba}$
$= z^{ab}$
$= \phi_{ab}(z)$

Inj ✓ Surj ✓

Classification

$|G| = p \Rightarrow G \simeq \mathbb{Z}_p$

$|G| = p^2 \Rightarrow G \simeq \mathbb{Z}_{p^2}$ or $\mathbb{Z}_p \times \mathbb{Z}_p$

Ex Groups of order pq
w/ $p < q$ & $p \nmid (q-1)$

$33 = 3 \cdot 11$ & $3 \nmid 10$
$51 = 3 \cdot 17$ & $3 \nmid 16$ — No

$\boxed{\text{But } G = 2 \cdot 3 \text{ but } 2 \mid 2}$

$G \simeq \mathbb{Z}_{pq}$. G is abelian

Pf/ 3 cases
1) $Z(G) = G$ ← Done
2) $|Z(G)| = p$ or q
$\Rightarrow |G/Z(G)| = p$ or q
$\Rightarrow G/Z(G)$
HW $\Rightarrow G$ abelian
Last Case
$Z(G) = 1$ ← Can't happen

$|x| = p$ or q
Suppose $\forall x$ have order p.
$\Rightarrow x \notin Z(G) \Rightarrow |C_G(x)| = p$
$\Rightarrow |G : C_G(x)| = q$
Class eqn
$|G| = |Z(G)| + \sum |G : C_G(x)|$
$pq \qquad 1 \qquad kq$ — contradn
q divides

$\Rightarrow$ Some $|x| = q$.
$H = \langle x \rangle$
$\Rightarrow |G : H| = \frac{pq}{q} = p$
p smallest prime div. pq
$\Rightarrow H \trianglelefteq G$

$H \leq C_G(H) \leq G$
b/c H cyclic — order p or ~~pq Lagrange~~

$\Rightarrow H \leq Z(G) = 1$

$H = C_G(H) \leq G$
$q \qquad pq$

$G \circlearrowright H$ via conj.

$G \xrightarrow{\phi} \operatorname{Aut}(H)$, $G \to G/C_G(H) \to \operatorname{Aut}(H)$

Lagrange
$|G/C_G(H)| \mid |\operatorname{Aut}(H)| = (\mathbb{Z}/q\mathbb{Z})^\times$
$p \mid q-1$

$Z(G) \neq 1$

$\Rightarrow G$ abelian

Exercise $p \neq q$

$\Rightarrow G \simeq \mathbb{Z}_{pq}$. ⊘