Section 4.4 Automorphisms

Definition An *automorphism* of a group G is an isomorphism $\varphi: G \to G$. The set of all automorphisms of G is a group, denoted $Aut(G)$, when the operation is composition.

Example Note that $Aut(G)$ really is a group. First, note that if $\varphi: G \to G$ and $\mu: G \to G$ are isomorphisms, then so is $\varphi \circ \mu$.

(i) $id: G \to G$ is an isomorphism.

(ii) function composition is associative.

(iii) if $\varphi: G \to G$ is an automorphism, then so is $\varphi^{-1}: G \to G$.

Example Find $Aut(\mathbb{Z}_3)$. $\mathbb{Z}_3 = \{1, a, a^2\}$

Note: any isomorphism $\mathbb{Z}_3 \to \mathbb{Z}_3$ must fix 1. There are only two maps that do this: $id = 1$ and $\varphi(x) = x^2$

$$\begin{array}{ccc} \mathbb{Z}_3 & \xrightarrow{id} & \mathbb{Z}_3 \\ 1 & \longrightarrow & 1 \\ a & \longrightarrow & a \\ a^2 & \longrightarrow & a^2 \end{array} \qquad \begin{array}{ccc} \mathbb{Z}_3 & \xrightarrow{x^2} & \mathbb{Z}_3 \\ 1 & \longrightarrow & 1 \\ a & \longrightarrow & a^2 \\ a^2 & \longrightarrow & a \end{array}$$

Also $\varphi(xy) = (xy)^2 = x^2y^2 = \varphi(x)\varphi(y)$ so φ is an isomorphism

$Aut(\mathbb{Z}_3) = \{id, \varphi\} \cong \mathbb{Z}_2$

$$\begin{array}{c|cc} & id & \varphi \\ \hline id & id & \varphi \\ \varphi & \varphi & id \end{array}$$

Important Example If $g \in G$, define $\varphi_g: G \to G$, $\varphi_g(x) = gxg^{-1}$

i.e. φ_g is conjugation by g. This is an automorphism:

Injective $\varphi_g(x) = \varphi_g(y) \Rightarrow gxg^{-1} = gyg^{-1} \Rightarrow x = y$

Surjective Given $x \in G$, $\varphi_g(g^{-1}xg) = x$.

Also $\varphi(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \varphi(x)\varphi(y)$.

Definition For each $g \in G$, $\varphi_g: G \to G$ when $\varphi_g(x) = gxg^{-1}$ is called an *inner automorphism of G*. $Inn(G) = \{\varphi_g : g \in G\}$ and $Inn(G) \leq Aut(G)$.

Reason: ① $\varphi_1 = id \in Inn(G)$

② If $\varphi_g\varphi_h(x) = ghxh^{-1}g^{-1} = gh\,x\,(gh)^{-1} = \varphi_{gh}(x)$

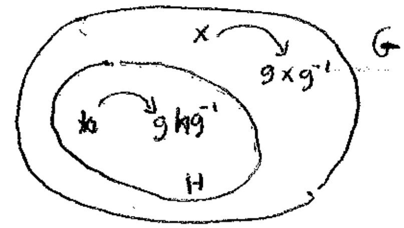
Thus $\varphi_g\varphi_h = \varphi_{gh}$ (i.e. $Inn(G)$ is closed.)

③ $\varphi_g^{-1} = \varphi_{g^{-1}} \in Inn(G)$.

Observation: $Inn(G) \cong G/Z(G)$.

Reason $\Psi: G \to Inn(G)$, $\Psi(g) = \varphi_g$ is a homomorphism
because $\Psi(gh) = \varphi_{gh} = \varphi_g\varphi_h = \Psi(g)\Psi(h)$. Kernel is $Z(G)$

<u>Note</u> If $H \trianglelefteq G$ then $\varphi_g(H) = H$, and φ_g restricts to an automorphism of H



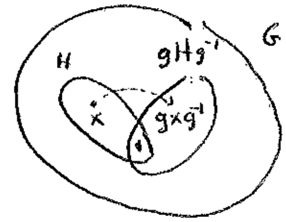
<u>Proposition 13</u> If $H \trianglelefteq G$ then G acts on H by conjugation, i.e. $g \cdot h = ghg^{-1} = \varphi_g(h)$ and φ_g is an automorphism of H. Permutation representation is

$$\begin{aligned} \Psi : G &\longrightarrow \mathrm{Aut}(H) \le S_H \\ g &\longmapsto \varphi_g \end{aligned}$$

The kernel of this is $C_G(H)$. Therefore $G/C_G(H) \cong \Psi(G) \le \mathrm{Aut}(H)$

<u>Corollary 14</u> (Really a consequence of our set up, not of Prop. 13)

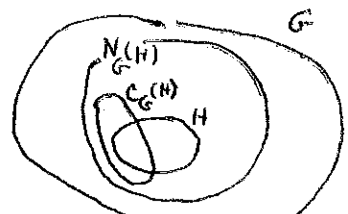
If $H \le G$, then $gHg^{-1} \cong H$,
i.e. $\varphi_g : G \to G$ restricts to an isomorphism $H \to gHg^{-1}$.
Thus $|H| = |gHg^{-1}|$ and $|x| = |gxg^{-1}|$.



<u>Corollary 15</u>

If $H \le G$, then $H \trianglelefteq N_G(H)$ and
$\Psi : N_G(H) \longrightarrow \mathrm{Aut}(H)$ has kernel $C_G(H)$.
Thus $N_G(H)/C_G(H) \cong$ (subgroup of $\mathrm{Aut}(H)$)

Letting $H = G$, we get $G/Z(G) \cong$ (subgroup of $\mathrm{Aut}(H)$)

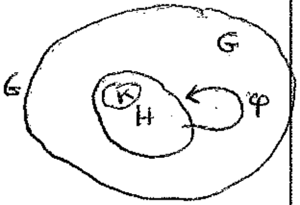


Text makes the point that information about $\mathrm{Aut}(H)$ gives information about $N_G(H)$ and $C_G(H)$ and $N_G(H)/C_G(H)$.

<u>Example</u> If $\mathrm{Aut}(H) = 1$, then $N_G(H) = C_G(H)$.

<u>Definition</u> $H \le G$ is <u>characteristic in G</u> if $\varphi(H) = H$ $\forall \varphi \in \mathrm{Aut}(G)$

① H characteristic in $G \Rightarrow H \trianglelefteq G$
② If H is only subgroup of G of order $|H|$, then H char G
③ K char H and $H \trianglelefteq G \Rightarrow K \trianglelefteq G$.



Computations of Automorphism Groups

Note If $G \cong H$ then $\text{Aut}(G) \cong \text{Aut}(H)$

Reason: If $\varphi : G \to H$ is isomorphism, then have isomorphism

$$\Phi : \text{Aut}(G) \longrightarrow \text{Aut}(H)$$
$$\mu \longmapsto \varphi \mu \varphi^{-1}$$

(check this)

Proposition 16 $\text{Aut}(Z_n) \cong (\mathbb{Z}/n\mathbb{Z})^\times$

Reason $Z_n = \{1\ a\ a^2 \dots a^{n-1}\}$ has generators a^k where $\gcd(k,n) = 1$
i.e. where $k \in (\mathbb{Z}/n\mathbb{Z})^\times$. Check $\psi_k : Z_n \to Z_n$, $\psi_k(x) = x^k$
is automorphism. Also any auto of Z_n sends a to a generator a^k
So $\text{Aut}(Z_n) = \{\psi_k \mid \gcd(k,n) = 1\}$.
Check $(\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow \text{Aut}(Z_n)$ where $k \mapsto \psi_k$ is isomorphism.

Read Proposition 17. It describes $\text{Aut}(G)$ for various G.
Much of this will be proved later - we'll revisit it then.
For now, we discuss just part of it.

> If p is prime then $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a field.
> Additive group $\mathbb{F}_p^n = \mathbb{F}_p \times \mathbb{F}_p \times \dots \times \mathbb{F}_p$ is a vector space over $\mathbb{F}_p$
> Scalar mult: $g(x_1, x_2, \dots, x_n) = (gx_1\ gx_2\ \dots\ gx_n)$.
> $\text{Aut}(\mathbb{F}_p^n) = \left(\begin{array}{c}\text{linear transformations} \\ \mathbb{F}_p^n \longrightarrow \mathbb{F}_p^n\end{array}\right) \cong GL_n(\mathbb{F}_p)$.

Example Klein 4-group $V_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 = \left\{ \begin{bmatrix}0\\0\end{bmatrix}, \begin{bmatrix}1\\0\end{bmatrix}, \begin{bmatrix}0\\1\end{bmatrix}\ \begin{bmatrix}1\\1\end{bmatrix} \right\}$
$\text{Aut}(V_4) = GL_2(\mathbb{F}_2)$

General Picture
If V is an abelian (additive) group of order p^n for prime p
with property $px = 0\ \forall\ x \in V$ then V is an n-dimensional
vector space over $\mathbb{F}_p$ and $\text{Aut}(V) \cong GL_n(\mathbb{F}_p)$.