Section 4.4 Automorphisms

Definition An automorphism of a group \( G \) is an isomorphism \( \Phi : G \rightarrow G \). The set of all automorphisms of \( G \) is a group denoted \( \text{Aut}(G) \), where the operation is composition.

Example Note that \( \text{Aut}(G) \) really is a group. First, note that if \( \Phi : G \rightarrow G \) and \( \Psi : G \rightarrow G \) are isomorphisms, then so is \( \Phi \circ \Psi \).

(i) \( \text{id} : G \rightarrow G \) is an isomorphism.

(ii) function composition is associative.

(iii) if \( \Phi : G \rightarrow G \) is an automorphism, then so is \( \Phi^{-1} : G \rightarrow G \).

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

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

\[
\begin{array}{ccc}
\mathbb{Z}_3 & \overset{\text{id}}{\longrightarrow} & \mathbb{Z}_3 \\
1 & \mapsto & 1 \\
\mapsto & 1 \\
a & \mapsto & a^2 \\
\mapsto & a^2 \\
a^2 & \mapsto & a \\
\mapsto & a \\
\end{array}
\]

Also \( \Phi(xy) = (xy)^2 = x^2y^2 = \Phi(x)\Phi(y) \) so \( \Phi \) is an isomorphism.

\[\text{Aut}(\mathbb{Z}_3) = \{ \text{id}, \Phi \} \cong \mathbb{Z}_2 \]

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

i.e. \( \Phi_g \) is conjugation by \( g \). This is an automorphism:

Injective \( \Phi_g(x) = \Phi_g(y) \Rightarrow g x g^{-1} = g y g^{-1} \Rightarrow x = y \)

Surjective Given \( x \in G \), \( \Phi_g(gxy) = x \).

Also \( \Phi(xy) = gxyg^{-1} = g x y g^{-1} g y g^{-1} = \Phi(x) \Phi(y) \).

Definition For each \( g \in G \), \( \Phi_g : G \rightarrow G \) where \( \Phi_g(x) = gxg^{-1} \) is called an inner automorphism of \( G \). \( \text{Inn}(G) = \{ \Phi_g : g \in G \} \)

and \( \text{Inn}(G) \leq \text{Aut}(G) \).

Reason:

(1) \( \Phi_1 = \text{id} \in \text{Inn}(G) \)

(2) \( \Phi_g \Phi_h(x) = g h x h^{-1} g^{-1} = g h (g h^{-1})^{-1} = \Phi_{g h} \)

Thus \( \Phi_g \Phi_h = \Phi_{g h} \) (i.e. \( \text{Inn}(G) \) is closed.)

(3) \( \Phi_g^{-1} = \Phi_{g^{-1}} \in \text{Inn}(G) \).

Observation: \( \text{Inn}(G) \cong G / Z(G) \).

Reason \( \Psi : G \rightarrow \text{Inn}(G) \), \( \Psi(g) = \Phi_g \) is a homomorphism.

because \( \Psi(gh) = \Phi_{gh} = \Phi_g \Phi_h = \Psi(g)\Psi(h) \). Kernel is \( Z(G) \).
Note If $H \leq G$ then 
$\Phi_\varphi(H) = H$, and $\Phi_\varphi$ restricts to an automorphism of $H$.

**Proposition 13** If $H \leq G$ then $G$ acts on $H$ by conjugation, i.e., $g \cdot h = ghg^{-1} = \Phi_\varphi(h)$ and $\Phi_\varphi$ is an automorphism of $H$. Permuation representation is 
$$
\Psi_H : G \rightarrow \text{Aut}(H) \leq S_H \\
\varphi \mapsto \Phi_\varphi 
$$
The kernel of this is $C_G(H)$. Therefore $G/C_G(H) \cong \Psi(G) \leq \text{Aut}(H)$.

**Corollary 14** (Really a consequence of our setup, not of Prop. 13) 
If $H \leq G$, then $gHg^{-1} = H$,
i.e., $\Phi_\varphi : G \rightarrow G$ restricts to an isomorphism $H \rightarrow gHg^{-1}$.
Thus $|H| = |gHg^{-1}|$ and $1x1 = |g \times g^{-1}|$.

**Corollary 15** 
If $H \leq G$, then $H \leq N_G(H)$ and 
$\Psi : N_G(H) \rightarrow \text{Aut}(H)$ has kernel $C_G(H)$.
Thus $N_G(H)/C_G(H) \cong (\text{subgroup of Aut}(H))$.

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

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

**Example** If $\text{Aut}(H) = 1$, then $N_G(H) = C_G(H)$.

**Definition** $H \leq G$ is characteristic in $G$ if $\Phi(H) = H \forall \Phi \in \text{Aut}(G)$.

01. $H$ characteristic in $G \implies H \leq G$
02. If $H$ is only subgroup of $G$ of order $|H|$, then $H$ char $G$
03. $K$ char $H$ and $H \leq G \implies K \leq G$. 
Computations of Automorphism Groups

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

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

$\Phi: \text{Aut}(G) \to \text{Aut}(H)$

$\mu \mapsto \Phi(\mu \Phi')$

(check this)

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

Reason: $\mathbb{Z}/n\mathbb{Z} = \{1, a, a^2, \ldots, a^{n-1}\}$ has generators $a^k$ where $\gcd(k, n) = 1$

i.e. when $\Phi_k: \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $\Phi_k(x) = x^k$

is automorphism. Also, any auto of $\mathbb{Z}/n\mathbb{Z}$ sends $a$ to a generator $a^k$

So $\text{Aut}(\mathbb{Z}/n\mathbb{Z}) = \{\Phi_k | \gcd(k, n) = 1\}$

Check $(\mathbb{Z}/n\mathbb{Z})^{\times} \to \text{Aut}(\mathbb{Z}/n\mathbb{Z})$ where $k \to \Phi_k$ 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 $\mathbb{F}_p^n = \mathbb{F}_p \times \mathbb{F}_p \times \ldots \times \mathbb{F}_p$ is a vector space over $\mathbb{F}_p$

Scalar mult: $g(x_1, x_2, \ldots, x_n) = (g x_1, g x_2, \ldots, g x_n)$

$\text{Aut}(\mathbb{F}_p^n) = (\text{linear transformations}) \cong GL_n(\mathbb{F}_p)$

Example: Klein 4-group $V_4 \cong \mathbb{Z}_2 \times \mathbb{Z}_2 = \{[0], [1], [0] [1]\}$

$\text{Aut}(V_4) = GL_2(\mathbb{F}_2)$

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 $\text{Aut}(V) \cong GL_n(\mathbb{F}_p)$. 