Chapter 1

Automorphism

Definition 1 (Automorphism)**.** An automorphism of a group G is an isomorphism[1] of G onto itself.

Theorem 1.1. The set $Aut(G)$ of all automorphisms of a group G is a group under the operation of composition of mappings.

Proof. Here $Aut(G)$ is the set of all automorphisms of a group G and the operation is the composition of mappings.
Let $f, g \in Aut(G)$. Then the composite map $g \circ f$ is bijective, because f and g are bijective.
Using the hypotheses that f and g are group homomorphisms, we can conclude that $g \circ f$ is also a group homomorphism, because

$$\begin{aligned}(g \circ f)(ab) &= g(f(ab)) \\ &= g(f(a)\ f(b)) \\ &= g(f(a))\ g(f(b)) \\ &= (g \circ f)(a)\ (g \circ f)(b)\end{aligned}$$

So, $g \circ f \in Aut(G)$. This is the closure property.

The associative law holds for $Map(G)$, the set of all mappings of G into itself; so it holds in $Aut(G)$, because $Aut(G)$ is closed under composition of mappings.

Clearly, 1_G is the identity element of $Aut(G)$.

If $f \in Aut(G)$, the inverse mapping $f^{-1} : G \to G$ exists and is likewise bijective. Let $f \in Aut(G)$ and $a, b, x, y \in G$ such that $f(a) = x$ and $f(b) - y$. Then we have $a = f^{-1}(x)$ and $b = f^{-1}(y)$.
Since f is a group homomorphism, we have $f(ab) = f(a)f(b) = xy$. It gives, $f^{-1}(xy) = ab = f^{-1}(x)f^{-1}(y)$. This implies that f^{-1} is also a group homomorphism.
Hence, $f^-1 \in Aut(G)$.
Therefore, $Aut(G)$ is a group under composition of mappings. □

1.1 Inner Automorphisms

For any fixed $a \in G$, we define a mapping $f_a : G \to G$ by setting $f_a(x) = axa^{-1}$.
Claim. $f_a \in Aut(G)$ for every $a \in G$.

[1]Homomorphism: Suppose G, G' are multiplicative groups. A mapping $f : G \to G'$ is called a group homomorphism iff $f(ab) = f(a)f(b)$ holds for all $a, b \in G$.
Isomorphism: A bijective group homomorphism is called an isomorphism.

Proof. f_a is injective (by the cancellation law), for

$$\begin{aligned} & f_a(x) = f_a(y) \\ & \Rightarrow axa^{-1} = aya^{-1} \\ & \Rightarrow x = y. \end{aligned}$$

f_a is surjective, because

$$\begin{aligned} & f_a(a^{-1}xa) \\ & = a(a^{-1}xa)a^{-1} \\ & = x. \end{aligned}$$

f_a is group homomorphism, because for all $x, y \in G$, we have

$$\begin{aligned} & f_a(xy) \\ & = a(xy)a^{-1} \\ & = (axa^{-1})(aya^{-1}) \\ & = f_a(x)f_a(y). \end{aligned}$$

□

Definition 2 (Inner Automorphism)**.** For any fixed $a \in G$ the mapping $f_a : G \to G$ defined by $f_a(x) = axa^{-1}$ is called the inner automorphism determined by a.

Theorem 1.2. The set $Inn(G)$ of all inner automorphisms of a group G is a subgroup of $Aut(G)$.

Proof. The relation $f_a \circ f_b = f_{ab}$ is the key.
This is easily proved, for

$$\begin{aligned} (f_a \circ f_b)(x) &= f_a(f_b(x)) \\ &= f_a(bxb^{-1}) \\ &= a(bxb^{-1})a^{-1} \\ &= (ab)x(ab)^{-1} \\ &= f_{ab}(x) \qquad \text{holds for all } x \in G \end{aligned}$$

So, $Inn(G)$ Is closed under composition of mappings.
The identity mapping l_G belongs to $Inn(G)$, because $f_e = 1_G$.
The inverse of f_a, which is obviously an automorphism, is the inner automorphism determined by a^{-1}, because

$$f_a \circ f_{a^{-1}} = f_{aa^{-1}} = f_e = 1_G$$

and

$$f_{a^{-1}} \circ f_a = f_{a^{-1}a} = f_e = 1_G$$

So, $Inn(G)$ is a subgroup of $Aut(G)$. It remains to show that $Inn(G)$ is a normal subgroup of $Aut(G)$. For any $\sigma \in Aut(G)$, we have $\sigma \circ f_a \circ \sigma^{-1} = f_{\sigma(a)}$, because

$$\begin{aligned} (\sigma \circ f_a \circ \sigma^{-1})(x) &= (\sigma \circ f_a)(\sigma^{-1}(x)) \\ &= \sigma(a\sigma^{-1}(x)a^{-1}) \\ &= \sigma(a)\sigma(\sigma^{-1}(x))\sigma(a^{-1}) \\ &= \sigma(a)x\sigma(a^{-1}) \\ &= \sigma(a)x(\sigma(a))^{-1} \\ &= f_{\sigma(a)}(x) \quad \in Inn(G) \end{aligned}$$

So, $Inn(G)$ is a normal subgroup of $Aut(G)$ □

Theorem 1.3. $Inn(G) \cong G/Z$, where Z denotes the center of G.

Proof. Define a mapping $\psi : G \to Inn(G)$ by setting $\psi(a) = f_a$.
We have $f_a \circ f_b$, for

$$\begin{aligned}(f_a \circ f_b)(x) &= f_a(f_b(x)) \\ &= f_a(bxb^{-1}) \\ &= a(bxb^{-1})a^{-1} \\ &= (ab)x(ab)^{-1} \\ &= f_{ab}(x) \qquad \text{holds for all } x \in G\end{aligned}$$

ψ is a group homomorphism, for

$$\psi(ab) = f_{ab} = f_a \circ f_b = \psi(a) \circ \psi(b) \qquad \text{holds for all } a, b \in G$$

What is $\ker \psi$?

$$\begin{aligned}a \in \ker \psi &\Leftrightarrow \psi(a) = f_e(a) \\ &\Leftrightarrow f_a = 1_G \\ &\Leftrightarrow f_a(x) = 1_G(x) \quad \text{holds for every } x \in G \\ &\Leftrightarrow axa^{-1} = x \quad \text{holds for every } x \in G \\ &\Leftrightarrow ax = xa \quad \text{holds for every } x \in G \\ &\Leftrightarrow a \in Z\end{aligned}$$

This proves $\ker \psi = Z$.
By the first isomorphism theorem, we get

$$G/Z \cong Inn(G)$$

Therefore, $Inn(G) \cong G/Z$, because being isomorphism is a symmetric relation. □

Example. Show that the automorphism group of Klein four-group G is isomorphic to the symmetric group S_3.

Proof. Being abelian, the identity mapping is the only inner automorphism. In any automorphism the identity element is mapped onto itself; so, the three non-identity elements of G are permuted amongst themselves. Therefore, every automorphism is an element of S_3.

Conversely, if σ is any permutation on three letters, and x, y, z are three non-identity elements of G in any order, then $xy = z$ (by the group table of the Klein four-group G).
By the same argument, $\sigma(x)\,\sigma(y) = \sigma(z)$. Extend σ to G by setting $\sigma(e) = e$; this extended mapping is then a bijective homomorphism of G.
Hence, $Aut(G) \cong S_3$ is proved. □