9. AUTOMORPHISMS

§9.1 The Automorphism Group

An **automorphism** of a group G is an isomorphism from G to G. We write the image of g under the automorphism θ as $\boldsymbol{g^{\theta}}$ and multiply automorphisms by defining $g^{\alpha\beta} = (g^{\alpha})^{\beta}$. Under this operation the set of all automorphisms of G forms a group **Aut(*G*)**.

The **conjugate** of g under h is $h^{-1}gh$ and we denote it by $\mathbf{g}^{\boldsymbol{h}}$. Conjugation by an element of the group is an automorphism, called an **inner automorphism**. Any automorphism that is not an inner one is called an **outer automorphism**. The inner automorphisms form a subgroup of Aut(G), denoted by **Inn(G)**.

Theorem 1: Inn(G) ≅ G/Z(G).

Proof: For $h \in$ G, let θ_h denote conjugation by h.
The map $h \to \theta_h$ is a homomorphism whose kernel is Z(G). Hence, by the First isomorphism Theorem

$$\mathrm{Inn(G)} \cong \mathrm{G/Z(G)}.$$

Theorem 2: $\mathrm{Aut}(\mathbf{C}_n) \cong \mathbb{Z}_n{}^{\#}$ and $\mathrm{Aut}(\mathbf{C}_\infty) \cong \mathbf{C}_2$.

Proof: $\mathbf{C}_n = \langle \mathrm{A} \mid \mathrm{A}^n \rangle$.

If m is coprime to n then $\Omega(m)$ = the automorphism $x \to x^m$ is an isomorphism between $\mathbb{Z}_n{}^{\#}$ and $\mathrm{Aut}(\mathbf{C}_n)$.

$\mathrm{Aut}(\mathbf{C}_\infty) \cong \mathbf{C}_2$ since the only automorphisms of the infinite cyclic group are $x \to x$ and $x \to x^{-1}$.

Example 1: $\mathrm{Aut}(\mathbf{C}_{100}) \cong \mathbb{Z}_{100}^{\#} \cong C_{20} \times C_2$.
$\mathrm{Inn}(\mathbf{C}_{100}) \cong \mathbf{1}$.

Example 2: $\mathbf{V}_4 = \langle \alpha, \beta \mid \alpha^2, \beta^2, \beta\alpha = \alpha\beta \rangle$.
If A is $\alpha \to \beta$, $\beta \to \alpha\beta$ and B is $\alpha \to \beta$, $\beta \to \alpha$ then
$\mathrm{Aut}(\mathbf{V}_4) = \langle A, B \mid A^3, B^2, BA = A^{-1}B \rangle$.
$\mathrm{Inn}(\mathbf{V}_4) \cong \mathbf{V}_4/Z(\mathbf{V}_4) \cong 1$.

Theorem 3: Suppose $n \geq 3$. Then $\mathrm{Aut}(\mathbf{D}_{2n}) \cong \mathbf{D}_{2n}$ and $\mathrm{Inn}(\mathbf{D}_n) \cong \mathbf{D}_{2n}$ if n is odd and $\mathbf{C}_n \times \mathbf{C}_2$ if n is even.
Proof: If A is $\alpha \to \alpha$, $\beta \to \alpha\beta$ and B is $\alpha \to \alpha^{-1}$, $\beta \to \beta$ then
$\mathrm{Aut}(\mathbf{D}_6) = \langle A, B \mid A^n, B^2, BA = A^{-1}B \rangle \cong \mathbf{D}_{2n}$.
If n is even then $Z(\mathbf{D}_{2n}) = \langle A^n \rangle$ and

$$\mathrm{Inn}(\mathbf{D}_{2\mathrm{n}}) \cong \mathbf{D}_{2\mathrm{n}}/\langle A^n \rangle \cong \mathbf{V}_4.$$

If n is odd then $Z(\mathbf{D}_{2n}) = \mathbf{1}$ and $\mathrm{Inn}(\mathbf{D}_{2n}) \cong \mathbf{D}_{2n}$.

Note that $\mathbf{D}_2 \cong \mathbf{C}_2$ and so $\mathrm{Aut}(\mathbf{D}_2) \cong 1$ and $\mathbf{D}_4 \cong \mathbf{C}_2 \times \mathbf{C}_2$ and so $\mathrm{Aut}(\mathbf{D}_4) \cong \mathbf{S}_3$.

Example 3: $\mathrm{Aut}(\mathbf{D}_6) \cong \mathrm{Inn}(\mathbf{D}_6) \cong \mathbf{D}_6$.

Recall that $\mathbf{S}_3 \cong \mathbf{D}_6$ and so $\mathrm{Aut}(\mathbf{S}_3) \cong \mathbf{S}_3$. What about the other symmetric groups? Clearly $\mathbf{S}_1$ and $\mathbf{S}_2 \cong \mathbf{C}_2$ have trivial automorphism groups. What about $\mathbf{S}_n$ in general. Is $\mathrm{Aut}(\mathbf{S}_n) \cong \mathbf{S}_n$ for all $n \geq 3$?

The curious answer is “in all but one case”. If n = 3, 4 or 5 then indeed Aut($\mathbf{S}_n$) ≅ $\mathbf{S}_n$. But Aut($\mathbf{S}_6$) is twice as big as $\mathbf{S}_6$ itself.

Example 4: If G is the direct sum of n copies of $\mathbb{Z}_p$, where p is prime, then Aut(G) ≅ GL(n, p) because an automorphism of G is a linear transformation when G is viewed as a vector space over $\mathbb{Z}_p$.

Example 5: Aut($\mathbf{Q}_8$) ≅ $\mathbf{S}_4$.
Solution: (based on a solution by Karen E. Smith from the University of Michigan)
$\mathbf{Q}_8 = \langle A, B \mid A^4, B^2 = A^2, BA = A^{-1}B\rangle$.
There are six elements of order 4:

$$A, A^{-1}, B, B^{-1}, AB \text{ and } (AB)^{-1}.$$

Label the six sides of cube with these labels so that elements and their inverses are on opposite faces.

An automorphism of $\mathbf{Q}_8$ corresponds to a rotation of the cube and so Aut($\mathbf{Q}_8$) is isomorphic to the rotation group of the cube, which is $\mathbf{S}_4$.

§9.2 Checking for Automorphisms

Suppose we have a finite group

$$G = \langle A, B, \dots \mid R_1, R_2, \dots\rangle$$

Where the R_i are words in the generators.

Suppose we have a function θ from the set of generators to G. This can be extended to a map from G to

G. We can check that θ is an endomorphism by checking that the images of the generators: A^θ, B^θ, … satisfy the same relators as A, B, … do in the presentation for G. Finally to ensure that θ is an automorphism we must check that G^θ has the same order as G.

Example 6: $\mathbf{Q}_8 = \langle A, B \mid A^4, B^2 = A^2, B^{-1}AB = A^{-1}\rangle$.
Let $A^\theta = B$ and $B^\theta = AB$.
Now $(A^\theta)^4 = B^4$.
$(B^\theta)^2 = (AB)^2 = ABAB = B^2 = (A^\theta)^2$.

$$\begin{aligned}(B^\theta)^{-1}A^\theta B^\theta &= (AB)^{-1}B(AB)\\ &= (B^{-1}A^{-1}B)AB\\ &= A^2B = B^{-1} = (A^\theta)^{-1}\end{aligned}$$

Now clearly the group generated by B and AB has order 8, as does $\mathbf{Q}_8$ so θ induces an automorphism.

This last step is necessary because θ might have been merely an endomorphism. For example if we had chosen $A^\theta = A^2$ and $B^\theta = A$, then all the relators would be satisfied by the corresponding images, yet the image of G under θ would have had order 4.

§9.3 Complete Groups

A group G is a **complete group** if:

$$Z(G) = 1 \text{ and } \mathrm{Aut}(G) = \mathrm{Inn}(G).$$

By theorem 1, Aut(G) ≅ G for a complete group G.

Theorem 2: Automorphisms take conjugacy classes to conjugacy classes.

Proof: $(h^{-1}gh)^\theta = h^{-\theta}g^\theta h^\theta$ so conjugates map to conjugates.

Example 7: $\mathbf{S}_3$ is complete. The conjugacy classes of $\mathbf{S}_3$ are I, (×××) and (××).

Any automorphism must send (123) to one of two possibilities and must send (12) to one of three possibilities.

Since (123) and (12) generate $\mathbf{S}_3$ $|\mathrm{Aut}(\mathbf{S}_3)| \le 6$.

But $Z(\mathbf{S}_3)$ is trivial and so $|\mathrm{Inn}(\mathbf{S}_3)| = 6$.

Hence $\mathrm{Aut}(\mathbf{S}_3) = \mathrm{Inn}(\mathbf{S}_3)$.

Theorem 3: If θ is an automorphism of $\mathbf{S}_n$ that takes every transposition to a transposition then θ is an inner automorphism.

Proof: Let θ_b denote the inner automorphism $x \to b^{-1}xb$.

We prove, by induction on m, that for some $b \in \mathbf{S}_n$,

$$\theta\theta_b \text{ fixes } (12), (13), \ldots, (1\ m).$$

Then, putting $m = n$ we conclude that $\theta\theta_b = 1$ and so

$$\theta = \theta_b^{-1} \in \mathrm{Inn}(G).$$

We start the induction at $m = 2$.
Let $(12)^\theta = (h\ k)$ where $h < k$.
If $h = 1$ and $k = 2$ let $b = \mathrm{I}$.
If $h = 1$ and $k > 2$ let $b = (2\ k)$.
If $h > 1$ then $k > 2$. Let $b = (1\ h)(2\ k)$.
In each case $(12)^{\theta\theta_b} = (12)$.
Suppose $m \geq 2$ and the result holds for m. Let $\alpha = \theta\theta_b$.
Since (12), (13), …, $(1\ m)$ generate $\mathbf{S}_m$, regarded as a subgroup of $\mathbf{S}_n$, α restricted to $\mathbf{S}_m$ is the identity.
Now $(1\ m{+}1)^\alpha = (h\ k)$ for some h, k where $h < k$.
If $k \leq m$ then $(h\ k) \in \mathbf{S}_m$ and so $(h\ k)^\alpha = (h\ k)$, in which case $(h\ k) = (1\ m{+}1)$, a contradiction.
Hence $k \geq m + 1$.
$(1\ 2\ \ m{+}1)^\alpha = [(12)(1\ m{+}1)]^\alpha = (12)(h\ k)$.
Since $(12)(h\ k)$ must have order 3,
$h = 1$ or 2.
If $h = 1$ let $c = (m{+}1\ k)$.
Then $\theta\theta_b\theta_c = \theta\theta_{bc}$ fixes (12), (13), … $(1\ m)$ and $(1\ m{+}1)$.
If $h = 2$ let $c = (12)(m{+}1\ k)$. Then $\theta\theta_b\theta_c = \theta\theta_{bc}$ fixes (12), (13), … $(1\ m)$ and $(1\ m{+}1)$.

We are close to a proof that $\mathbf{S}_n$ is always complete. What is missing is showing that automorphisms take transpositions to transpositions. By Theorem 2, the simplest way to show this is to show that the number of transpositions is different to the size of any other conjugacy class in $\mathbf{S}_n$. This is true in all cases except $n = 6$. In fact $\mathbf{S}_6$ is not complete. $\mathbf{S}_2$ is also not complete, but for a different reason. It does not have trivial centre.

Theorem 4:

$\mathbf{S}_n$ is complete for all n except $n = 2$ and $n = 6$.

Proof: Clearly $\mathbf{S}_2$ is not complete since $Z(\mathbf{S}_2) > 1$.

I omit the proof that $\mathbf{S}_6$ has an outer automorphism.

Suppose $n \neq 2$ and $n \neq 6$. Then $Z(\mathbf{S}_n) = 1$.

Let Γ_k denote the conjugacy class consisting of all permutations in $\mathbf{S}_n$ that are products of k disjoint transpositions. For $k \leq n/2$,

$$|\Gamma_k| = \frac{n(n-1)\ ...\ (n-2k+1)}{2^k k!}$$

$$= |\Gamma_1|.\frac{(n-2)(n-3)\ ...\ (n-2k+1)}{2^{k-1}k!}$$

Since $2k \leq n$, $(n-2)(n-3) \dots (n-2k+1) \geq (2k-2)!$

Now we can prove by induction that if $k \geq 4$ then $(2k-2)! > k!2^{k-1}$ and so $|\Gamma_k| > |\Gamma_1|$.

Now $|\Gamma_3| = |\Gamma_1|.\dfrac{(n-2)(n-3)(n-4)(n-5)}{3.2.2.2}$.

Now $n \geq 6$. If $n > 6$ then $|\Gamma_3| \geq |\Gamma_1|.\dfrac{5.4.3.2}{3.2.2.2} > |\Gamma_1|$.

$|\Gamma_2| = |\Gamma_1|.\dfrac{(n-2)(n-3)}{4}$.

Now $n \geq 4$. If $n \geq 5$ then $|\Gamma_2| \geq |\Gamma_1|.\dfrac{6}{4} > |\Gamma_1|$.

If $n = 4$ then $|\Gamma_2| = \dfrac{|\Gamma_1|}{2} < |\Gamma_1|$.

So for $k > 1$, except for the case $n = 6$, $k = 3$, $|\Gamma_k| \neq |\Gamma_1|$.
(If $n = 6$ then $|\Gamma_3| = |\Gamma_1| = 15$.)

EXERCISES FOR CHAPTER 9

Exercise 1: For each of the following statements determine whether it is true or false.

(1) If G is any group, the map $x \to g^{-1}xg$ is an automorphism of G for all $g \in$ G.

(2) The map $\theta:\mathbf{S}_3 \to \mathbf{S}_3$ given by the following table is an automorphism of $\mathbf{S}_3$.

x	I	(123)	(132)	(12)	(23)	(13)
x^θ	I	(132)	(123)	(23)	(13)	(12)

(3) The map $x \to x^7$ is an automorphism of $\mathbf{S}_3$.

(4) $\text{Inn}(\mathbf{D}_{40}) \cong \mathbf{C}_{10} \times \mathbf{C}_2$.

(5) $\text{Aut}(\mathbf{C}_{62})$ is cyclic.

(6) $\text{Aut}(\mathbf{Q}_8) \cong \mathbf{S}_4$.

(7) If $n \geq 3$, $\mathbf{S}_n$ is complete.

(8) $\mathbf{D}_{14}$ is complete.

Exercise 2: Let G = $\langle A, B \mid A^{16}, B^4, BA = A^3B\rangle$.
Show that the map induced by $A^\theta = A^7$, $B^\theta = A^5B$ is an automorphism of G.

Exercise 3: Let G = $\langle A, B \mid A^{16}, B^4, BA = A^{-1}B\rangle$.
Show that the map induced by $A^\theta = AB$, $B^\theta = B$ is not an automorphism of G.

SOLUTIONS FOR CHAPTER 9

Exercise 1:

(1) TRUE

(2) FALSE: $[(12)(13)]^f = (123)^f = (132)$ while
$(12)^f(13)^f = (23)(12) = (123)$.

(3) TRUE: This is the identity map in disguise.

(4) FALSE: It is $\mathbf{C}_2 \times \mathbf{C}_2$.

(5) TRUE: $\mathrm{Aut}(C_{62}) \cong \mathbb{Z}_{62}^{\#} \cong \mathbb{Z}_2^{\#} \times \mathbb{Z}_{31}^{\#} \cong 1 \times \mathbf{C}_{30} \cong \mathbf{C}_{30}$.

(6) TRUE

(7) FALSE: $\mathbf{S}_6$ is not complete.

(8) TRUE: $Z(\mathbf{D}_{14}) = 1$ so $\mathrm{Inn}(\mathbf{D}_{14}) \cong \mathbf{D}_{14}$ and
$\mathrm{Aut}(\mathbf{D}_{14}) \cong \mathbf{D}_{14}$ whence $\mathrm{Aut}(\mathbf{D}_{14}) = \mathrm{Inn}(\mathbf{D}_{14})$.

Exercise 2: $(A^\theta)^{16} = (A^{16})^\theta = 1$.
$(B^\theta)^2 = (A^5B)^2 = A^5BA^5B = A^5A^{5.15}B^2 = A^{80}B^2 = B^2$.
Hence $(B^\theta)^2 \neq 1$ but $(B^\theta)^4 = 1$.
Finally $(B^\theta)(A^\theta) = A^5BA^7 = A^{5+21}B = A^{26}B = A^{10}B$ while
$(A^\theta)^3B^\theta = A^{21}A^5B = A^{26}B = A^{10}B$.
Since $\langle A^7, A^5B\rangle = G$, θ is an automorphism of G.

Exercise 3:
$(B^\theta)(A^\theta) = B(AB) = A^{-1}B^2 = A^{15}B^2$ while
$(A^\theta)^{-1}B^\theta = (AB)^{-1}B = B^{-1}A^{-1}B = AB^{-2} = AB^2$.