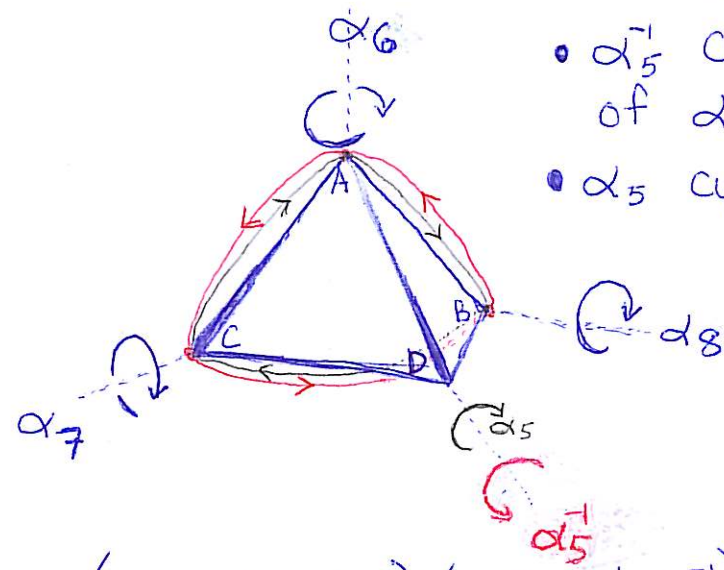
Inner Automorphism $\varphi_{\alpha_5}: x \to \alpha_5 x \alpha_5^{-1}$ on A_4



- α_5^{-1} cycles the axes of α_6, α_7, and α_8
- α_5 cycles them back

$$\varphi_{\alpha_5} = (\alpha_6 \alpha_8 \alpha_7)\underbrace{(\alpha_6^{-1} \alpha_8^{-1} \alpha_7^{-1})}_{(\alpha_{11} \alpha_{10} \alpha_{12})}(\alpha_2 \alpha_4 \alpha_3)$$

$\alpha_2 = (AB)(CD)$

$\alpha_3 = (AC)(BD)$

$\alpha_4 = (AD)(BC)$

Theorem 6.4 Aut(G) and Inn(G) are Groups

Proof sketch

Use a subgroup test.

1. show the identity bijection is in both Aut(G) and Inn(G).
   (Hint: Compute φ_e)
2. Show closure:
   (i) $f, g \in Aut(G) \Rightarrow fg \in Aut(G)$
   (ii) $\varphi_x, \varphi_y \in Inn(G) \Rightarrow \varphi_x \varphi_y \in Inn(G)$
3. Show inverses are present:
   (i) $f \in Aut(G) \Rightarrow f^{-1} \in Aut(G)$
   (ii) $\varphi_x \in Inn(G) \Rightarrow \varphi_y \in Inn(G)$
   where $(\varphi_x)^{-1} = \varphi_y$

Fact $Aut(\mathbb{Z}_8) \approx U(8)$

$\mathbb{Z}_8$	1	2	3	4	5	6	7	0
φ_1	**1**	2	3	4	5	6	7	0
φ_3	**3**	6	1	4	7	2	5	0
φ_5	**5**	2	7	4	1	6	3	0
φ_7	**7**	6	5	4	3	2	1	0

We construct the Cayley table of $Aut(\mathbb{Z}_8) = \{\varphi_1, \varphi_3, \varphi_5, \varphi_7\}$ by

(i) Recalling that the composition of automorphisms is an automorphism

(ii) Determining the resulting automorphism by the image of 1, because $\mathbb{Z}_8$ is cyclic.

$\varphi_1\varphi_3(1) = \varphi_1(3) = 3$ $\quad \varphi_1\varphi_5(1) = \varphi_1(5) = 5$ $\quad \varphi_1\varphi_7(1) = \varphi_1(7) = 7$

$\varphi_3\varphi_3(1) = \varphi_3(3) = 1$ $\quad \varphi_3\varphi_5(1) = \varphi_3(5) = 7$ $\quad \varphi_3\varphi_7(1) = \varphi_3(7) = 5$

$\varphi_5\varphi_3(1) = \varphi_5(3) = 7$ $\quad \varphi_5\varphi_5(1) = \varphi_5(5) = 1$ $\quad \varphi_5\varphi_7(1) = \varphi_5(7) = 3$

$\varphi_7\varphi_3(1) = \varphi_7(3) = 5$ $\quad \varphi_7\varphi_5(1) = \varphi_7(5) = 3$ $\quad \varphi_7\varphi_7(1) = \varphi_7(7) = 1$

$Aut(\mathbb{Z}_8)$	φ_1	φ_3	φ_5	φ_7
φ_1	φ_1	φ_3	φ_5	φ_7
φ_3	φ_3	φ_1	φ_7	φ_5
φ_5	φ_5	φ_7	φ_1	φ_3
φ_7	φ_7	φ_5	φ_3	φ_1

$U(8)$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

Theorem 6.5 When $n \in \mathbb{Z}^+$, $Aut(\mathbb{Z}_n) \approx U(n)$

Lemma An automorphism $\alpha \in Aut(\mathbb{Z}_n)$ is completely determined by $\alpha(1)$.

Proof $\mathbb{Z}_n$ is cyclic. So for any $x \in \mathbb{Z}_n$,

$$\begin{aligned}\alpha(x) &= \alpha(x \cdot 1)\\ &= x \cdot \alpha(1) \quad \text{Theorem 6.2 Part 2.}\end{aligned}$$

Therefore $\alpha(1) = \beta(1) \Rightarrow \alpha = \beta$.

Proof of Thm 6.5 (sketch)

Define

$$T : Aut(\mathbb{Z}_n) \to U(n)$$

by

$$T(\alpha) = \alpha(1)$$

T 1-1: By the lemma.

T onto: if $r \in U(n)$ then

$$\begin{aligned}\alpha &: \mathbb{Z}_n \to \mathbb{Z}_n\\ \alpha(1) &= r\\ \alpha(s) &= sr \pmod{n}\end{aligned}$$

is an automorphism of $\mathbb{Z}_n$ with $T(\alpha) = r$.

T operation preserving:

$$\begin{aligned}T(\alpha\beta) = (\alpha\beta)(1) &= \alpha(\beta(1)) \quad \text{fxn composition}\\ &= \alpha(\underbrace{1+1+\cdots+1}_{\beta(1)\text{ times}})\\ &= \underbrace{\alpha(1)+\alpha(1)+\cdots+\alpha(1)}_{\beta(1)\text{ times}} \quad \text{Thm 6.2 Part 2}\\ &= \alpha(1)\beta(1) = T(\alpha)T(\beta)\end{aligned}$$

$\square$