

To begin with

$$\text{LATEX!} f(x, y) = \left( \frac{2|x| + 2|y|}{2} \right)$$

$$\cos a - \cos b = -2 \sin\left(\frac{a+b}{2}\right) \sin\left(\frac{a-b}{2}\right)$$

$$Q : (Aut\mathbb{Z}_{11}^*, \circ) \cong (\mathbb{Z}_4, +).$$

(In actuality,  $Aut\mathbb{Z} \cong \mathbb{Z}_2$ ,  $Aut\mathbb{Z}_6 \cong \mathbb{Z}_2$ ,  $Aut\mathbb{Z}_8 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$ ,  $Aut\mathbb{Z}_p \cong \mathbb{Z}_{p-1}$  for prime  $p$ .)

*Proof :*

(i)

$$2^0 = 1, 2^1 = 2, 2^2 = 4, 2^3 = 8, 2^4 = 5, 2^5 = 10, 2^6 = 9, 2^7 = 7, 2^8 = 3, 2^9 = 6, 2^{10} = 1, \min\{s \in \mathbb{N} \mid 2^s = 1\} = 10.$$

$$\therefore (\mathbb{Z}_{11}^*, \cdot) = (< 2 >, \cdot) \text{ is cyclic, } 1 \in B := \{s \in \mathbb{N} \cap [1, 9] \mid (\mathbb{Z}_{11}^*, \cdot) = (< 2^s >, \cdot)\} \neq \emptyset.$$

(In reality,  $p$  is prime  $\Rightarrow (\mathbb{Z}_p^*, \cdot)$  is cyclic.)

(ii)

$$s \in B \equiv \exists n \in \mathbb{Z} \text{ s.t. } (2^s)^n = 2 \equiv 10 \mid sn - 1 \equiv \exists m \in \mathbb{Z} \text{ s.t. } sn + 10m = 1 \equiv \gcd(s, 10) = 1 \equiv s \in \{1, 3, 7, 9\};$$

that is,  $2 = 2^1, 6 = 2^9, 7 = 2^7, 8 = 2^3$  are the generators of  $\mathbb{Z}_{11}^*$ .

(iii)

$$\forall \rho \in Aut\mathbb{Z}_{11}^*, < 2 > = Aut\mathbb{Z}_{11}^* = < \rho(2) > \equiv \rho(2) \in \{2, 6, 7, 8\}.$$

Define  $\rho_{26} : \mathbb{Z}_{11}^* \longrightarrow \mathbb{Z}_{11}^* : \rho_{26}(2^i) = 6^i$ , where  $i \in \mathbb{Z} \cap [0, 9]$ .  $\therefore \rho_{26}$  is surjective immediately.

Claim  $\rho_{26} \in Aut\mathbb{Z}_{11}^*$ .

$$\forall i, j \in \mathbb{Z} \cap [0, 9], 2^i = 2^j \Leftrightarrow 2^{i-j} = 1 \Leftrightarrow 10 \mid i - j \Leftrightarrow 6^{i-j} = 1 \Leftrightarrow 6^i = 6^j,$$

where  $i - j = 10q + r$  for some  $q \in \mathbb{Z}, r \in \mathbb{Z} \cap [0, 9] \Rightarrow r = 0$ ;  $\rho_{26}$  is well-defined and injective.

$$\therefore < 6 > = Aut\mathbb{Z}_{11}^*, \rho_{26}(2^i \cdot 2^j) = \rho_{26}(2^{i+j}) = 6^{i+j} = 6^i \cdot 6^j = \rho_{26}(2^i) \cdot \rho_{26}(2^j), \therefore \rho_{26} \text{ is an epimorphism.}$$

(iv)

Analogously, define  $\rho_{22}, \rho_{27}, \rho_{28} : \mathbb{Z}_{11}^* \longrightarrow \mathbb{Z}_{11}^* : \rho_{22}(2^i) = 2^i, \rho_{27}(2^i) = 7^i, \rho_{28}(2^i) = 8^i$ , where  $i \in \mathbb{Z} \cap [0, 9]$ .

Subsequently, similar to  $\rho_{26}$ ,  $\rho_{22} (= \iota)$ ,  $\rho_{27}$  and  $\rho_{28}$  are distinct automorphisms,  $\therefore \rho \in \{\iota, \rho_{26}, \rho_{27}, \rho_{28}\}$ .

$$\therefore Aut\mathbb{Z}_{11}^* = \{\iota, \rho_{26}, \rho_{27}, \rho_{28}\}. \text{ Now note } \rho_{27}^2(2) = \rho_{27}(7) = \rho_{27}(2^7) = 7^7 = 6 \neq 2, \therefore \rho_{27}^2 \neq \iota, |\rho_{27}| \neq 2.$$

Hence, Klein 4-group  $\not\cong Aut\mathbb{Z}_{11}^* \cong \mathbb{Z}_4$ .

(Alternatively, define  $\lambda : Aut\mathbb{Z}_{11}^* \longrightarrow \mathbb{Z}_4 : \iota \mapsto 0, \rho_{26} \mapsto 2, \rho_{27} \mapsto 1, \rho_{28} \mapsto 3$ .

$\therefore \lambda$  is bijective immediately. Claim  $\lambda$  is a homomorphism.

The operation preservation between  $\iota$  and  $\rho'_{2k}$ s is trivial.

$$\lambda(\rho_{26} \circ \rho_{27}) = \lambda(\rho_{28}) = 3 = 2 + 1 = \lambda(\rho_{26}) + \lambda(\rho_{27}), \lambda(\rho_{27} \circ \rho_{26}) = \lambda(\rho_{28}) = 3 = 1 + 2 = \lambda(\rho_{27}) + \lambda(\rho_{26}),$$

$$\lambda(\rho_{26} \circ \rho_{28}) = \lambda(\rho_{27}) = 1 = 2 + 3 = \lambda(\rho_{26}) + \lambda(\rho_{28}), \lambda(\rho_{28} \circ \rho_{26}) = \lambda(\rho_{27}) = 1 = 3 + 2 = \lambda(\rho_{28}) + \lambda(\rho_{26}),$$

$$\lambda(\rho_{27} \circ \rho_{28}) = \lambda(\iota) = 0 = 1 + 3 = \lambda(\rho_{27}) + \lambda(\rho_{28}), \lambda(\rho_{28} \circ \rho_{27}) = \lambda(\iota) = 0 = 3 + 1 = \lambda(\rho_{28}) + \lambda(\rho_{27}).$$

Thus,  $\lambda$  is an isomorphism,  $Aut\mathbb{Z}_{11}^* \cong \mathbb{Z}_4$ .)