Euler ϕ-function is a map $\phi : \mathbb{N} \to \mathbb{N}$ defined by

$$\phi(n) = \begin{cases} 1 & \text{if } n = 1 \\ \#\text{ of } m \text{ s.t. } 1 \le m \le n \text{ and } \gcd(m,n) = 1 \end{cases}$$

Note: we know that $|U(n)| = \phi(n)$ ← group of units in $\mathbb{Z}_n$

$|U(n)|$ = # of m $(1 \le m \le n)$ s.t. $\gcd(m,n) = 1$

Thm $\phi(n) = |U(n)|$, $U(n)$ - group of units modulo n.

Ex $U(12) = \{1, 5, 7, 11\}$, $\phi(12) = |U(12)| = 4$

If p is prime $\phi(p) = p - 1$

Thm. (Euler Thm.): Let a and n be integers s.t. $n > 0$ and $\gcd(a,n) = 1$. Then

$$a^{\phi(n)} \equiv 1 \pmod{n}$$

Proof: Since $|U(n)| = \phi(n) \Rightarrow b^{\phi(n)} = 1$ $\forall b \in U(n)$ "element to power of order of group = identity"

and since a with $\gcd(a,n) = 1 \Rightarrow a \in U(n)$

$a^{\phi(n)} = 1$ ∎

Thm (Fermats Little Thm). Let p be any prime number and suppose that $p \nmid a$. Then

$$a^{p-1} \equiv 1 \pmod p$$

Furthermore for any $b \in \mathbb{Z}$, $b^p \equiv b \pmod p$.

Proof: Since p is prime, $\Rightarrow \phi(p) = p-1$

By Eulers ϕ thm $a^{\phi(p)} \equiv 1 \pmod p$ since $p \nmid a$ meaning $a \not\equiv 0 \mod p$ (and $\gcd(a,p)=1$)

multiplying both sides by a

$\Rightarrow a^p \equiv a \mod p$, still true if $a \equiv 0 \mod p$ ∎

Isomorphisms

Two Groups $(G, \cdot)$, $(H, \circ)$ are isomorphic if $\exists$ a 1-1 and onto map $\phi : G \to H$ such that the group operation is perserved, i.e. $\forall a, b \in G$

$$\phi(a \cdot b) = \phi(a) \circ \phi(b)$$

ϕ is called an isomorphism.

write $G \simeq H$ or $G \cong H$.

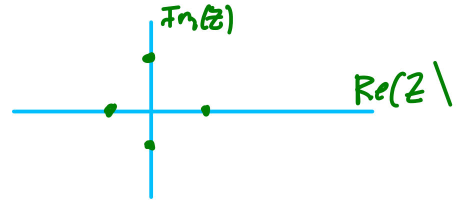
Ex] Show $\mathbb{Z}_4 \simeq \langle i \rangle$ = the 4^{th} roots of unity

i.e. complex solutions of $z^4 = 1$

$= \{1, -1, i, -i\}$

$\mathbb{Z}_4 = \{0,1,2,3\}$

$\uparrow$ add mod 4



Define a map $\phi : \mathbb{Z}_4 \to \langle i \rangle$

$: n \mapsto i^n$

$\phi(0) = 1$

$\phi(1) = i$

$\phi(2) = -1$

$\phi(3) = -i$

$$\phi(m+n) = i^{m+n} = i^m i^n = \phi(m)\phi(n)$$

Ex] $\phi : (\mathbb{R}, +) \longrightarrow (\mathbb{R}^+, \cdot)$

$x \mapsto e^x$

By calculus this 1-1 and onto.

$$\phi(x+y) = e^{x+y} = e^x e^y = \phi(x)\phi(y).$$

Ex] $|\mathbb{Z}_8| \neq |\mathbb{Z}_{12}| \therefore \mathbb{Z}_8 \not\simeq \mathbb{Z}_{12}$

$U(8) \simeq U(12)$

$U(8) = \{1,3,5,7\}$ $\quad$ $U(12) = \{1,5,7,11\}$

$\phi : 1 \mapsto 1$
$3 \mapsto 5$
$5 \mapsto 7$
$7 \mapsto 11$

$$\begin{aligned}\phi(3\cdot 5 \bmod 8) &= \phi(7 \bmod 8)\\ &= 11 \bmod 12\\ &= 35 \bmod 12\\ &= 5\cdot 7 \bmod 12\\ &= \phi(3 \bmod 8)\cdot\phi(5 \bmod 8)\end{aligned}$$

Ex] $|S_3| = |\mathbb{Z}_6|$, $\mathbb{Z}_6 \not\cong S_3$

Proof:

Suppose $\exists$ an isomorphism $\phi : \mathbb{Z}_6 \to S_3$

Let $a, b \in S_3$ s.t. $ab \neq ba$.

Since ϕ is an isomorphism then $\exists$

$\phi(m) = a$, $\phi(n) = b$

$$ab = \phi(m)\phi(n) = \phi(m+n) = \phi(n+m) = \phi(n)\phi(m) = ba.$$

This is a contradiction

$\therefore$ no isomorphism exists ■

Thm/ Let $\phi : G \to H$ be an isomorphism of Groups, we have

1) $\phi^{-1} : H \to G$ is an isomorphism

2) $|G| = |H|$

3) G is abelian iff H is abelian

4) G is cyclic iff H is cyclic

If $G = \langle a \rangle$
$\Updownarrow$
$H = \langle \phi(a) \rangle$ since
$\phi(a^n) = \phi(a)^n$

5) G has a subgroup of order n iff H has a subgroup of order n.

Proof (3)

Suppose G is abelian

$\Rightarrow g_1 g_2 = g_2 g_1 \quad \forall g_1, g_2 \in G$

ϕ is a isomorphism $\therefore$ bijective $\therefore$ $\phi(g_1) = h_1$, $\phi(g_2) = h_2$

and all $h_1, h_2 \in H$ have this form (for some g_1, g_2)

for some $g_1, g_2 \in G$

$$h_1 h_2 = \phi(g_1)\phi(g_2) = \phi(g_1 g_2) = \phi(g_2 g_1) = \phi(g_2)\phi(g_1)$$
$$= h_2 h_1$$

∎

Thm All cyclic groups of infinite order are isomorphic to $(\mathbb{Z}, +)$.

Proof: Let $G = \langle a \rangle$ be a cyclic group of infinite order $|G| = |a| = \infty$

Define a map

$$\phi : \mathbb{Z} \to G$$
$$n \mapsto a^n$$

Then

$$\phi(m+n) = a^{m+n} = a^m a^n = \phi(m)\,\phi(n)$$

Let $m, n \in \mathbb{Z}$, $m \neq n$, $m > n$

Suppose $\phi(m) = \phi(n) \Leftrightarrow a^m = a^n \Rightarrow a^{m-n} = e$ identity in G

and $m - n > 0$

This is a contradiction of fact $|a| = \infty$

$\therefore \phi$ is 1-1

Since G is cyclic for all $g \in G$ $\quad g = a^n = \phi(n)$

$\therefore\ \phi$ is onto.

Thm/ If G is a cyclic group of order n then $G \simeq \mathbb{Z}_n$

proof: Let $G = \langle a \rangle$, $a \in G$, $|a| = n$

$$\phi : \mathbb{Z}_n \longrightarrow G$$
$$k \mapsto a^k$$

$k_1, k_2 \in \mathbb{Z}_n$

$\hat{k}_1 + \hat{k}_2 + cn = k_1 + k_2 \mod n$

for $0 \le \hat{k}_1, \hat{k}_2 < n$

$$\phi(\hat{k}_1 + \hat{k}_2 \bmod n) = \phi(\hat{k}_1 + \hat{k}_2 + cn)$$
$$= a^{\hat{k}_1 + \hat{k}_2 + cn}$$
$$= a^{\hat{k}_1} a^{\hat{k}_2} a^{cn} = a^{\hat{k}_1} a^{\hat{k}_2} = \phi(\hat{k}_1 \bmod n)\,\phi(\hat{k}_2 \bmod n)$$

$\blacksquare$

Cor./ If $|G| = p$, where p is prime, then $G \simeq \mathbb{Z}_p$

Proof/ if p is prime $|G| = p \Rightarrow G$ is cyclic. $\blacksquare$

Previous thm

Thm/ The isomorphism of groups determines an equivalence relation on the class of all groups.

Proof: Homework.