Group Theory

Next Topic:

Multiplication Modulo n Group (U_n)

(U_n = The Group of Units in the Integers mod n)

Instructor:

Deepak Poonia

IISc Bangalore

GATE CSE AIR 53; AIR 67;
AIR 107; AIR 206; AIR 256

Discrete Mathematics Complete Course:

https://www.goclasses.in/courses/Discrete-Mathematics-Course

Join **GO+ GO Classes Combined Test Series** for BEST quality tests, matching GATE CSE Level:

Visit www.gateoverflow.in website to join Test Series.

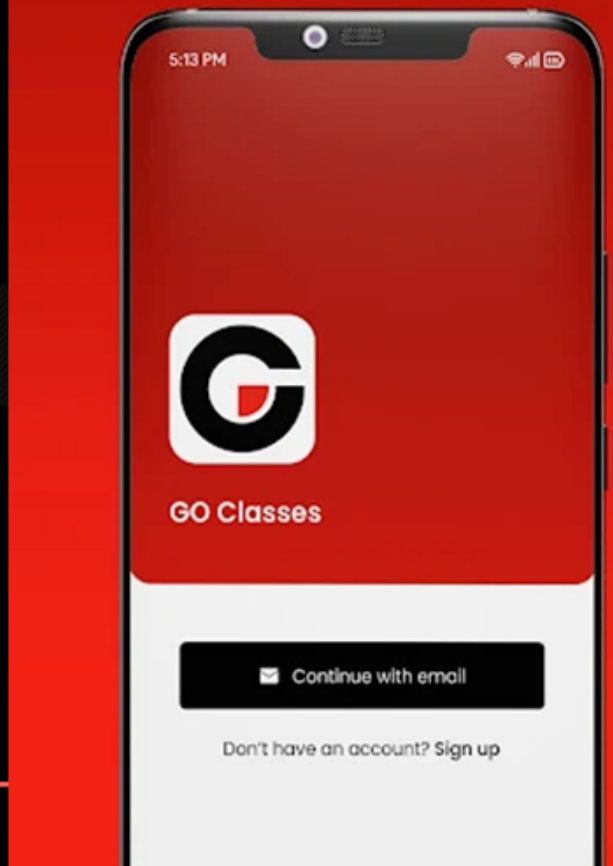
1. **Quality Questions:** No Ambiguity in Questions, All Well-framed questions.
2. Correct, **Detailed Explanation**, Covering Variations of questions.
3. **Video Solutions.**

https://gateoverflow.in/blog/14987/gate-overflow-and-go-classes-test-series-gate-cse-2024

Download the GO Classes Android App:

https://play.google.com/store/apps/details?id=com.goclasses.courses

Search "GO Classes" on Play Store.



NOTE :

Complete Discrete Mathematics & Complete Engineering

Mathematics Courses, by GO Classes, are **FREE** for ALL learners.

Visit here to watch : https://www.goclasses.in/s/store/

SignUp/Login on Goclasses website for free and start learning.

We are on Telegram. **Contact us** for any help.

Link in the Description!!

Join GO Classes **Doubt Discussion** Telegram Group :

Username:

@GATECSE_Goclasses

We are on Telegram. **Contact us** for any help.

Join GO Classes Telegram Channel, Username: @GOCLASSES_CSE

Join GO Classes **Doubt Discussion** Telegram Group :

Username: @GATECSE_Goclasses

(Any doubt related to Goclasses Courses can also be asked here.)

Join GATEOverflow Doubt Discussion Telegram Group :

Username: @GateOverflow_CSE

A Small Topic:

Coprime Integers Or Relatively Prime

Coprime Or Relatively Prime:

In number theory, two integers a and b are coprime Or relatively prime Or mutually prime if the only positive integer that is a divisor of both of them is 1.

Or

DEFINITION 3 The integers *a* and *b* are *relatively prime* if their greatest common divisor is 1.

Int a, b

a, b are coprime iff GCD(a, b) = 1

9, 10 are Co-prime. GCD(9, 10) = 1

6, 10 are not Co-prime. GCD(6, 10) = 2 ≠ 1

Coprime Or Relatively Prime:

In number theory, two integers a and b are coprime Or relatively prime Or mutually prime if the only positive integer that is a divisor of both of them is 1.

The numbers 8 and 9 are coprime, despite the fact that neither considered individually is a prime number, since 1 is their only common divisor. On the other hand, 6 and 9 are not coprime, because they are both divisible by 3.

Coprime Or Relatively Prime:

Q: Which positive integers less than 12 are relatively prime to 12?

Coprime Or Relatively Prime:

Q: Which positive integers less than 12 are relatively prime to 12? ⇒ 1, 5, 7, 11

1 ✓, 2 ✗, 3 ✗, 4 ✗, 5 ✓, 6 ✗, 7 ✓, 8 ✗, 9 ✗, 10 ✗, 11 ✓

GCD(5,12) = 1 ; GCD(6,12) = 6

Coprime Or Relatively Prime:

Q: Which positive integers less than 9 are relatively prime to 9 ?

Coprime Or Relatively Prime:

Q: Which positive integers less than 9 are relatively prime to 9 ? ⇛ 1, 2, 4, 5, 7, 8

GCD (6, 9) = 3

✓ 1, ✓ 2, ✗ 3, ✓ 4, ✓ 5, ✗ 6, ✓ 7, ✓ 8

GCD(3,9) = 3 ≠ 1 ; GCD (9,4) = 1

Coprime Or Relatively Prime:

Q: Which positive integers less than 30 are relatively prime to 30? ⇒ 1, 7, 11, 13, 17, 19, 23, 29

✓ 1, ✗ 2, ✗ 3, ✗ 4, ✗ 5, ✗ 6, ✓ 7, ✗ 8, ✗ 9, ✗ 10, ✓ 11, ✗ 12, ✓ 13

✗ 14, ✗ 15, ✓ 17, ✓ 19, ✗ 21, ✓ 23, ✗ 25, ✗ 27, ✓ 29

Coprime Or Relatively Prime:

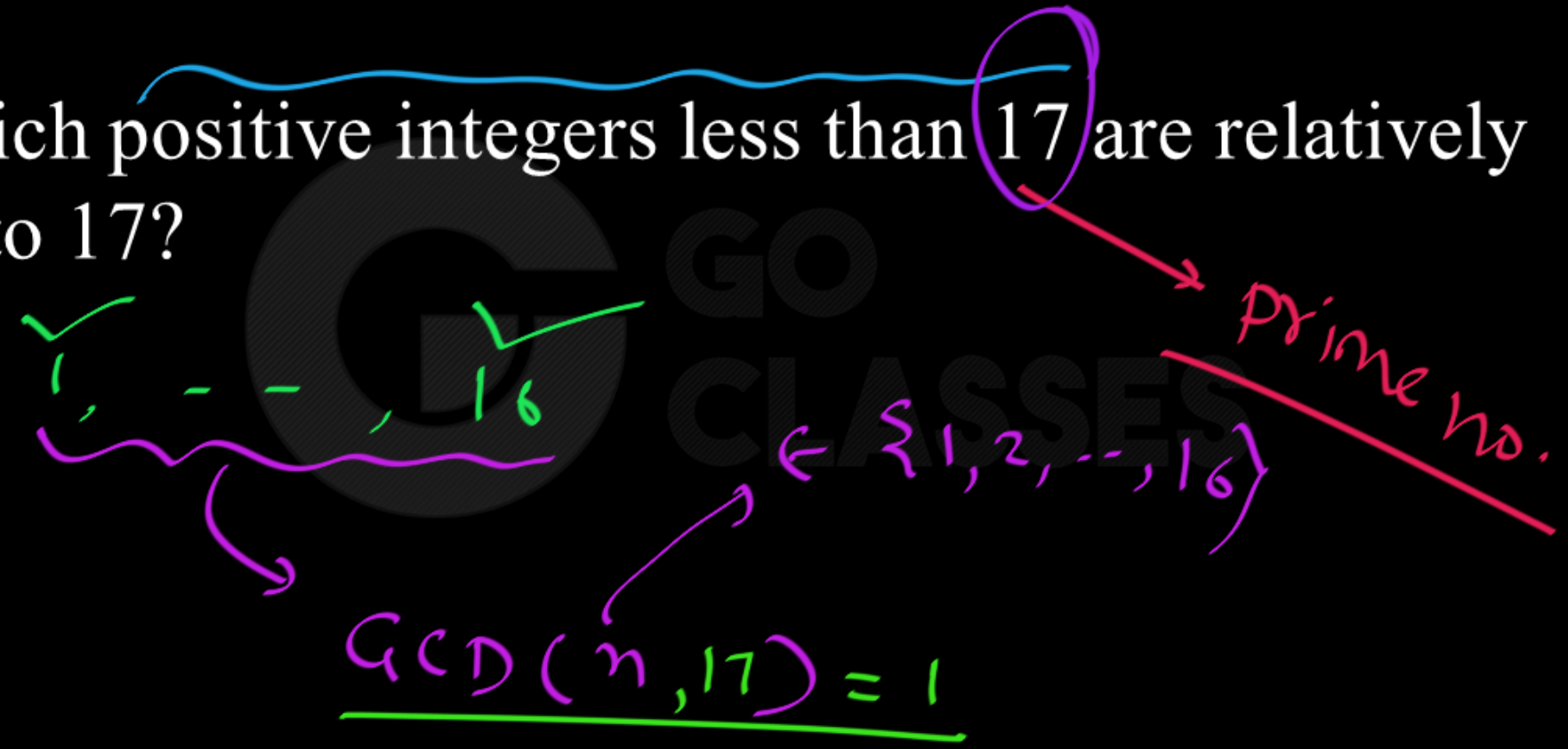
Q: Which positive integers less than 7 are relatively prime to 7?

1, 2, 3, 4, 5, 6

prime number

Coprime Or Relatively Prime:

Q: Which positive integers less than 17 are relatively prime to 17?



Coprime Or Relatively Prime:

Q: Which positive integers less than P are relatively prime to P (where P is a prime number)?

Coprime Or Relatively Prime:

Q: Is a prime number P always co-prime with n if $1 \leq n < P$?

Prime no. P is coprime with each of them

$\overline{1}, \overline{2}, \ldots, \overline{P-1}$

Next Topic:

Multiplication Modulo n Group (U_n)

(U_n = The Group of Units in the Integers mod n)

We have already seen the Addition Modulo n Group

Definition 2.9. [3] *The set* $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$ *for* $n \geq 1$ *is a group under addition modulo* n. *For any* i *in* $\mathbb{Z}_n$, *the inverse of* i *is* $n - i$. *This group is usually referred to as* ***the group of integers modulo n***.

The group $\mathbb{Z}_n$ consists of the elements $\{0, 1, 2, \ldots, n-1\}$ with *addition* mod n as the operation.

$$Z_n = \{0, 1, 2, \ldots, n-1\}$$

$(Z_n, \oplus_n)$ group.

$$a \oplus_n b = (a+b) \bmod n$$

$(Z_4$, Addition Mod 4)

$Z_4 = \{0, 1, 2, 3\} = \{0, 1, \cdots, 4-1\}$ $\oplus_4$

$3 \oplus_4 2 = (3+2) \bmod 4 = 5 \bmod 4 = 1$

$3 \oplus_4 3 = (3+3) \bmod 4 = 6 \bmod 4 = 2$

$2 \oplus_4 2 = 0$ & $3 \oplus_4 0 = 3$

$(Z_4 = \{0, 1, 2, 3\}, \oplus_4)$ → Group

$\otimes_4$

Can we Multiply elements of Z_4 ?

i.e. What is $(Z_4 , \text{Mul Mod } 4)$

$Z_4 = \{0, 1, 2, 3\}$

$\otimes_4$

a Group ?

$a \otimes_4 b = (a \times b) \bmod 4$

$Z_4 = \{0, 1, 2, 3\}$, $\otimes_4$ → mul mod 4

$a \otimes_4 b = (a \times b) \bmod 4$

$3 \otimes_4 2 = (3 \times 2) \bmod 4 = 6 \bmod 4 = 2$

$3 \otimes_4 3 = 9 \bmod 4 = 1$

$2 \otimes_4 1 = 2$

$Z_4 = \{0, 1, 2, 3\}$, $\otimes_4$

(1) Closure ✓

$a \otimes_4 b = (a \times b) \bmod 4$

(2) Associative: $\otimes_n$ is Asso.

0, 1, 2, 3

(3) Identity:

$e = 1$

$a \otimes_4 1 = a \bmod 4 = a$

$(Z_4, \otimes_4)$ → Closed ✓ Asso ✓ Identity ✓

$Z_4 = \{0, 1, 2, 3\}$

$0 \otimes_4 ? = 1$

$0^{-1} = DNE$

No inverse property

$0 \otimes_4 a = 0 \bmod 4 = 0$

$2^{-1} = DNE$

$Z_4 = \{0, 1, 2, 3\}$; $\otimes_4$

2^{-1} ?

$2 \otimes_4 0 \neq 1$ ↷ e

$2 \otimes_4 1 = 2 \neq e$

$2 \otimes_4 2 = 0 \neq e$

$2 \otimes_4 3 = 2 \neq e$

2^{-1} = DNE

$1^{-1} = 1$ ✓

$e^{-1} = e$

$3^{-1} = 3$

$(Z_4 = \{0, 1, 2, 3\}, \otimes_4)$

0^{-1} : DNE

2^{-1} = DNE

$1^{-1} = 1$

$3^{-1} = 3$

Monoid (Commutative monoid)

Closed ✓
Asso ✓
Identity $e = 1$ ✓
Inverse ✗
Commutative ✓

$3 \otimes_4 3 = 9 \bmod 4 = 1 \neq e$

Hence we have shown that $(\mathbb{Z}_n, \otimes)$ is a commutative semigroup with identity.

This semigroup fails to be a group since the inverse of the elements does not always exist as we see in the following example.
Consider $\mathbb{Z}_4 = \{0, 1, 2, 3\}$ with the multiplication table

$* \, mod \, n$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

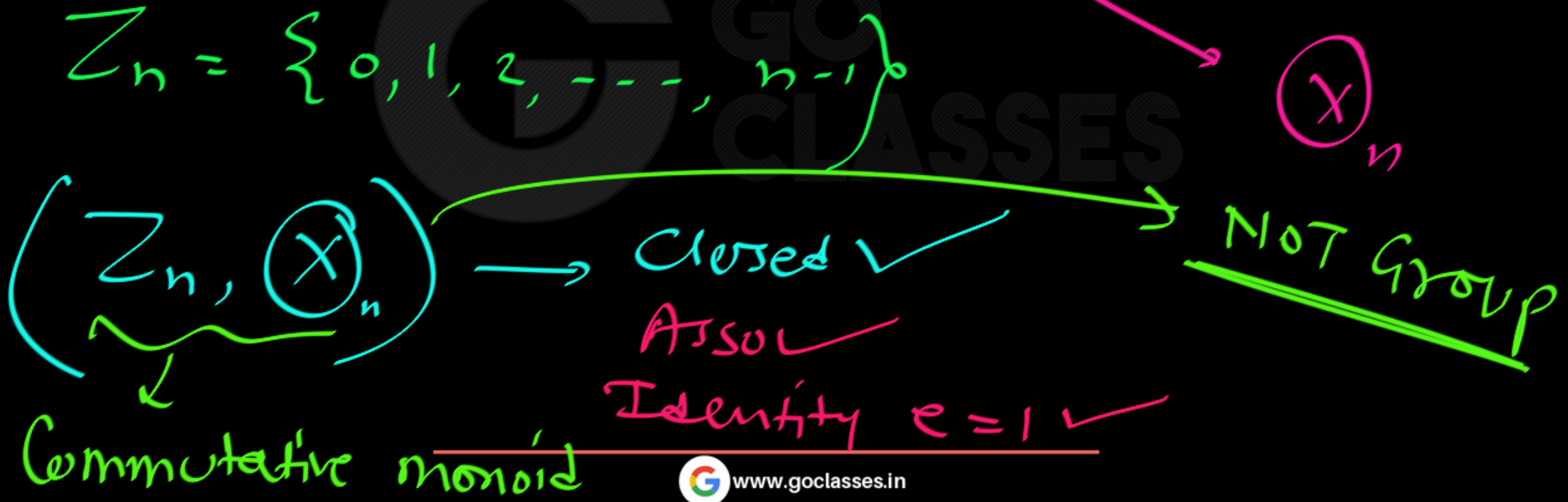
From this table we see that $3^{-1} = 3, 1^{-1} = 1$, but 0^{-1} and 2^{-1} are not exist.

Can we Multiply elements of Z_n ?

i.e. What is (Z_n , Mul Mod n)

Can we Multiply elements of Z_n ?

i.e. What is (Z_n , Mul Mod n)



Can we Multiply elements of Z_n ?

i.e. What is (Z_n , Mul Mod n)

The group $\mathbb{Z}_n$ consists of the elements $\{0, 1, 2, \ldots, n-1\}$ with *addition* mod n as the operation. You can also *multiply* elements of $\mathbb{Z}_n$, but you do not obtain a group: The element 0 does not have a multiplicative inverse, for instance.

$(Z_n, \otimes_n)$ → Monoid

→ Not a Group

Closed ✓

Asso ✓

$e = 1$ ✓

Problem: Inverse Property ✓

An Interesting Question:

How to Convert Z_n into a Group under Multiplication Mod n Operation??


x'
n
mul mod n
inverse ≡ multiplicative inverse

Consider Z_4 Again under Mul Mod 4

$(Z_4$, Mul Mod 4)

$Z_4 = \{0, 1, 2, 3\}$, $\otimes_4$

0^{-1} : DNE

2^{-1} : DNE

} problem

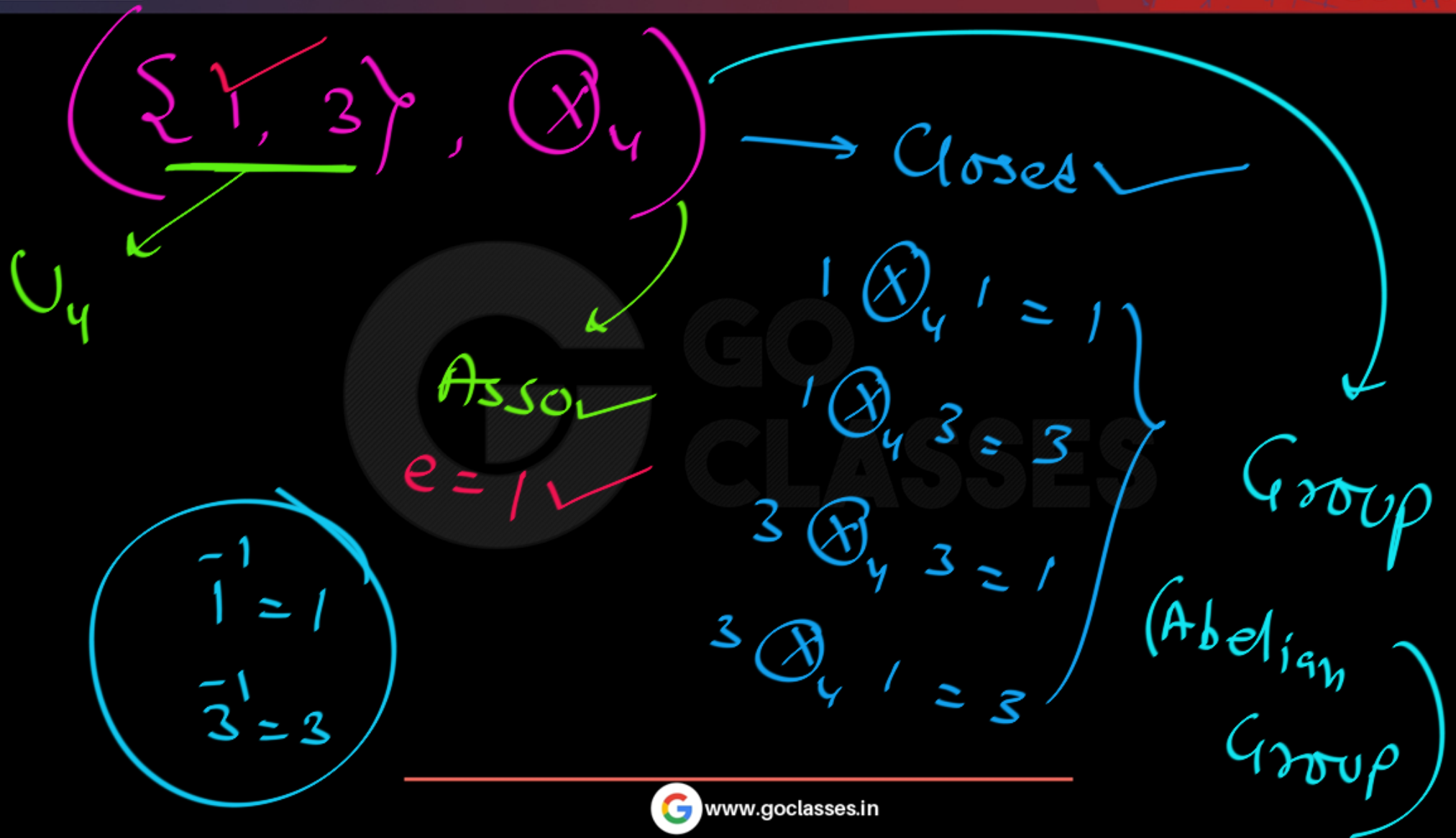
$3^{-1} = 3$

$1^{-1} = 1$

U_4

$(\{1, 3\}, \otimes_4)$

Group


$(\{1, 3\}, \otimes_4)$
U_4
Closed
Assoc
$e = 1$
$1 \otimes_4 1 = 1$
$1 \otimes_4 3 = 3$
$3 \otimes_4 3 = 1$
$3 \otimes_4 1 = 3$
Group
(Abelian Group
$1^{-1} = 1$
$3^{-1} = 3$

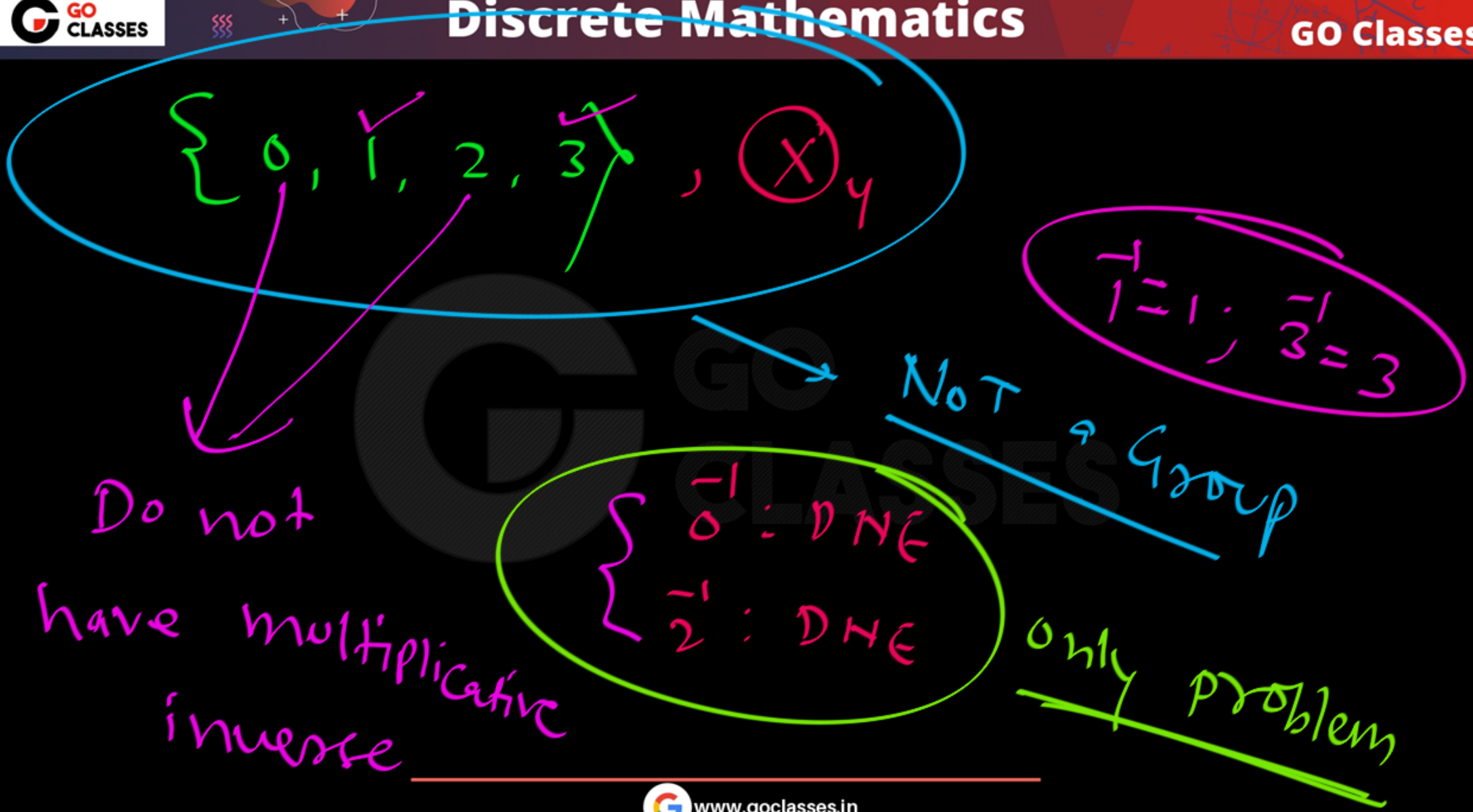
$(Z_4 = \{0, 1, 2, 3\}, \oplus_4)$ → Group

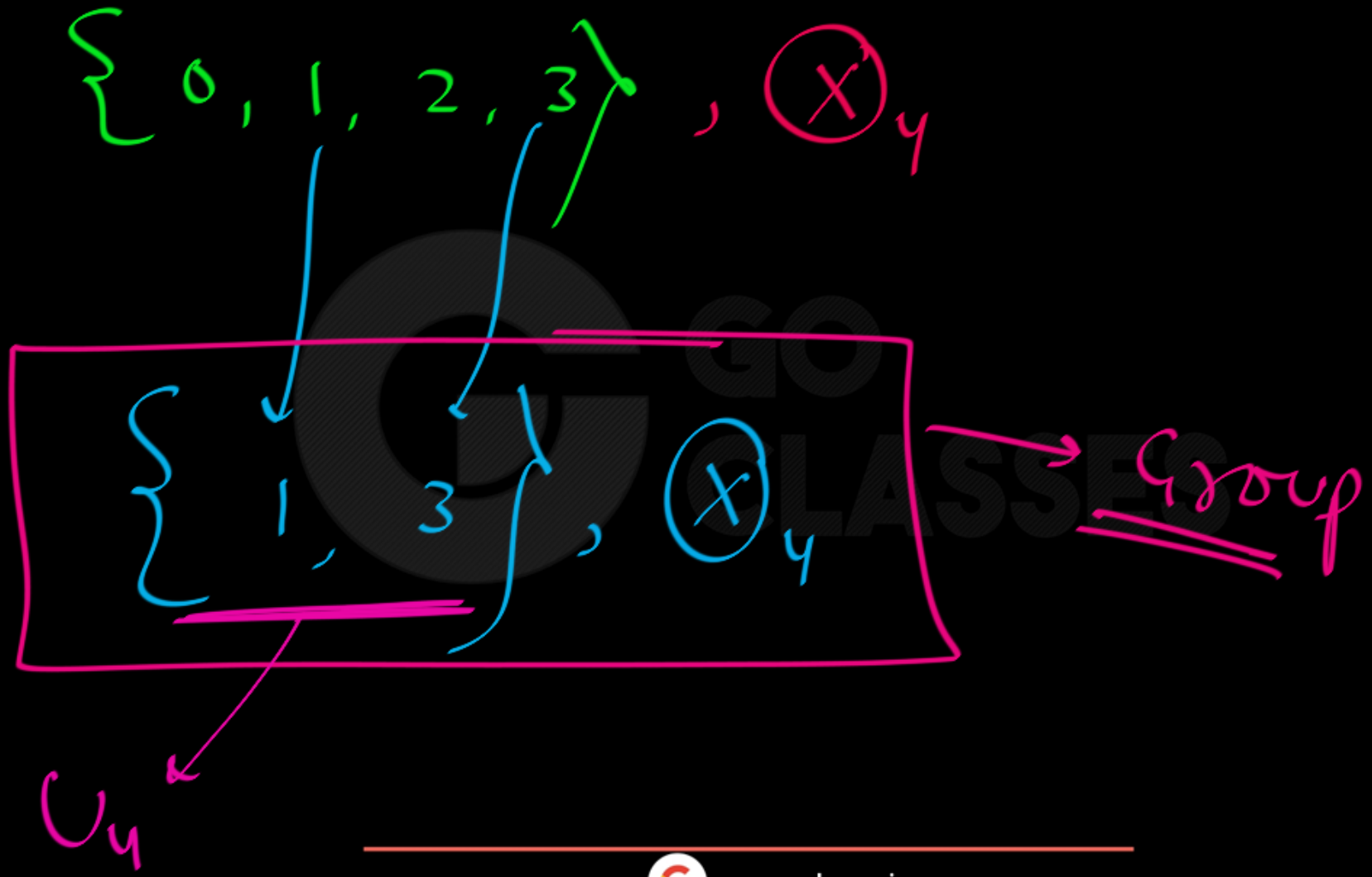
$(Z_4, \otimes_4)$ — Monoid but not Group

→ No inverse property

Convert !

→ Group ?


{0, 1, 2, 3}, ×4
Do not have multiplicative inverse
Not a Group
1⁻¹ = 1 ; 3⁻¹ = 3
0⁻¹ : DNE
2⁻¹ : DNE
only problem


{0, 1, 2, 3}
, $\otimes_4$
{1, 3}
, $\otimes_4$
Group
U_4

Z_4 :

0

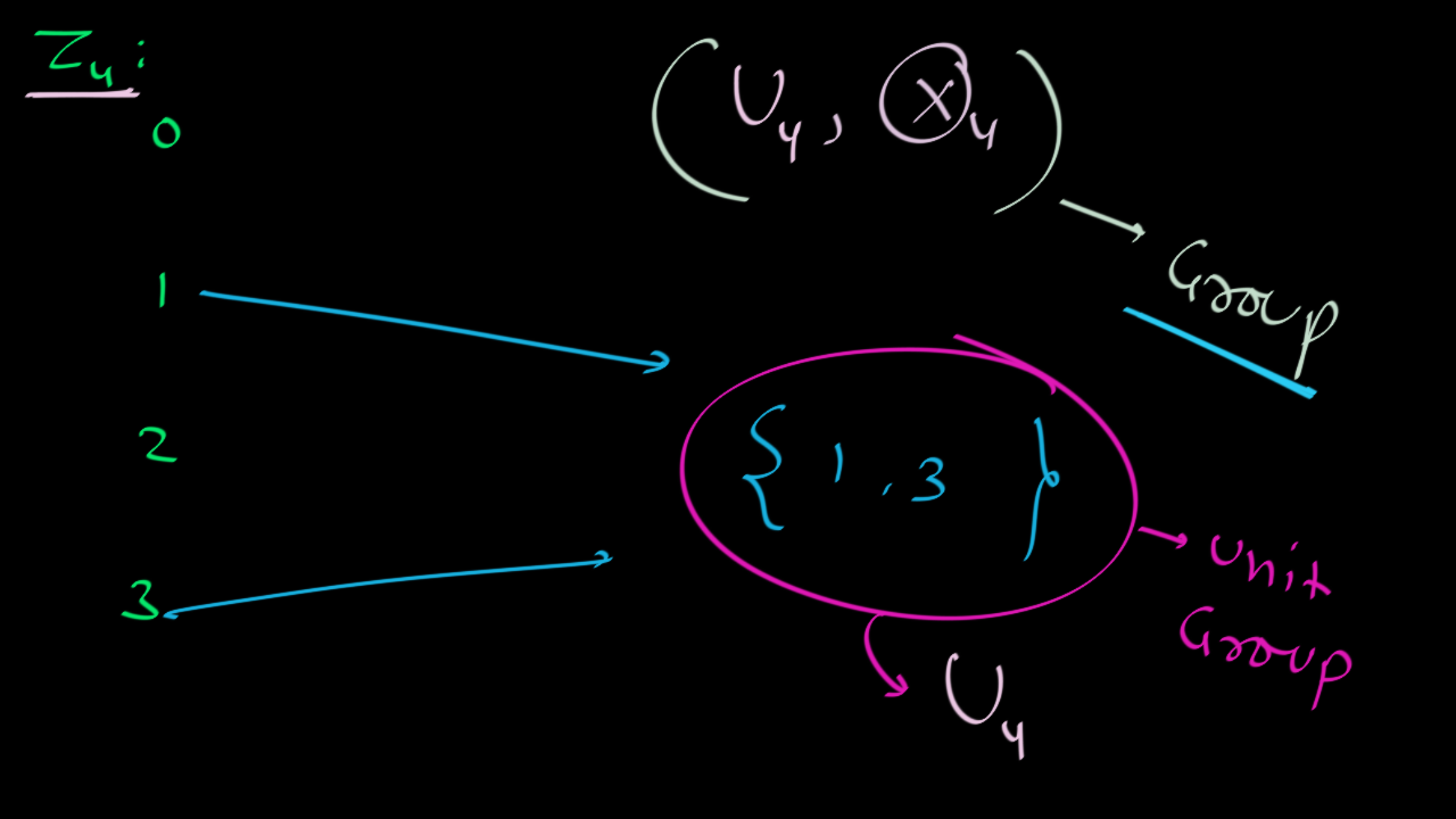
opn : $\otimes_4$

1 → has multiplicative inverse

2

3 → has mul. inverse

unit


Z_4 :
0
1
2
3
$(U_4, \otimes_4)$
Group
$\{1, 3\}$
Unit Group
U_4

Consider Z_6 under Mul Mod 6

$(Z_6$, Mul Mod 6)

$(Z_6 = \{0, 1, 2, 3, 4, 5\}, \otimes_6)$ → Not a Group

Closed

Asso

$e = 1$

0^{-1} : DNE

2^{-1} : DNE

3^{-1} : DNE

4^{-1} : DNE

$1^{-1} = 1$

$5^{-1} = 5$

$e^{-1} = e$

$Z_6 = \{0, 1, 2, 3, 4, 5\}$, $\otimes_6$

2^{-1} ?

$2 \otimes_6 0 = 0 \neq e$

$2 \otimes_6 1 = 2 \neq e$

$2 \otimes_6 2 = 4 \neq e$

$2 \otimes_6 3 = 0 \neq e$

$2 \otimes_6 4 = 2 \neq e$

$2 \otimes_6 5 = 4 \neq e$

$Z_6 = \{0, 1, 2, 3, 4, 5\}$, $\times_6$

$5 \times_6 5 = 25 \bmod 6 = 1 = e$

$5^{-1} = 5$

$1^{-1} = 1$

2^{-1} : DNE

3^{-1} : 1,

4^{-1} : DNE

0^{-1} : DNE

$Z_6 = \{0, 1, 2, 3, 4, 5\}$, $\otimes_6$

Monoid

Not a Group

No Inverse Property

problem?

0, 2, 3, 4 Do NOT have inverse under $\otimes_6$

$Z_6 = \{0, 1, 2, 3, 4, 5\}$, $\otimes_6$

Given into Group

have inverse under $\otimes_6$

units

$U_6 = \{1, 5\}$, $\otimes_6$

Unit

Group

$1^{-1} = 1$; $5^{-1} = 5$

$(Z_8, \oplus_8)$ — Abelian Group

→ Addition mod 8

Consider Z_8 under Mul Mod 8

$(Z_8$, Mul Mod 8)

$Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$, $\otimes_8$

Closed ✓
Asso ✓
e = 1 ✓

No inverse property

Consider Z_8 under Mul Mod 8

$(Z_8$, Mul Mod 8)

$Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$, $\otimes_8$

0, 2, 4, 6 do not have inverse.

$1^{-1} = 1$; $3^{-1} = 3$; $5^{-1} = 5$; $7^{-1} = 7$

$e^{-1} = e$

$3 \otimes_8 3 = 1$ (e)

$7 \otimes_8 7 = 1$ (e)

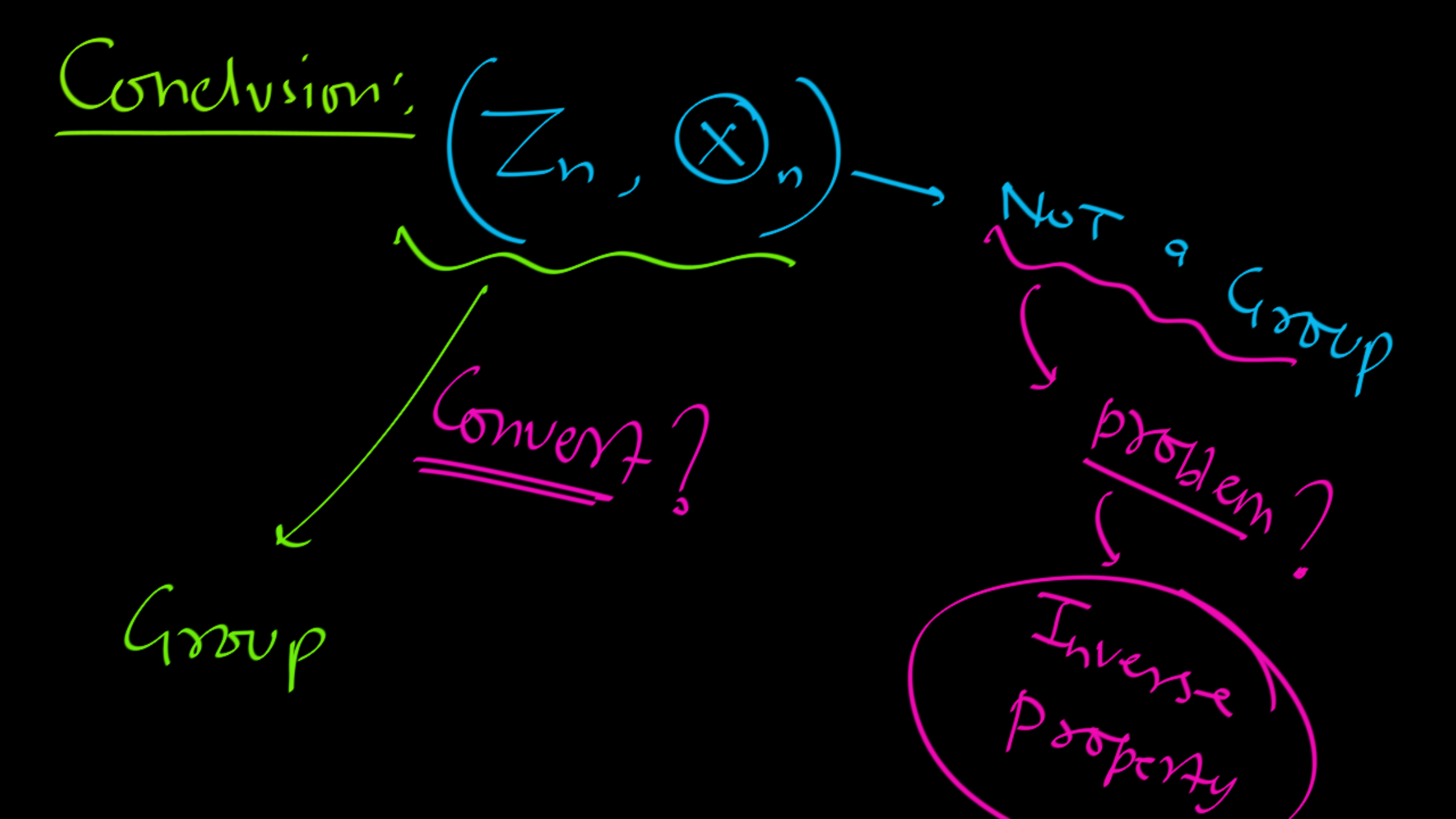
$Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$, $\otimes_8$

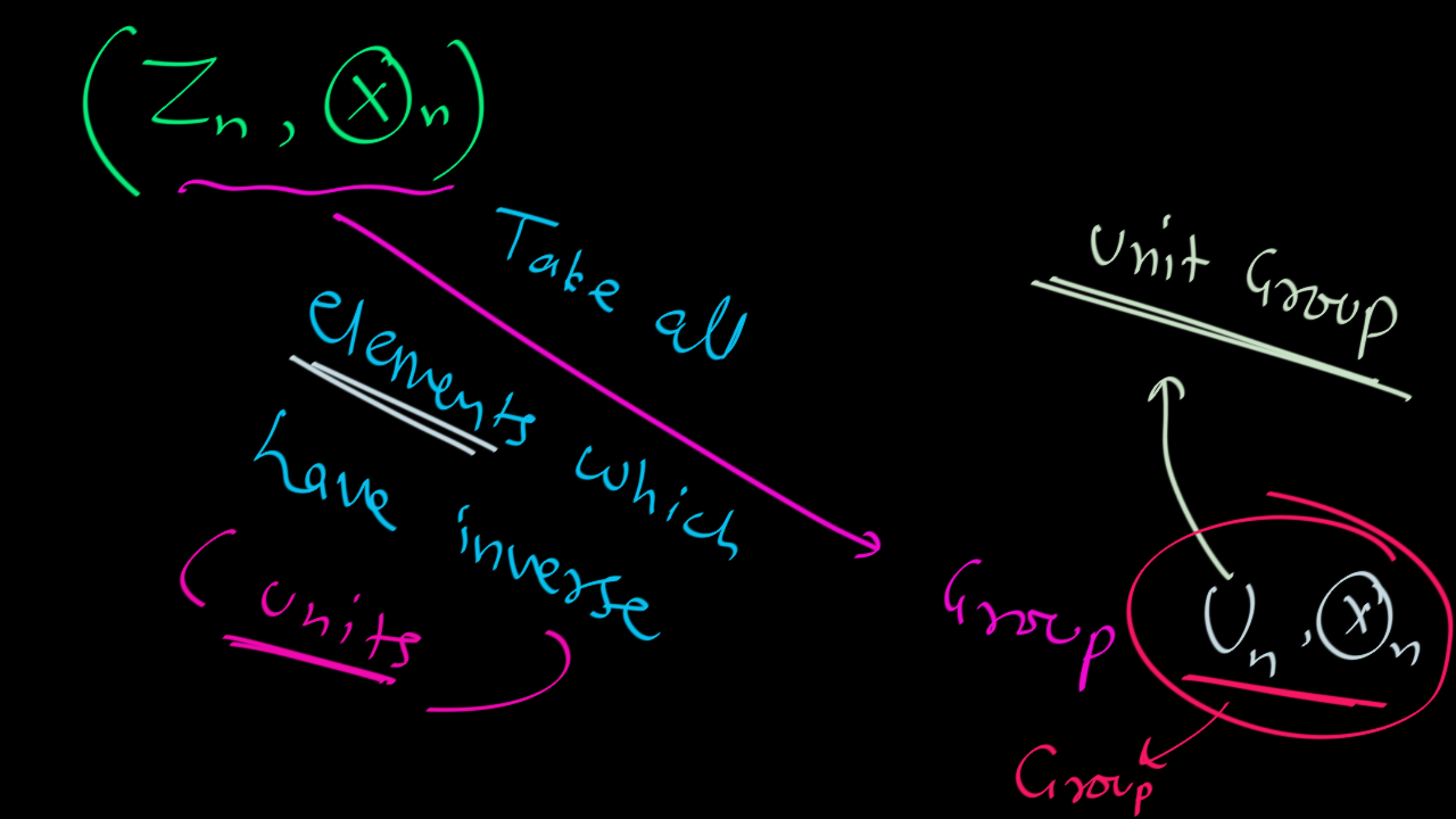
have inverse

1, 3, 5, 7 are called units

unit $U_8 = \{1, 3, 5, 7\}$, $\otimes_8$

$U_8, \otimes_8$ → Group


Conclusion:
$(Z_n, \otimes_n)$
Not a Group
Convert?
problem?
Group
Inverse Property


$(Z_n, \otimes_n)$
Take all
elements which
have inverse
(units)
Unit Group
Group
$U_n, \otimes_n$
Group

Which elements have inverse?

i.e.

which elements are units?

One final observation:

$Z_4 = \{0, 1, 2, 3\}$, $\times_4$

0, 2 Donot have inverse. → NOT Relatively prime to 4

$GCD(2,4) = 2$; $GCD(0,4) = 4$

1, 3 have inverse. → Coprime to 4

Units

$GCD(1,4) = 1$; $GCD(3,4) = 1$

$Z_6 = \{0, 1, 2, 3, 4, 5\}$, $(\times)_6$

0, 2, 3, 4 Do not have inverse.

→ Not Coprime to 6

→ Coprime to 6

1, 5 have inverse.

→ Units

$Z_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$, $\otimes_8$

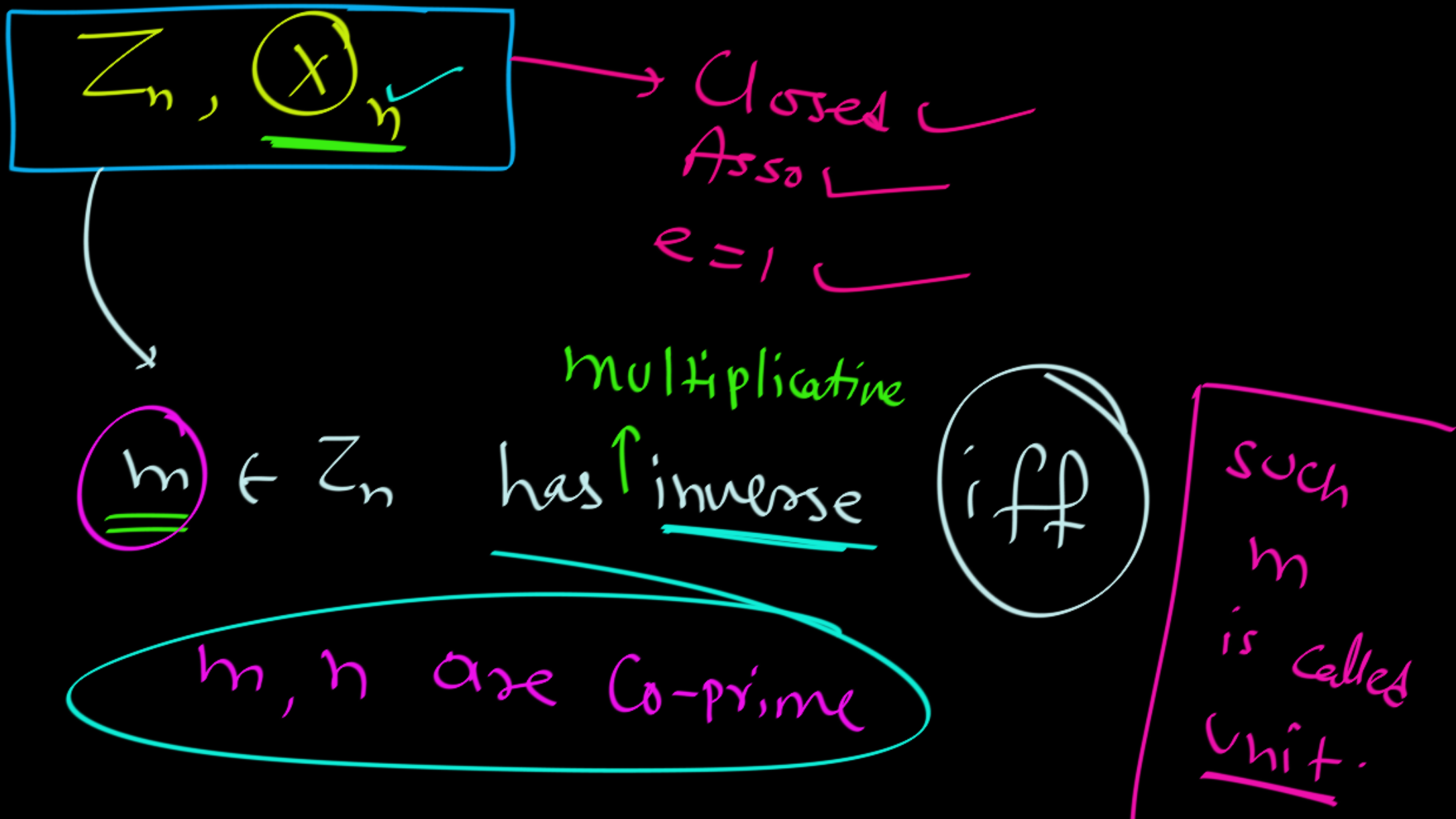
0, 2, 4, 6 — Donot have inverse.

Not Coprime with 8

Coprime with 8,

1, 3, 5, 7 — have inverse

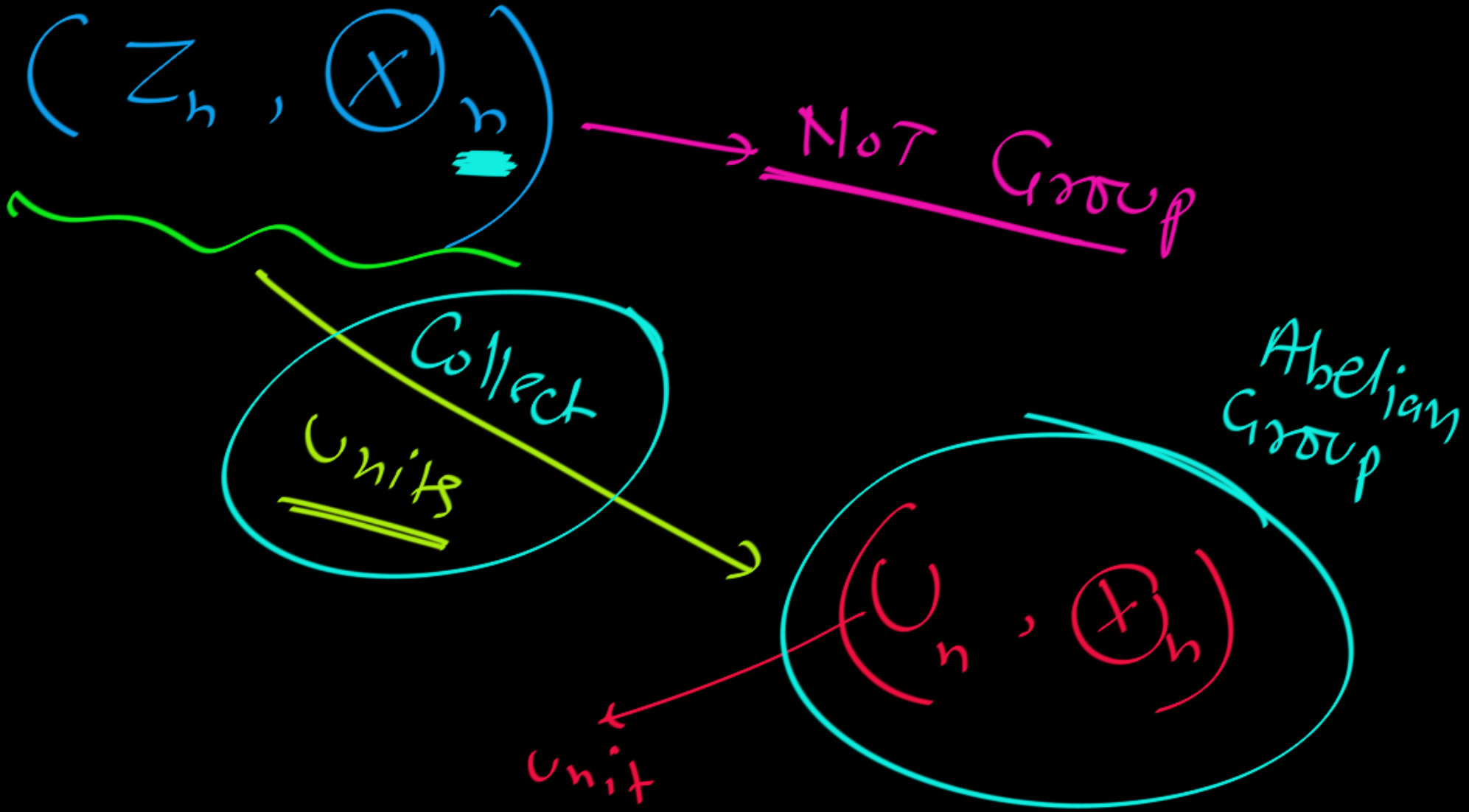
units


Z_n, $\otimes_n$
Closed
Asso
$e = 1$
multiplicative
$m \in Z_n$ has inverse
iff
m, n are Co-prime
such m is called unit.

$(Z_n, \otimes_n)$

Unit = element having multiplicative inverse

= Coprime with n


$(Z_n, \otimes_n)$
Not Group
Collect
Units
Abelian Group
$(U_n, \otimes_n)$
Unit

Consider Z_9 under Mul Mod 9

$(Z_9$, Mul Mod 9)

$Z_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$, $\otimes_9$

Not a Group → Problem?

Monoid

inverse property

$Z_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$, $\times_9$

e

0, 3, 6

Do not have inverse

Not Coprime with 9

not units

$\bar{3}^{-1} = DNE$; $\bar{6}^{-1}$: DNE ; $\bar{0}^{-1}$: DNE

$\bar{3}^{-1}$:

$3 * 0 = 0 \neq e$

$3 * 1 = 3 \neq e$

$3 * 2 = 6 \neq e$

$3 * 3 = 0 \neq e$

$3 * 4 = 3 \neq e$

$3 * 5 = 6 \neq e$

$Z_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$, $\times_9$

Units = elements have multiplicative inverse = Coprime with 9

1, 2, 4, 5, 8, 7 Coprime with 9

units

$Z_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$, $\otimes_9$

Unit

Collection of units

Unit Group

Group

$U_9 = \{1, 2, 4, 5, 7, 8\}$

Group

$\{1, 2, 4, 5, 7, 8\}$, $\otimes_9$

Note :

$(Z_n, \otimes_n)$

elements having inverse = units

= Coprime with n

$$U_n = \{ m \in Z_n \mid m \text{ is unit} \}$$

$$U_n = \{ m \in Z_n \mid m \text{ is coprime with } n \}$$

$$U_n = \{ y \mid y \in \{1, 2, \cdots, n-1\}, \; y \text{ is coprime with } n \}$$

An Interesting Question:

How to Convert Z_n into a Group under Multiplication Mod n Operation??

① $Z_n = \{0, 1, \cdots, n-1\}$

② $(Z_n, \oplus_n)$ — Abelian Group.

③ $(Z_n, \otimes_n)$ — Monoid (Commutative)

Asso ✓
e = 1 ✓
Closed ✓

→ not a Group

(4) $(Z_n, \otimes_n)$ — not a Group

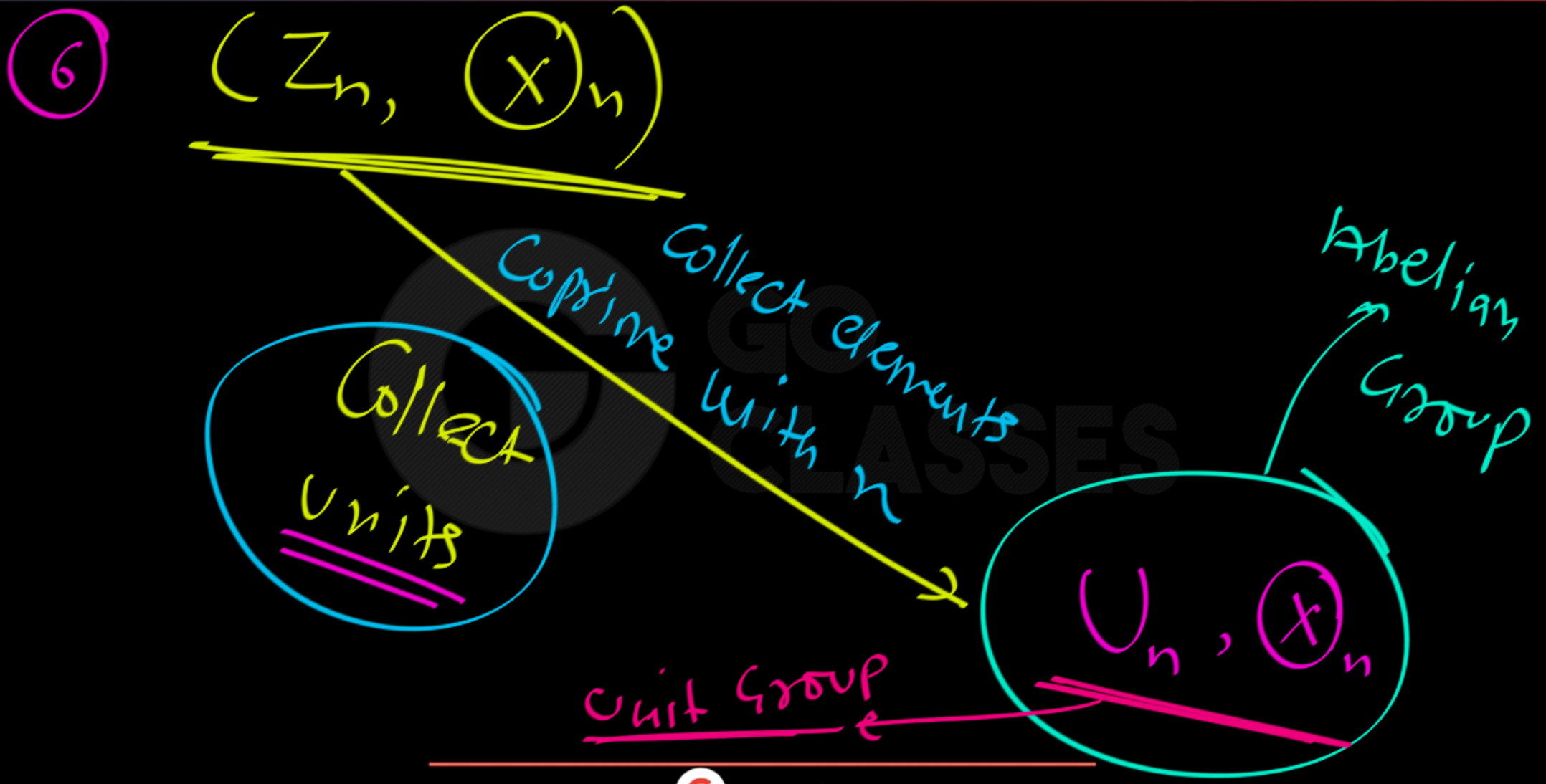
Problem ?

Some elements Don't have inverse under $\otimes_n$

(5) $(Z_n, \otimes_n)$

elements having inverse = units

= Coprime with n


6
$(Z_n, \otimes_n)$
Collect elements
Coprime with n
Collect
Units
Abelian
Group
$U_n, \otimes_n$
Unit Group

(7)

$$U_n = \{ y \mid y \in \{1, 2, \cdots, n-1\} \text{ and } y \text{ is Coprime with } n \}$$

$(U_n, \otimes_n)$ → mul mod n Group → Abelian Group

Unit Group

U_n

Definition 2.10. [3] *For each $n > 1$, we define $U(n)$ to be the set of all positive integers less than n and relatively prime to n. Then $U(n)$ is* ***a group under multiplication modulo n.***

$$U_n = \{ y \mid y \in \{1, 2, \cdots, n-1\} \ \& \ y \text{ is Relatively prime to } n \}$$

Ex: $U_{14} = \{1, 3, 5, 9, 11, 13\}, \otimes_{14}$

$GCD(7, 14) = 7$

$GCD(8, 14) = 2$

$U_{14}, \otimes_{14}$ Abelian Group

$U_{14} = \{ \underset{e}{1}, 3, 5, 9, 11, 13 \}, \otimes_{14}$

$1^{-1} = 1 \quad (e^{-1} = e)$

Group

$3^{-1} = 5$

$5^{-1} = 3$

$9^{-1} = 11$

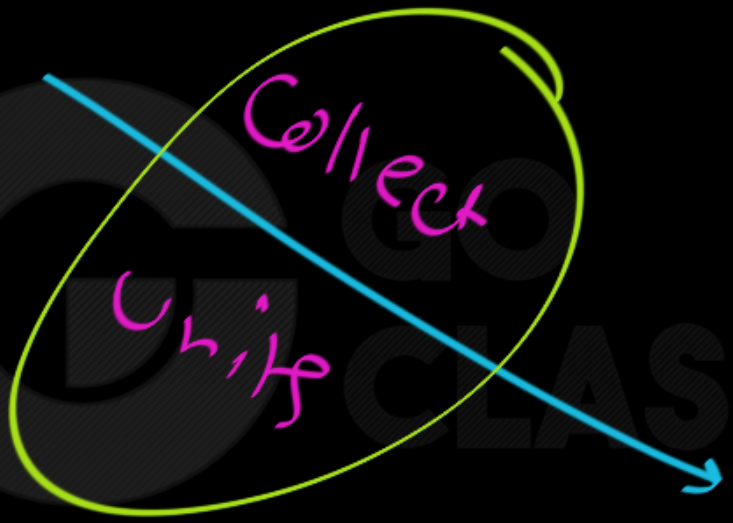
$11^{-1} = 9$

$13^{-1} = 13$

$3 \otimes_{14} 5 = 15 \bmod 14 = 1$

$9 \otimes_{14} 11 = 99 \bmod 14 = 1$

Z_{14}



U_{14}

U_{14} = Unit Group = Group of units in Z_{14}

Example. (The groups of units in $\mathbb{Z}_{14}$) Construct a multiplication table for U_{14}.

U_{14} consists of the elements of $\mathbb{Z}_{14}$ which are relatively prime to 14. Thus,

$$U_{14} = \{1, 3, 5, 9, 11, 13\}.$$

You multiply elements of U_{14} by multiplying as if they were integers, then reducing mod 14. For example,

$$11 \cdot 13 = 143 = 3 \pmod{14}, \quad \text{so} \quad 11 \cdot 13 = 3 \quad \text{in} \quad \mathbb{Z}_{14}.$$

Here's the multiplication table for U_{14}:

*	1	3	5	9	11	13
1	1	3	5	9	11	13
3	3	9	1	13	5	11
5	5	1	11	3	13	9
9	9	13	3	11	1	5
11	11	5	13	1	9	3
13	13	11	9	5	3	1

Notice that the table is symmetric about the main diagonal. Multiplication mod 14 is commutative, and U_{14} is an **abelian group**.

Be sure to keep the operations straight: The operation in $\mathbb{Z}_{14}$ is *addition* mod 14, while the operation in U_{14} is *multiplication* mod 14. □

$(Z_n, \oplus_n)$ — Abelian Group

$(U_n, \otimes_n)$ — Abelian Group

$(Z_n, \oplus_n)$ — Abelian Group

$(Z_n, \otimes_n)$ — Monoid

Not Group

$(U_n, \otimes_n)$ — Group

Q: If p is prime, what is U_p ?

Q: If p is prime, what is U_p ?

every no. from 1 to p-1 is Coprime to p.

$U_p = \{1, 2, 3, \ldots, p-1\}$

Example. (**The groups of units in** $\mathbb{Z}_p$) What are the elements of U_p if p is a prime number? Construct a multiplication table for U_{11}.

If p is prime, then all the positive integers smaller than p are relatively prime to p. Thus,

$$U_p = \{1, 2, 3, \ldots, p-1\}.$$

For example, in $\mathbb{Z}_{11}$, the group of units is

$$U_{11} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}.$$

The operation in U_{11} is multiplication mod 11. For example, $8 \cdot 6 = 4$ in U_{11}.

Summary of U_n:

Definition. Let $n \geq 2$ be a positive integer. Then

$$U(n) := \{a \in \{0, \ldots, n-1\} : \gcd(a, n) = 1\},$$

is the set of integers between 0 and n that are relatively prime to n.

Example. Let $n = 6$. Then $U(n) = \{1, 5\}$, and is a group under multiplication mod 6 with Cayley table

$U(6)$	1	5
1	1	5
5	5	1

Definition. Let $n \geq 2$ be a positive integer. Then

$$U(n) := \{a \in \{1, \ldots, n-1\} : \gcd(a, n) = 1\},$$

is the set of integers between 1 and n that are relatively prime to n.

Example. Let $n = 6$. Then $U(n) = \{1, 5\}$, and is a group under multiplication mod 6 with Cayley table

$U_6 = \{1, 5\}$

$U(6)$	1	5
1	1	5
5	5	1

$(U_6, \otimes_6)$ – Group

In Z_n,

m has multiplicative inverse

iff

m is Coprime to n.

Proposition 1. Let $n \geq 2$ be a positive integer. An element $a \in \{0, 1, \ldots, n-1\}$ has a unique multiplicative inverse in $\{0, 1, \ldots, n-1\}$ under multiplication mod n iff $\gcd(a, n) = 1$.

The Group of Units in the Integers mod n

The group $\mathbb{Z}_n$ consists of the elements $\{0, 1, 2, \ldots, n-1\}$ with *addition* mod n as the operation. You can also *multiply* elements of $\mathbb{Z}_n$, but you do not obtain a group: The element 0 does not have a multiplicative inverse, for instance.

However, if you confine your attention to the **units** in $\mathbb{Z}_n$ — the elements which have multiplicative inverses — you *do* get a group under multiplication mod n. It is denoted U_n, and is called the **group of units** in $\mathbb{Z}_n$.

Proposition. Let U_n be the set of units in $\mathbb{Z}_n$, $n \geq 1$. Then U_n is a group under multiplication mod n.

m is a unit in $\mathbb{Z}_n$ if and only if m is relatively prime to n.

In Z_n;

Unit = element having mul inverse

= Coprime to n

1. We prove here that $(\mathbb{Z}_n, \oplus)$ is an abelian(a commutative) group.

2. When considering the multiplication $mod\, n$, the elements in Z_n fail to have inverses. We study $\mathbb{Z}_4$ as an example . However, we still have $(\mathbb{Z}_n, \otimes)$ is an abelian semigroup with identity as we will prove later.

3. We know that an integer a has a multiplicative inverse $mod\, n$ if and only if a and n are relatively prim $(gcd(a, n) = 1)$. So for each $n > 1$, we define $U(n)$ to be the set of all positive integers less than n and relatively prim to n. Then $(U(n), \otimes)$ is an abelian group where the multiplication is taken $mod\, n$.

4. If n is a positive integer, then $U(n)$ denotes the *group of units modulo n*. The elements of $U(n)$ are all of the numbers from 1 up to $n-1$ that are relatively prime to n (i.e. that share no common divisors with n). The binary operation is multiplication modulo n.

   For example, the elements of $U(8)$ are $U(8) = \{1, 3, 5, 7\}$. The Cayley table or multiplication table for $U(8)$ is:

	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

2. Let $U(n)$ be the set of all positive integers less than n that are relatively prime to n. We call this the **unit group** of $\mathbb{Z}_n$.

   (a) Determine the elements of $U(8)$, $U(10)$, and $U(12)$.

   (b) Complete the Cayley tables for $U(8), U(10), U(12)$.

   (c) Choose one of the sets $U(n)$, for $n = 8, 10$ or 12, and prove that it is a group under multiplication modulo n. Note: you need to first verify that this is a binary operation on $U(n)$!

   (d) What's similar and different about the above groups? Are any of these groups the same? Explain your reasoning.

2. Let $U(n)$ be the set of all positive integers less than n that are relatively prime to n. We call this the **unit group** of $\mathbb{Z}_n$.

   (a) Determine the elements of $U(8)$, $U(10)$, and $U(12)$.

   (b) Complete the Cayley tables for $U(8), U(10), U(12)$.

   (c) Choose one of the sets $U(n)$, for $n = 8, 10$ or 12, and prove that it is a group under multiplication modulo n. Note: you need to first verify that this is a binary operation on $U(n)$!

   (d) What's similar and different about the above groups? Are any of these groups the same? Explain your reasoning.

$U_8 \equiv U_{12}$

$U_8 \not\equiv U_{10}$

(a) $U_8 = \{1, 3, 5, 7\}$

$U_{10} = \{1, 3, 7, 9\}$

$U_{12} = \{1, 5, 7, 11\}$

$(U_n, \otimes_n)$ — Abelian Group

(a) $U_8 = \{1, 3, 5, 7\}$, $\otimes_8$

$\otimes_8$	1	3	5	7
1	1	3	5	7
3	3	1	7	5
5	5	7	1	3
7	7	5	3	1

e ← 1

$3^{-1} = 3$

Abelian Group

$3 \otimes_8 3 = 1$

$3 \otimes_8 5 = 7$

$5 \otimes_8 3 = 7$

$5^{-1} = 5$

$7^{-1} = 7$

(b) $U_{10} = \{1, 3, 7, 9\}$, $\otimes_{10}$ → Group, Abelian

e	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

Closure ✓
id e = 1 ✓
$3^{-1} = 7$; $7^{-1} = 3$; $9^{-1} = 9$
Asso ✓

$3 \otimes_{10} 3 = 9$

$3 \otimes_{10} 7 = 1$

$3 \otimes_{10} 7 = 7$

$7 \otimes_{10} 3 = 1$

$7 \otimes_{10} 7 = 9$

$7 \otimes_{10} 9 = 3$

$9 \otimes_{10} 3 = 7$

$9 \otimes_{10} 7 = 3$

$9 \otimes_{10} 9 = 1$

(b) $U_{12} = \{1, 5, 7, 11\}$, $\otimes_{12}$

Abelian Group

Closed ✓

Asso ✓

$\otimes_{12}$	1	5	7	11
1 ← e	1	5	7	11
5	5	1	11	7
7	7	11	1	5
11	11	7	5	1

$e = 1$

$1^{-1} = 1$; $5^{-1} = 5$

$7^{-1} = 7$; $11^{-1} = 11$

$5 \otimes_{12} 5 = 1$

$5 \otimes_{12} 7 = 11$

$5 \otimes_{12} 11 = 7$

$7 \otimes_{12} 5 = 11$

$7 \otimes_{12} 7 = 1$

$7 \otimes_{12} 11 = 5$

$11 \otimes_{12} 5 = 7$

$11 \otimes_{12} 7 = 5$

$11 \otimes_{12} 11 = 1$

$U_8 = \{1, 3, 5, 7\}$

Group of order 4

$U_{10} = \{1, 3, 7, 9\}$

Group of order 4

$U_{12} = \{1, 5, 7, 11\}$

Group of order 4

At least 2 of them are Isomorphic (have same structure / template.)

Groups of order 4 :

Two Templates :

Template ① $\{ e \xrightarrow{id}, x, y, z \} \longrightarrow x^{-1} = x,\ y^{-1} = y,\ z^{-1} = z,\ e^{-1} = e$

Template ② $\{ e \xrightarrow{id}, x, y, z \} \longrightarrow x^{-1} = y,\ y^{-1} = x,\ z^{-1} = z$

$U_8 = \{1, 3, 5, 7\}$

$3^{-1} = 3$; $5^{-1} = 5$

$7^{-1} = 7$

Template 1

$U_{10} = \{1, 3, 7, 9\}$

$3^{-1} = 7$ | $9^{-1} = 9$

$7^{-1} = 3$

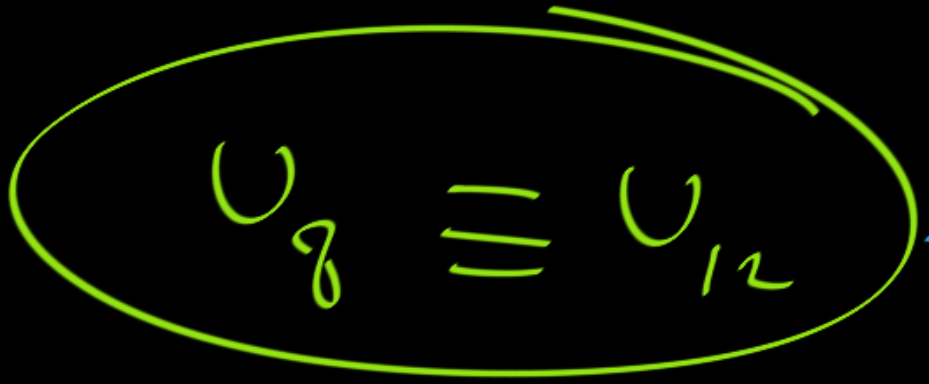
Template 2

$U_{12} = \{1, 5, 7, 11\}$

$5^{-1} = 5$

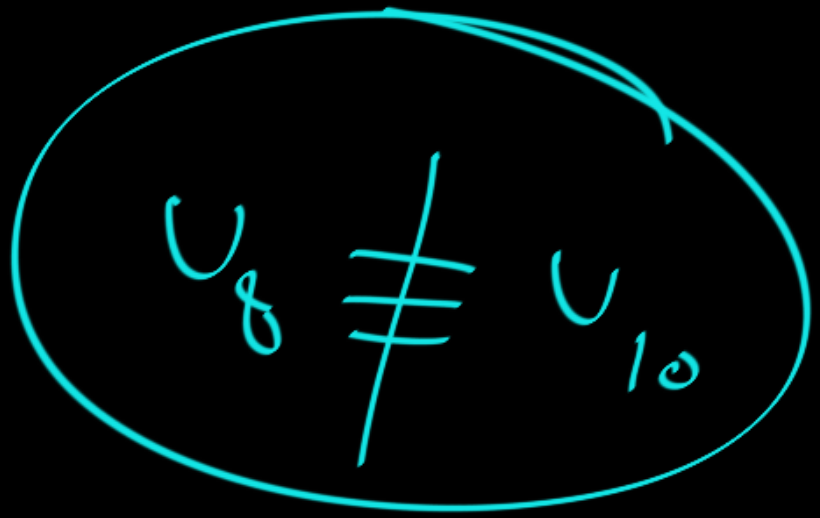
$7^{-1} = 7$ $\quad$ $11^{-1} = 11$

Template 1



— Same template
Same structure

Isomorphic



— Diff structure