# 4800-5

## Symmetries of Cyclic Gps

An abelian group $A$, is **cyclic** if there is an element $a \in A$ such that

$$\left\{ -2a, \overset{\downarrow}{-a}, 0, \underset{A}{\overset{\downarrow}{a}}, a+a, \overset{3a}{\overset{\shortparallel}{a+a+a}}, \dots \right\}$$

exhausts all the elements of $A$.

Issue: Finding a generator!

Examples: $(\overset{1,\,-1}{\mathbb{Z}},+,0)$ is cyclic. generators

(infinite cyclic gp)

$(\mathbb{Z}/n\mathbb{Z},+,0)$ are cyclic. (finite)

$\underline{0+n\mathbb{Z}}, 1+n\mathbb{Z}, 2+n\mathbb{Z}, \ldots$

$(0, 1, 2, \ldots, n-1)$

This comes with two generators.

$\rightarrow 1+n\mathbb{Z}$ $\qquad \underbrace{0, 1, 2, \ldots\ldots,}\overset{0}{\overset{\shortparallel}{n}}, \ldots$

$\rightarrow -1+n\mathbb{Z} = (n-1)+n\mathbb{Z}$

Example: $(n=4)$

$0, 1, 2, 3, \ldots$ 1 generates

$0, 2, 0, \ldots$ 2 does not generate

$0, 3, 2, 1, 0$ $3=-1$ does generate

---

$(n=5)$

$0, 1, 2, 3, 4$
$0, 2, 4, 1, 3$
$0, 3, 1, 4, 2$
$0, 4, 3, 2, 1$

all generate

Lemma: If $(A,+,0)$ is a cyclic gp, then $A$ is isomorphic to $\begin{matrix}\mathbb{Z} \\ \text{or} \\ \mathbb{Z}/n\mathbb{Z}\end{matrix}$

for $n = \#$ elements of $A$

---

Pf: If $a \in A$ is a generator, then

$$f: A \longrightarrow \begin{matrix}\mathbb{Z} \\ \text{or} \\ \mathbb{Z}/n\mathbb{Z}\end{matrix} \qquad \underline{f(na)=0}$$

$f(-a) = -1,$

$f(0)=0,\ f(a)=1,\ f(2a)=2,\ \ldots$

This is linear because

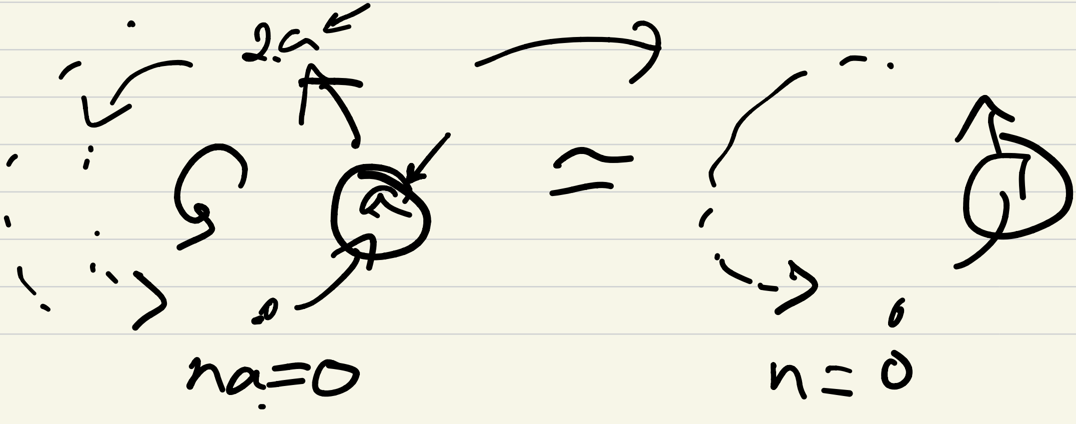
$$b, c \in A \Rightarrow b = ma$$

$$c = na$$

$$\Rightarrow f(b+c) = m+n$$

$$= f(b) + f(c).$$

---



Q: What are all the generators of $\mathbb{Z}/n\mathbb{Z}$ ?

✓ ‖

($C_n$ cyclic gp. w/ $n$ elements)

---

Let $m \in \mathbb{Z}/n\mathbb{Z}$. To generate requires

$$1 \in 0, m, 2m, \ldots, \overset{0}{\overset{\shortparallel}{nm}}$$

And if $1 = km$, then $m$ generates.

To say $1 = km$ in $\mathbb{Z}/n\mathbb{Z}$

is saying that

inverses for .

$$\left[\ \underline{1 = \overset{\downarrow}{k}m + ln}\ \right]$$

has a solution for some $k, l$.

This is exactly when

$$\gcd(m, n) = 1$$

---

i.e. $m$ & $n$ are relatively prime.

E.g. $(n=8)$

$$\left\| \begin{array}{cccccccc} 1 & 2 & 3 & 4 & \ldots & & & \\ 3 & 6 & 1 & 4 & 7 & 2 & 5 & 0 \\ 5 & \ldots & & & & & & \\ 7 & 6 & 5 & 4 & \ldots & & & \end{array} \right\|$$

---

The <u>symmetries</u> of $\mathbb{Z}/n\mathbb{Z}$ are in bijection with

$$\left(\mathbb{Z}/n\mathbb{Z}\right)^* = \left\{ \underline{\underline{m}} \in {}^{1,\ldots,n-1} \mid \gcd(m,n)=1 \right\}$$

A symmetry $\sigma : \mathbb{Z}/7\mathbb{Z} \to \mathbb{Z}/7\mathbb{Z}$

sends $\sigma(1) = m \leftarrow$

$\nwarrow$ "seed"

$\sigma(1) = m, \sigma(2) = 2m, \ldots\ldots$

---

The symmetries are isomorphic to the abelian gp

$$\boxed{\left( (\mathbb{Z}/7\mathbb{Z})^*, \overset{\text{multiplication}}{\cdot}, 1 \right)}$$

rel. prime

$$\underline{\left\{\begin{matrix}\text{Symmetries}\\ \sigma\end{matrix}\right\}} \xrightarrow{\text{seed}} \underline{\left(\mathbb{Z}/n\mathbb{Z}\right)^*}$$

$$\underline{\sigma} \longmapsto \underline{\sigma(1)} = m$$

$$1_{\mathbb{Z}/n\mathbb{Z}} \longmapsto \underset{\mathbb{Z}/n\mathbb{Z}}{1}(1) = \underset{A}{1}$$

$$\sigma, \tau \longmapsto \sigma(1) = m$$

$$\tau(1) = \underline{k}.$$

$$\sigma(\tau(1)) = \underline{\sigma(k)} = k \cdot m$$

$$\sigma \circ \tau \longmapsto k \cdot m.$$

**Q:** What are these gps

$$\left(\left(\mathbb{Z}/n\mathbb{Z}\right)^{\times}, \cdot, 1\right)?$$

**Fact:** If $n$ is prime, then $\left(\left(\mathbb{Z}/p\mathbb{Z}\right)^{\times}, \cdot, 1\right)$ is cyclic.

$p-1$ elements

# Examples:

(n=8) $\quad (\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\}$

$1^2 = 1, \; 1^3 = 1, \; \_\_\_$

$\rightarrow 3^2 = 9 = 1$, not generator

$\rightarrow 5^2 = 25 = 1$ not

$7^2 = 49 = 1$ not

$(\mathbb{Z}/3\mathbb{Z})^*$

$=$

$\{\pm 1\}$

$-1, -1^2 = 1$

Not cyclic

$(n=7)$

$1$ ×

$2, 2^2=4, 2^3=8=1$ ×

✓ $3, 3^2=2, 3^3=6, 3^4=4, 3^5=5,$

$4, 4^2=2, 4^{\textcircled{3}}=1$ ×  $\underline{3^6=1}$

✓ $g=5, 5^2=4, 5^3=6, \ldots$

$6=-1, (-1)^2=1$ ×

**Thm:**

$(\mathbb{Z}/p\mathbb{Z})^*$ has a generator.

Idea of pf: $\boxed{\mathbb{Q}, \mathbb{R}, \mathbb{C}}$

$(\mathbb{Z}/p\mathbb{Z})$ is a field ✓

- $+$ ✓, additive inverses
- $*$, multiplicative inverses $(\neq 0)$

---

Every element of $(\mathbb{Z}/p\mathbb{Z})^*$

is a root of

$x^{p-1} - 1$

To generate $(\mathbb{Z}/p\mathbb{Z})^\times$,

the element a should

not be a root of

$x^d - 1$ for any

[redacted] $d < p-1$

(in fact $d \mid p-1$)

---

$(n=7)$

$1^1 = 1$ ✓ ✓

$2^3 = 1$ $4^3 = 1$ $6^2 = 1$

$3^6 = 1$ $5^6 = 1$

Pf: Count all the roots of $x^d - 1$ for $d < p-1$ (divisors of $p-1$).

Check that there are some left over!

---

Let $\phi(d) = \left|\left(\mathbb{Z}/d\mathbb{Z}\right)^*\right|$

= # of elements of $\mathbb{Z}/d\mathbb{Z}$ rel. prime to $d$

Euler $\phi$ function

## Formula:

# of primitive roots of $x^d - 1$

$$\Rightarrow \boxed{\underline{n} = \sum_{d|n} \phi(d)}$$

$$8 = \phi(1) + \phi(2) + \phi(4) + \phi(8)$$

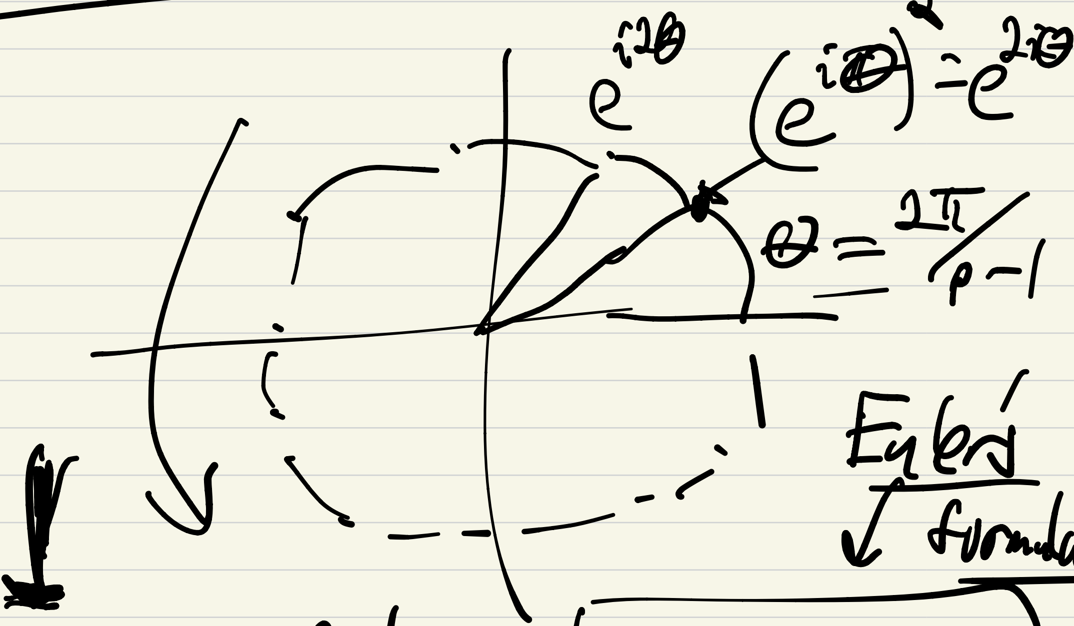
$$= 1 + 1 + 2 + 4$$

---

✪ This says that all the polys $x^d - 1$ have roots for all $d|p-1$.

# think about ℂ:

## Solutions to $x^{p-1}-1$ in ℂ:



Euler's ✓ formula

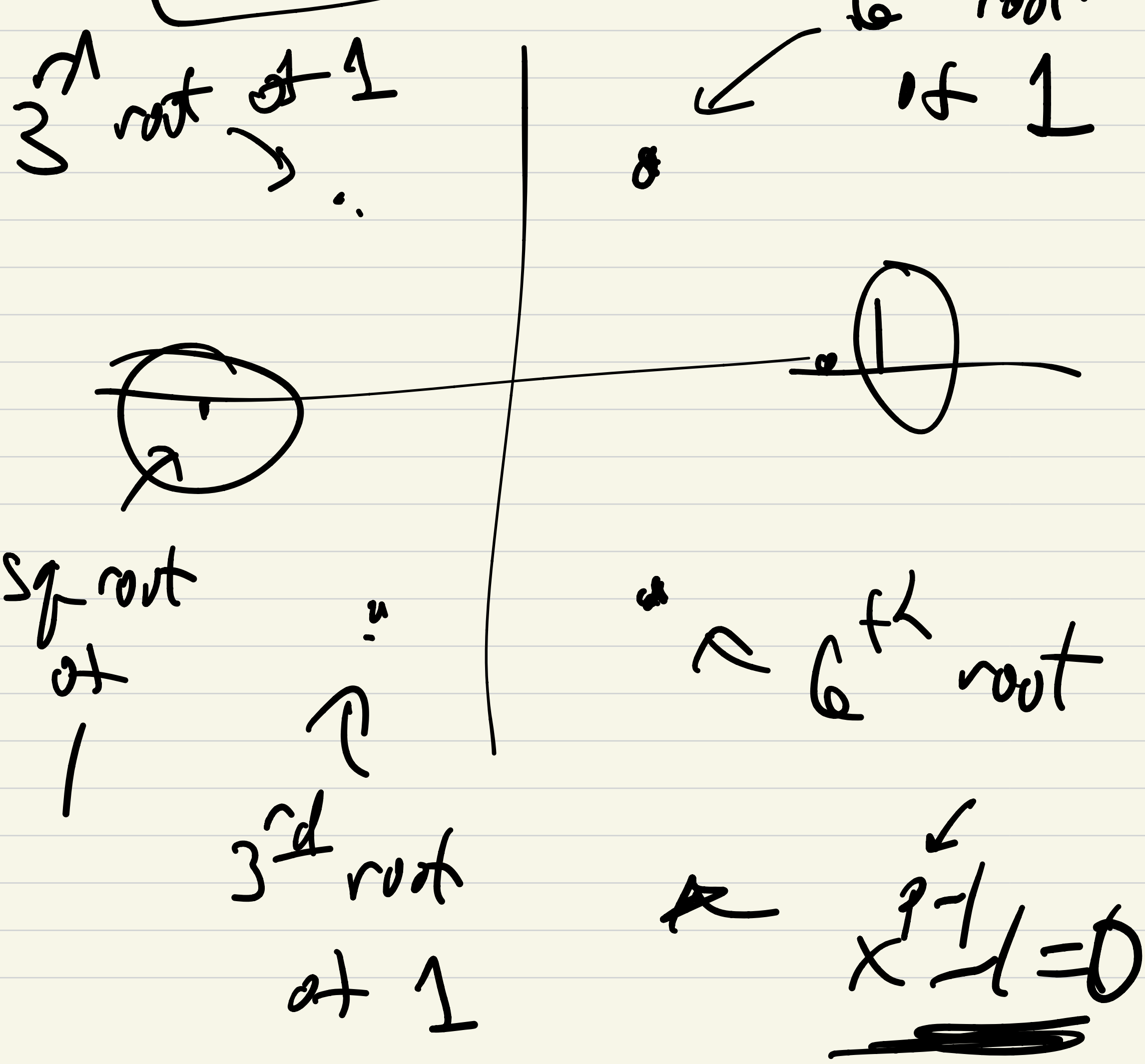
$$\underline{\left(e^{i\frac{2\pi}{p-1}}\right)^{p-1}} = \boxed{e^{i2\pi} = 1}$$

(primitive root of 1) $\boxed{e^{i\pi} = -1}$

$p = 7$

$\boxed{p - 1 = 6}$

$$6 = \overset{1}{\overset{\parallel}{\phi(1)}} + \overset{1}{\overset{\parallel}{\phi(2)}} + \underset{\underset{2}{\parallel}}{\phi(3)} + \underset{2}{\underline{\phi(6)}}$$



$p=5$ Generator

$2, 2^2=4, 2^3=3, 2^4=1$ ✓

$p=7$

$2, 2^2, 2^3=1$ ✗

$p=11$

$2, 4, 8, 5, 10, \ldots$ ✓

$p=13$

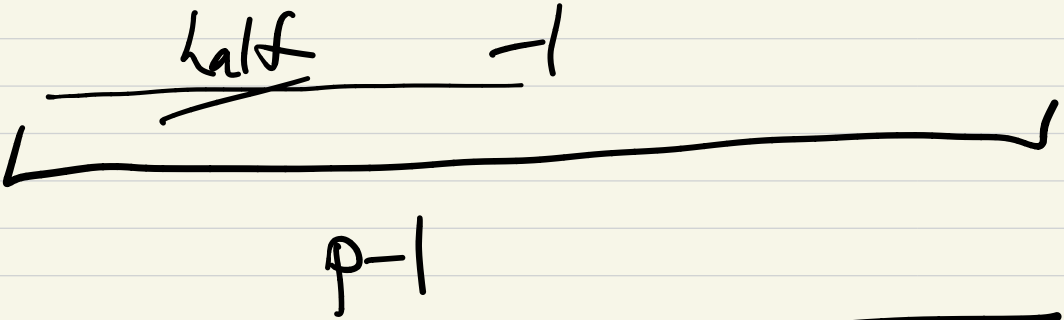
$2, 4, 8, 3, 6, 12 \ldots$ ✓

1

$p=17$ ,

$p=31$ $2, 4, 8, 16, 32$ "

$(\mathbb{Z}/p\mathbb{Z})^*$ cyclic.



---

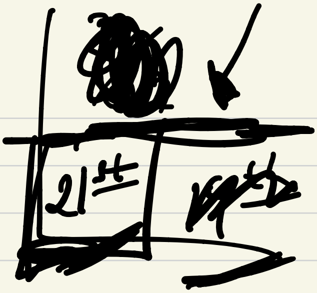
**Q:** when is

$$\underline{\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}}$$

also cylic?

**A:** when $\gcd(m,n)=1$.

There is always a linear function



inverse fcn

$$f: \mathbb{Z}/\underline{nm}\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

$$f(1) = (1,1)$$

$$f(2) = (2,2)$$

$$\vdots$$

**Q:** When is this a <u>bijection</u>?