LECTURE 10

(Friday OCT. 18, 2019)

PROOF: Looking for the smallest integer $m>0$ s.t. $(a^n)^m = e$. — Know (by previous theorem) this amounts to: $GCD := GCD(ord, n)$

$$ord(a) \mid mn \iff \frac{ord(a)}{GCD} \mid m\frac{n}{GCD}$$

[remember: "Euclid's Lemma" $u \mid vw$ and $GCD(u,v)=1$, then $u \mid w$.]

coprime (integers).

$$\iff \frac{ord(a)}{GCD} \mid m \quad \square$$

smallest such $m>0$.

Corollary

$\langle a^n \rangle = \langle a \rangle$ when n is coprime to $ord(a)$.

(always have $\subseteq$ and if $GCD=1$ they have same size)

Corollary If $(G,*)$ is finite cyclic generated by a. Then a^n is another generator precisely when $GCD(n, |G|) = 1$.

Ex $(G,*)$ cyclic of size $|G| = 21 = 3 \cdot 7$.

Pick a generator $a \in G$, i.e. $G = \langle a \rangle$

consists of all its powers:

$$e \quad a \quad a^2 \quad a^3 \quad \ldots\ldots \quad a^{20}.$$

Order of a^n is:

$$\operatorname{ord}(a^n) = \frac{21}{\operatorname{GCD}(n,21)}.$$

(note $\operatorname{ord}(a) = |G| = 21$)

In particular a^n generates G precisely when n and 21 are coprime (i.e., $3 \nmid n$ and $7 \nmid n$):

$$n = 1, 2, 4, 5, 8, 10, 11, 13, 16, 17, 19, 20$$

($12 = \varphi(21) = \varphi(3)\varphi(7) = 2 \cdot 6$ of them)

- Also,

$$\operatorname{ord}(a^3) = \frac{21}{\operatorname{GCD}(3,21)} = \frac{21}{3} = 7$$

$$\operatorname{ord}(a^7) = \frac{21}{\operatorname{GCD}(7,21)} = \frac{21}{7} = 3.$$

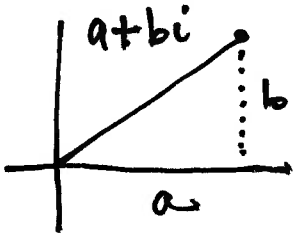
e.g., $\langle a^7 \rangle = \{e, a^7, a^{14}\}$.

Roots of unity:

Complex numbers: $\mathbb{C} = \{a+bi : a,b \in \mathbb{R}\}$, $i^2 = -1$.

— has addition & multiplication.

$(\mathbb{C}, +)$ groups $(\mathbb{C}^\times, \cdot)$



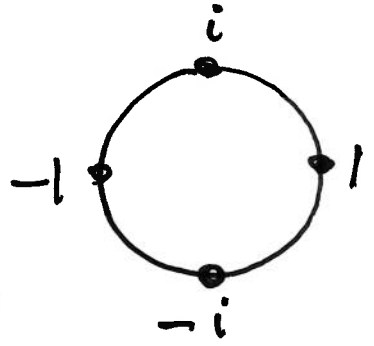
[recall $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$ "punctured complex plane"]

EX:

— Inside $\mathbb{C}^\times$:

$G = \{\pm 1, \pm i\}$

(all solutions $z \in \mathbb{C}$ to eqn. $z^4 = 1$)



$(G, \cdot)$ is a group w. composition table:

↖ cyclic:

$\langle -1 \rangle = \{\pm 1\}$

$\langle i \rangle = \{1, i, i^2, i^3\}$

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

$\cdot$	1	-1	i	$-i$
1	1	-1	i	$-i$
-1	-1	1	$-i$	i
i	i	$-i$	-1	1
$-i$	$-i$	i	1	-1

(HW)

Exc For any given $N > 0$,

$$U_N = \{z \in \mathbb{C} : z^N = 1\}$$

is a group under multiplication.

("subgroup of $\mathbb{C}^\times$")

— name:

"N^{th} roots of unity in $\mathbb{C}$".

$U_4 = \{\pm 1, \pm i\}$

– How to solve $z^N = 1$?

in "Polar form" $z = r(\cos\theta + i\sin\theta)$

$$\Rightarrow z^N = r^N(\cos N\theta + i \sin N\theta)$$

so must have $r = 1$ and $N\theta = 2\pi \cdot (\text{integer})$

(so z on complex unit circle)

i.e.) $$z = \cos\left(\frac{2\pi}{N}n\right) + i\sin\left(\frac{2\pi}{N}n\right)$$

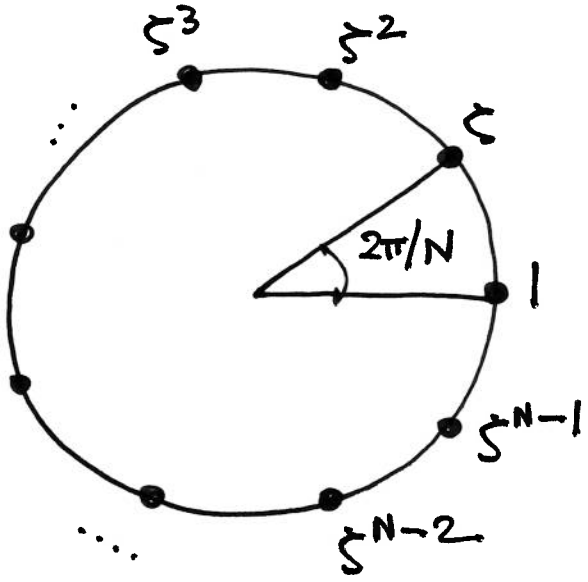
where $n = 0, 1, 2, \ldots, N-1$. (N solutions)

– Letting

$$\zeta := \cos\left(\frac{2\pi}{N}\right) + i\sin\left(\frac{2\pi}{N}\right)$$

"primitive N^{th} root of 1"

find that $z = \zeta^n$ for some $0 \leq n < N$.



— in other words:

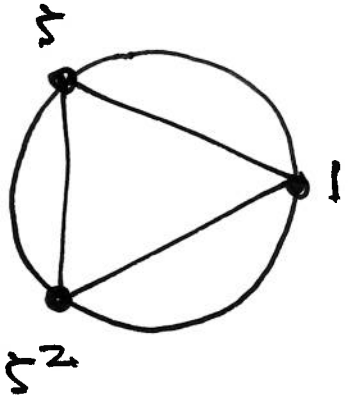
$U_N = \langle\zeta\rangle = \{1, \zeta, \zeta^2, \ldots, \zeta^{N-1}\}$ is cyclic of size N.

a regular polygon (N-gon).

Ex ($N=3$) Solutions to $z^3=1$?

Here $\zeta = \cos\left(\frac{2\pi}{3}\right) + i\sin\left(\frac{2\pi}{3}\right)$

$$= -\frac{1}{2} + i\frac{\sqrt{3}}{2}$$



w. composition table

$\bullet$	1	ζ	ζ^2
1	1	ζ	ζ^2
ζ	ζ	ζ^2	1
ζ^2	ζ^2	1	ζ

$U_3 = \{1, \zeta, \zeta^2\}$.

Compare this to $(\mathbb{Z}_3, +)$:

$+$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[1]$	$[2]$
$[1]$	$[1]$	$[2]$	$[0]$
$[2]$	$[2]$	$[0]$	$[1]$

– via the "Dictionary"

$1 \longmapsto [0]$

$\zeta \longmapsto [1]$

$\zeta^2 \longmapsto [2]$

get same "pattern"

— works for <u>any</u> N.

$\sim$ an example of an "<u>isomorphism</u>"

$$U_3 \simeq \mathbb{Z}_3$$

U_3: multiplicative. $\mathbb{Z}_3$: additive