LECTURE 11

(Wednesday OCT. 23, 2019)

Thm. ("Classification of cyclic groups").

(1) Let $(G, *)$ be an infinite cyclic group, generated by a. Then

$$f : \mathbb{Z} \longrightarrow G$$
$$n \longmapsto a^n$$

i.e., $\forall m, n \in \mathbb{Z}$: $f(m+n) = f(m) * f(n)$.

is bijective and preserves composition laws.
(an "isomorphism")

(2) If $(G, *)$ finite cyclic, $G = \langle a \rangle$ of size N. Then

$$f : \mathbb{Z}_N \longrightarrow G$$
$$[n] \longmapsto a^n$$

is bijective & preserves composition laws.
("isomorphism")

Summary: Up to isomorphism, $\mathbb{Z}$ and $\mathbb{Z}_N$ are the only cyclic groups.
$(N = 1, 2, 3, \ldots)$

PROOF (1): Noted that $a^{m+n} = a^m * a^n$, i.e. f preserves composition laws.

- f surjective: Every element of G is of the form $a^n = f(n)$, some n (since $G = \langle a \rangle$ is cyclic)
- f injective: $a^m = a^n \iff a^{m-n} = e$. If $m - n > 0$ this shows a has finite order, but $\mathrm{ord}(a) = |\langle a \rangle| = |G| = \infty$.

(2): First, f is well-defined: $n \equiv n' \pmod N \implies a^n = a^{n'}$ ✓ using: $a^N = e$ ($N = \mathrm{ord}(a)$)

- As in (1), f preserves composition laws. ✓

- f surjective: Same argument – all elts. of G may be written as $a^n = f(n)$.
- f injective: Follows. $|\mathbb{Z}_N| = N = |G| < \infty$. (or direct argument: Saw earlier that $a^m = a^n \iff \underset{\overset{\|}{N}}{\mathrm{ord}(a)}$ divides $m - n$) $\square$

Def. Let $(G,*)$ be a group. A <u>subgroup</u> is a subset $H \subseteq G$ with the following "closure" properties:

(1) $a, b \in H \implies a*b \in H$

(so $*$ restricts to a composition law $H \times H \to H$) — automatically <u>associative</u>.

(2) $e \in H$.

the neutral element of G.

(3) $a \in H \implies a^{-1} \in H$.

a priori in G only..

Ex. even numbers is a subgroup $\mathbb{Z}$, odd numbers are not,....

Thus $(H,*)$ is itself a <u>group</u>. NOTATION: $H \leqslant G$.

<u>Exc</u>: Equivalently (1)–(3) can be sumarized in:

$H \subseteq G$ is a <u>non-empty</u> subset for which

$$a, b \in H \implies a * b^{-1} \in H.$$

<u>Hint</u>: Show (2)–(3)–(1) in that order.

"TRIVIAL" subgroups: $H = \{e\}$ and $H = G$.

Recall, any fixed $a \in G$ gives a <u>subgroup</u> $\langle a \rangle$ (= the smallest subgroup containing a, cf. "$\mathrm{span}_{\mathbb{R}}(\vec{v})$")