Lec 8/26

Monday, August 26, 2019 11:31

- $a_1 \cdots a_n$ makes sense
- $a^n$ makes sense $\forall n \in \mathbb{Z}$.
- if $ab = ba$, $(ab)^n = a^n b^n$
- Def: if $S \subset G$, $\langle S \rangle$ is the smallest gp containing $S$.

<u>Prop</u>: $\langle S \rangle = \{ s_1^{\varepsilon_1} \cdots s_m^{\varepsilon_m} \mid m \in \mathbb{Z}_{\geq 0},\ s_i \in S,\ \varepsilon_i = \pm 1 \}$.

<u>Prop</u> Any infinite cyclic gp is $\cong \mathbb{Z}$.

<u>Pf</u> Let $G = \langle a \rangle$. Let $\varphi : n \longmapsto a^n$.

Clearly $\varphi$ is surjective & $\varphi(n+m) = \varphi(n) \cdot \varphi(m)$.

Also, $\varphi$ is injective: suppose $a^m = a^n$.

Then $a^{n-m} = 1$. If $n - m \neq 0$, then

$\langle a \rangle = \{ a^j : |j| \leq |n-m| \}$ and $|G| < \infty$. So $n = m$. □

<u>Prop</u> any two finite cyclic groups of the same order are isomorphic.

pf Let $G = \langle a \rangle$. Let $r = \min\{k \in \mathbb{Z}_{>0} : a^k = 1\}$.

The set is not empty since $\varphi : n \mapsto a^n$ is <u>not</u> injective

So $\exists\ n > m$ w/ $a^n = a^m$ so $a^{n-m} = 1$.

Claim: $G = \{1, a, a^2, \dots, a^{r-1}\}$.

$\forall\, m \in \mathbb{Z}$, by the division alg,

$m = qr + p$ for some $p \in \{0, 1, \dots, r-1\}$.

So $a^m = a^{qr} a^p = (a^r)^q a^p = a^p$.

So $|G| = r$. (there is no rep. in $\{1, a, a^2, \dots, a^{r-1}\}$ since $r$ was minimal: if $a^k = a^m$ w/ $r > k > m \geq 0$, then $a^{k-m} = 1$, contradiction).

If $\langle a \rangle$ and $\langle b \rangle$ are cyclic of the same order

then $a^n \mapsto b^n$ is an isomorphism. $\square$

The order of $a$ is $o(a)$ or $|a|$.

if $|a| = r$ and $a^n = 1$, $r \mid n$.

$|a| = |\langle a \rangle|$ (finite or infinite)

<u>Prop.</u> Let $G = \langle a \rangle$.

(i) If $\langle a \rangle = \infty$, then $G = \langle a^n \rangle$ iff $n = \pm 1$.

(ii) if $|a| = r < \infty$, then $G = \langle a^n \rangle$ iff $(n, r) = 1$.

The number of generators of $G$ is $\varphi(r)$.

Proof of <u>(ii)</u>: Let $d = (n, r)$. Then $|a^n| = \frac{r}{d}$ so $|a^n| = r$ iff $d = 1$.

<u>Proof of (ii)</u>: Let $d = (n,r)$. Then $\underbrace{|a^n| = \frac{r}{d}}$ so $|a^n| = r$ iff $d = 1$.

$$(a^n)^{\frac{r}{d}} = (a^r)^{n/d} = 1, \text{ and so } |a^n| \,\Big|\, \frac{r}{d}.$$

Conversely, if $\ell = |a^n|$ then $a^{n\ell} = 1$, so $r \,|\, n\ell$,

so $\frac{r}{d} \,\Big|\, \ell$. so $\frac{r}{d} = \ell$. $\square$