LECTURE 8

(Monday OCT. 14, 2019)

Powers:

Let $(G,*)$ be a group. $a\in G$, $n>0$ integer.

Def. $a^n = \underbrace{a*a*\cdots*a}_{n}$ (n factors)

– makes sense: By "associativity" of $*$.

Similarly $a^{-n} = \underbrace{a^{-1}*a^{-1}*\cdots*a^{-1}}_{n} = (a^{-1})^n$.

Convention: $a^0 = e$.

Exc: $a^{m+n} = a^m * a^n$, and $(a^m)^n = a^{mn}$. $\forall m,n\in\mathbb{Z}$.

Note In an additive group "a^n" really means the multiple:

$$\underbrace{a+a+\cdots+a}_{n} =: na$$

– For instance in $(\mathbb{Z},+)$ the "powers" of $N\in\mathbb{Z}$ are all its multiples:

$$\{nN : n\in\mathbb{Z}\} = \{0, \pm N, \pm 2N, \dots\} = \langle N\rangle$$

Def. Let $(G,*)$ be a group, $a\in G$.

$\langle a\rangle = \{a^n : n\in\mathbb{Z}\} = \{\underbrace{e, a^{\pm 1}, a^{\pm 2}, \dots}\}$.

all powers of a – may have repetitions.

continued

Exc $\langle a \rangle$ is a group. ("subgroup" of G).

Def. We say $a \in G$ has finite order if $a^n = e$ for some $n > 0$. The smallest such n is called the order of a:

$$\mathrm{ord}(a) = \min\{n > 0 : a^n = e\}.$$

EX $\mathrm{ord}(e) = 1$, $\quad \mathrm{ord}(a^{-1}) = \mathrm{ord}(a)$.

Thm. Suppose $a \in G$ has finite order. Then, for $m, n \in \mathbb{Z}$:

$$a^m = a^n \iff \mathrm{ord}(a) \text{ divides } m - n.$$

PROOF. (special case: $a^n = e \iff \mathrm{ord}(a) \mid n$)
w. $m = 0$

Can reduce the general case to the special case: $a^m = a^n \iff a^{m-n} = e$.

SPECIAL CASE:

$\Leftarrow$: Suppose $\mathrm{ord}(a) \mid n$. I.e., $n = \mathrm{ord}(a)t$ for some $t \in \mathbb{Z}$. Therefore

$$a^n = \left(a^{\mathrm{ord}(a)}\right)^t = e^t = e \checkmark$$