LECTURE 8
(Monday Oct. 14, 2019)
Powers:

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

Def. \(a^n = \underbrace{a \ast a \ast \cdots \ast a}_n\) (\(n\) factors)

makes sense by "associativity of \(\ast\).

Similarly \(a^{-n} = \underbrace{a^{-1} \ast a^{-1} \ast \cdots \ast a^{-1}}_n = (a^{-1})^n\).

Convention: \(a^0 = e\).

Ex: \(a^{m+n} = a^m \ast a^n\), \(\forall m, n \in \mathbb{Z}\).

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:
\[
\{nN : n \in \mathbb{Z}\} = \{0, \pm N, \pm 2N, \ldots\} = \langle N \rangle
\]

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

\(
\langle a \rangle = \{a^n : n \in \mathbb{Z}\} = \{e, a, a^{-1}, a^2, a^{-2}, \ldots\}
\)

all powers of \(a\) — may have repetitions.
Ex. \( \langle a \rangle \) 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 \( a \):

\[
\text{ord}(a) = \min \{ n > 0 : a^n = e \}.
\]

**Ex.** \( \text{ord}(e) = 1 \), \( \text{ord}(a^{-1}) = \text{ord}(a) \).

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

\[
a^m = a^n \iff \text{ord}(a) \mid m - n.
\]

**Proof.** (Special case: \( a^n = e \iff \text{ord}(a) \mid n \))

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

**Special Case:**

\[
\leftarrow: \text{Suppose } \text{ord}(a) \mid n. \text{ I.e., } n = \text{ord}(a)t \text{ for some } t \in \mathbb{Z}. \text{ Therefore,}
\]

\[
a^n = (a^{\text{ord}(a)})^t = e^t = e.
\]