LECTURE 11

(Wednesday Oct. 23, 2019)
Thm. ("Classification of cyclic groups").

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

\[ f: \mathbb{Z} \rightarrow G \]

\[ n \mapsto a^n \]

\(\text{i.e., } \forall m, n \in \mathbb{Z}:\)

\[ f(m+n) = f(m) \ast f(n). \]

is bijective and preserves composition laws.

(\text{an "isomorphism"})

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

Then

\[ f: \mathbb{Z}_N \rightarrow G \]

\[ [n] \mapsto a^n \]

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): Note 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 $n \in \mathbb{N}$ (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 $\text{ord}(a) = |Ka| = |G| = \infty$.

(2): First, $f$ is well-defined: $n \equiv n'(\text{mod } N) \implies a^n = a^{n'}$.

- 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. $|\mathbb{Z}_N| = N = |G| < \infty$.

(a direct argument: Saw earlier that $a^m = a^n \iff \text{ord}(a) \mid m-n$) $\square$
Def: Let \((G,*)\) be a group. A **subgroup** is a subset \(H \subseteq G\) with the following "closure" properties:

1. \(a, b \in H \implies a * b \in H\)
   
   
   \((\ast \ast \text{ restricts to a composition law } H \times H \rightarrow H)\)
   
   \(-\text{ automatically associative.}\)

2. \(e \in H\).

   \(-\text{ the neutral element of } G.\)

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

Thus \((H,\ast)\) is a priori in \(G\) only... itself a group. **NOTATION**: \(H \subseteq G\).

Ex.: Equivalently \((1)-(3)\) can be summarized in:

\[ H \subseteq G \text{ is a non-empty subset for which } \]

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

**Hint**: Show \((2)-(3)-(1)\) in that order.

"**TRIVIAL**" subgroups: \(H = \{ e \}\) and \(H = G\).

Recall, any fixed \(a \in G\) gives a subgroup \(\langle a \rangle\)

\((= \text{ the smallest subgroup containing } a, \text{ of } \text{"span}(\{a\}))\)