MATH 456: ALGEBRA 3 (FALL 2020 SEMESTER)

SHEREEN ELAIDI, BASED ON THE LECTURES OF PROF. GOREN

1. Basic Concepts and Key Examples

First we'll review some notions from Algebra 1.

Definition 1.1 (Group)**.** A **group** G is a non-empty set with a set function $m : G \times G \to G$. This can be abbreviated by $g * h$. This function satisfies the following:

(1) **(Associativity)**: $f(gh) = (fg)h$ for all $f, gh \in G$.
(2) **(Identity)**: there is an element $g \in G$ such that for all $g \in G$ we have $eg = ge = g$.
(3) **(Inverse)**: for every $g \in G$, there is an element $h \in G$ such that $gh = hg = e$.

A group with finite element is called of **finite order**. A group is called **abelian** if its commutative.

1.1. Subgroup and Order.

Definition 1.2. A **subgroup** H of G is a subset of G which obeys the following:

(1) $e \in H$.
(2) **(Closed under multiplication)**: $g, h \in H$ implies that $gh \in H$.
(3) **(Closed under inversion)**: if $g \in H$ then $g^{-1} \in H$.

A **cyclic subgroup** is a subgroup H for which there is an element $h \in H$ such that $H = \{h^n \mid n \in \mathbb{Z}\}$. We denote the set $\{h^n \mid n \in \mathbb{Z}\}$ by $\langle h \rangle$; it is the **cyclic subgroup generated by** h. The **order** of an element $h \in G$, denoted by $\mathrm{ord}(h)$, is the minimal $n \in \mathbb{Z}^+$ such that $h^n = e$. $h \in G$ has **infinite order** if no such n exists.

Proposition 1.3. *Let H be a group and $h \in H$. Then,* $\mathrm{ord}(h) = \#\langle h \rangle$.

Proof. Suppose that h has finite order n. To prove this, we'll first show that

$$\langle h \rangle = \{1, h, ..., h^{n-1}\}.$$

This will allow us to conclude that $\#\langle h \rangle = n$. Let's prove this statement.
"$\supseteq$": Clear from the definition of $\langle h \rangle$.
"$\subseteq$": To prove this inclusion, we need to show that $h^n = h^i$ for $0 \leq i \leq n-1$ and that none of the elements $1, h, ..., h^{n-1}$ are equal. Write $r = tn + i$, where $0 \leq i \leq n-1$. Then, this means that we can write

$$h^r = (h^n)^t h^i = (1)^t h^i = h^i. \checkmark \tag{1.4}$$

Now we need to show that none of the elements $1, h, ..., h^{n-1}$ are equal. For a contradiction, suppose that $h^i = h^j$ are the same, where $0 \leq i \leq j \leq n-1$. This implies that $h^{j-i} = 1_G$, which is a contradiction because $0 < j - i < n$. This contradicts that $\mathrm{ord}(h) = n$. ☐

We have the following examples of groups: $\mathbb{Z}, \mathbb{Z}/n\mathbb{Z}$ and $(\mathbb{Z}/n\mathbb{Z})^+$. Let's investigate these groups further.

- For $\mathbb{Z}$, we have that $(\mathbb{Z}, +)$ is a group. The elements are given by $\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$. The number of elements in this group, denoted by $\#\mathbb{Z}$, is infinite.
- If $n \geq 1$ is an integer, then we have the group $\mathbb{Z}/n\mathbb{Z}$; this can also be denoted by $\mathbb{Z}_n$. There is also a notion of the order of an element in the group. The **order** is the minimum integer $n > 0$ such that $g^n = 1_G$. That is for a multiplicative group; for an additive group, the order is the minimal $n > 0$ such that $ng = 0$ in G.

Date: Fall 2020 Semester.