Group Basics (Not Mandatory)

October 19, 2013

Recall that a *group* $(G, \cdot)$ is a set G with a binary operation $\cdot$ defined on G for which the following properties hold:

- **Closure**: $a \cdot b \in G$ For all $a, b \in G$.
- **Identity**: There is an element $e \in S$ such that $e \cdot a = a \cdot e = a$ for all $a \in G$.
- **Associativity**: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in S$.
- **Inverses**: For every $a \in G$ there exists an unique element $b \in S$ such that $a \cdot b = b \cdot a = e$.

The *order* of a group, denoted by $|G|$, is the number of elements in G. If the order of a group is a finite number, the group is said to be a *finite group*. If a group $(G, \cdot)$ satisfies the *commutative law* $a \cdot b = b \cdot a$ for all $a, b \in G$ then it is called an *Abelian group*.

1. Prove that the identity element e in the group is **unique**, and that every element a has a **single** inverse.

2. Let a be an element in a group and let a^{-1} denote the (unique) inverse of a. Then, for every natural number k we define:

$$a^k := \begin{cases} \underbrace{a \cdot a \cdot \ldots \cdot a}_{k}, & \text{if } k > 0; \\ e, & \text{if } k = 0; \\ \underbrace{a^{-1} \cdot a^{-1} \cdot \ldots \cdot a^{-1}}_{-k}, & \text{if } k < 0. \end{cases}$$

   Prove that for any integers (m, n) (not necessarily positive):

   (a) $a^m \cdot a^n = a^{m+n}$.

   (b) $(a^m)^n = a^{nm}$.

3. If $(G, \cdot)$ is a group, $G' \subseteq G$, and $(G', \cdot)$ is also a group, then $(G', \cdot)$ is called a *subgroup* of $(G, \cdot)$. Prove that if $(G, \cdot)$ is a finite group and G' is any subset of G such that $a \cdot b \in G'$ for all $a, b \in G'$, then $(G', \cdot)$ is a subgroup of $(G, \cdot)$.

4. Let a be an element of a finite group $(G, \cdot)$, define the set $\langle a \rangle := \{a^k : k \geq 1\}$. Prove that $\langle a \rangle$ is an Abelian subgroup of G. A group of the above form is called a *cyclic group*.

5. Let $(G, \cdot)$ be a group. An element $a \in G$ is said to be of order $i = \mathsf{ord}(a)$, if i is the minimal such that a^i is the identity element.

   - Prove that G is a cyclic group iff there is an element $g \in G$ of order $|G|$. Equivalently show that g is a generator of G iff it has order $|G|$.
   - Prove that, in a group G of prime order, every element but the identity, is a generator. (Recall Lagrange theorem from class).
   - Let $(G, \cdot)$ be a group and let $|G| = p_1^{r_1} \cdot p_2^{r_2} \cdots p_k^{r_k}$ be the factorization of its order $|G|$ to prime factors. Show that $g \in G$ is a generator iff for all $1 \leq i \leq k$: $g^{|G|/p_i}$ is *not* the identity.