BASIC PROPOSITIONS ABOUT GROUPS

We will assume that G is a group in the following propositions.

1. There exists a *unique* element $e \in G$ such that $ea = a = ae$ for all $a \in G$.

2. For every $a \in G$, there exists a *unique* element $b \in G$ such that $ab = ba = e$. We denote that element b by a^{-1}.

3. For every $a \in G$, we have $(a^{-1})^{-1} = a$.

4. For every $a, b \in G$, we have $(ab)^{-1} = b^{-1}a^{-1}$.

5. (Cancellation Laws) *(i)*. If $a, b, c \in G$ satisfy $ac = bc$, then $a = b$. *(ii)*. If $a, b, c \in G$ satisfy $ca = cb$, then $a = b$.

6. *(i)* If $a, b \in G$, then there exists a unique $c \in G$ such that $ac = b$, namely $c = a^{-1}b$.

(ii) If $a, b \in G$, then there exists a unique $d \in G$ such that $da = b$, namely $d = ba^{-1}$.

7. (Law of exponents.) Suppose that $a \in G$ and $n, m \in \mathbf{Z}$. Then $a^n a^m = a^{n+m}$ and $(a^n)^m = a^{nm}$.

8. Suppose that $a \in G$ and that a has finite order. Let m be the order of a. *(i)* Suppose $k \in \mathbf{Z}$. Then $a^k = e$ if and only if m divides k. *(ii)* Suppose $h, k \in \mathbf{Z}$. Then $a^h = a^k$ if and only if $h \equiv k \pmod{m}$.