Properties of Powers in Groups

Math 307 - Spring 2012

In this handout, we prove the properties of powers in groups, as stated in the text in Chapter 2, page 49.

Theorem 1. *Let G be a group, let $g \in G$, and let $m, n \in \mathbb{Z}$. Then*

$$g^{m+n} = g^m g^n \quad \text{and} \quad (g^m)^n = g^{mn}.$$

Proof. Because of the various possibilities of signs that can occur as powers, we prove these statements in parts based on these cases.

Since we define $g^0 = e$, where $e \in G$ is the identity element, then we have, for any $m \in \mathbb{Z}$, $g^{m+0} = g^m = g^m e = g^m g^0$, as claimed. Now, if we take $m > 0$, then by definition, $g^{m+1} = g^m g = g^m g^1$. Also by definition, still with $m > 0$, $g^{-m} = (g^{-1})^m$, and so

$$g^{-m} g^1 = (g^{-1})^m g^1 = (g^{-1})^{m-1} g^{-1} g^1 = (g^{-1})^{m-1} = g^{-m+1}.$$

That is, we have for all $m \in \mathbb{Z}$, $g^{m+1} = g^m g$. We now prove by induction that if $m \in \mathbb{Z}$, then for any integer $n \geq 1$ that $g^{m+n} = g^m g^n$. We have just proved the base case $n = 1$. Suppose that for some $k \geq 1$ we have $g^{m+k} = g^m g^k$. Then $g^{m+k+1} = g^{m+k} g^1$ by the base case. By the induction hypothesis, $g^{m+k} = g^m g^k$, so

$$g^{m+k+1} = g^{m+k} g^1 = g^m g^k g^1 = g^m g^{k+1},$$

where the last equality is also by the base case. Thus, by induction (and the case $n = 0$), for any $m \in \mathbb{Z}$, we have $g^{m+n} = g^m g^n$ for any integer $n \geq 0$.

Let $n \geq 1$ be an integer, and we now prove $(g^n)^{-1} = g^{-n}$. Note that by definition, $g^{-n} = (g^{-1})^n$. If $n = 1$, then $(g^n)^{-1} = g^{-1} = (g^{-1})^1$, as desired. Applying induction, suppose for some integer $k \geq 1$ that $(g^k)^{-1} = g^{-k}$. Then we have, by applying the induction hypothesis, the base case, and the additive property of exponents shown above,

$$g^{-(k+1)} = (g^{-1})^{k+1} = (g^{-1})^k (g^{-1})^1 = (g^k)^{-1} g^{-1} = (g g^k)^{-1} = (g^{k+1})^{-1},$$

where we have also applied the socks-shoes property of inverses. By induction, we now have $(g^n)^{-1} = g^{-n}$ for any $n \geq 1$.

Now, for any integer $n \geq 1$, we show $g^{m-n} = g^m g^{-n}$. From the above, we have

$$g^m = g^{m-n+n} = g^{m-n}g^n,$$

and since we've shown that $(g^n)^{-1} = g^{-n}$ we may multiply both sides of $g^m = g^{m-n}g^n$ on the right by g^{-n} and obtain $g^{m-n} = g^m g^{-n}$. We have now shown that for any integers m, n, that $g^{m+n} = g^m g^n$.

Let $m \in \mathbb{Z}$. We have $(g^m)^1 = g^m = g^{m\cdot 1}$. Assume that for some $k \geq 1$ that $(g^m)^k = g^{mk}$. Then

$$(g^m)^{k+1} = (g^m)^k (g^m)^1 = g^{mk}g^m = g^{mk+m} = g^{m(k+1)}.$$

Thus, by induction (on n), for any $m \in \mathbb{Z}$, and any integer $n \geq 1$, $(g^m)^n = g^{mn}$. Note also that if $n = 0$ or $m = 0$, then $g^{mn} = e = (g^m)^n$.

Next, if we assume $m, n \geq 0$ are integers, we have $(g^m)^{-n} = ((g^m)^n)^{-1} = (g^{mn})^{-1} = g^{-mn}$, from results proved above. We now have that if at least one of m or n is non-negative, then $(g^m)^n = g^{mn}$.

Finally, we must consider when both exponents are negative. First, consider $(g^{-1})^{-1}$. On homework, you proved that $(g^{-1})^{-1} = g$, and one possible proof of this goes as follows. If $h = (g^{-1})^{-1}$, then by definition of inverses, h is an element of G which satisfies $hg^{-1} = g^{-1}h = e$. We proved that inverses of elements in groups are unique, and we know $gg^{-1} = g^{-1}g = e$, by definition of inverse. Thus, by uniqueness, we must have $h = g$, so $(g^{-1})^{-1} = g$.

Let $m, n \geq 1$ be integers, so both $-m$ and $-n$ are negative. Then, we have, using the fact $(a^s)^{-1} = a^{-s} = (a^{-1})^s$ for any $a \in G$ and any integer $s \geq 1$,

$$(g^{-m})^{-n} = ((g^{-1})^m)^{-n} = (((g^{-1})^m)^{-1})^n = (((g^{-1})^{-1})^m)^n = (g^m)^n = g^{mn}.$$

We have now completed the proof that for any group G, any $g \in G$, and any $m, n \in \mathbb{Z}$, we have $g^{m+n} = g^m g^n$ and $(g^m)^n = g^{mn}$. □

When we write the operation of a group additively, say in the group G, then we write the inverse of g as $-g$, we write $g+g$ as $2g$ (as opposed to $g\cdot g$ as g^2), and in general if $n \geq 1$ is an integer, ng is the sum $g+\cdots+g$ with n terms, and we define $(-n)g = -(ng)$. If we write the additive indentity as 0 (as well as the integer), then we define $ng = 0$ for $n = 0$. With this additive notation, our properties of powers translate into the statements $(m + n)g = mg + ng$ and $(mn)g = m(ng)$ for any $m, n \in \mathbb{Z}$.