Math 113. On $x^n$

Throughout this handout, let $G$ be a group, written multiplicatively, with identity element $e$. Until further notice, we will use the notation $x'$ for the inverse of an element $x \in G$.

**Definition.** For $x \in G$ and $n \in \mathbb{Z}$, we define $x^n \in G$ by

$$x^n = \begin{cases} x \cdot x \cdots x \ (n \text{ times}) & \text{if } n > 0; \\ e & \text{if } n = 0; \text{ and} \\ (x')^{-n} & \text{if } n < 0. \end{cases}$$

It is clear from the above definition that $x^1 = x$ for all $x \in G$ and therefore $x^{-1} = (x')^1 = x'$, so we can now go back to using $x^{-1}$ to denote inverse.

**Theorem.** For all $n, m \in \mathbb{Z}$, we have

$$x^n \cdot x^m = x^{n+m}.$$ 

**Proof.**

**Case I.** $n > 0$, $m > 0$. In that case, the result follows by associativity, since the product of $n$ copies of $x$ with $m$ copies gives the product of $n + m$ copies.

**Case II.** $n = 0$ or $m = 0$. In that case the result follows by definition of the identity element.

**Case III.** $n \leq 0$ and $m \geq 0$. Induction on $\min(-n, m)$. If this number is 0, then we’re actually in Case II, and the result is true. Otherwise, the number is $> 0$, and we have

$$x^n x^m = (x^{-1})^{-n} \cdot x^m$$

$$= (x^{-1})^{-n-1} \cdot x^{-1} \cdot x \cdot x^{m-1}$$

$$= x^{n+1} \cdot e \cdot x^{m-1}$$

$$= x^{n+1} \cdot x^{m-1}$$

$$= x^{(n+1)+(m-1)}$$

$$= x^{n+m},$$

as was to be shown. Note that, in the first step, $(x^{-1})^{-n} = (x^{-1})^{-n-1} \cdot x^{-1}$ and $x^m = x \cdot x^{m-1}$ follow from Case I if $n < -1$ and $m > 1$, respectively, and Case II otherwise. The next to last step is by the inductive hypothesis.

In this case, we allowed $n = 0$ and $m = 0$ in order to make the induction easier.

**Case IV.** $n \geq 0$ and $m \leq 0$. This is similar to Case III.

**Case V.** $n < 0$ and $m < 0$. In this case

$$x^n x^m = (x^{-1})^{-n}(x^{-1})^{-m} = (x^{-1})^{-n-m} = x^{n+m}$$
Proposition. If $n \in \mathbb{Z}$, then $e^n = e$.

Proof. Again, this is by cases.

Case I. If $n \geq 0$, then this is proved by induction. The base case $n = 0$ holds by definition. If $n > 0$, then we have

$$e^n = e^{n-1} \cdot e^1 = e \cdot e = e$$

by the inductive hypothesis, so the proposition holds by induction.

Case II. If $n < 0$, then

$$e^n = (e^{-1})^{-n} = e^{-n} = e$$

by the fact that $e^{-1} = e$ and by Case I.

□

Proposition. If $x \in G$ and $n, m \in \mathbb{Z}$, then $x^{nm} = (x^n)^m$.

Proof. Again, use cases.

Case I. If $m \geq 0$, then this is proved by induction on $m$. If $m = 0$, then the identity holds because both sides are equal to $e$. If $m > 0$, then by induction on $m$ and the earlier theorem, we have

$$(x^n)^m = (x^n)^{m-1} \cdot x^n = x^{n(m-1)} \cdot x^n = x^{nm}.$$ 

Case II. If $m = -1$, then by definition of inverse and by the earlier theorem,

$$(x^n)^{-1} \cdot x^n = e = x^0 = x^{-n+n} = x^{-n} \cdot x^n.$$ 

Cancelling $x^n$ from the right then gives $(x^n)^{-1} = x^{-n}$.

Case III. If $m < 0$, then by definition and by Cases II and I,

$$(x^n)^m = ((x^n)^{-1})^{-m} = (x^{-n})^{-m} = x^{nm}.$$ 

□

Proposition. If $G$ is abelian, then $(xy)^n = x^ny^n$.

Proof. Case I. If $n \geq 0$, then we use induction on $n$. When $n = 0$, this is true because both sides are equal to $e$. If $n > 0$, then

$$(xy)^n = (xy)^{n-1} \cdot xy = x^{n-1}y^{n-1}xy = x^{n-1}xy^{n-1}y = x^ny^n.$$ 

Case II. If $n < 0$, then

$$(xy)^n = ((xy)^{-1})^{-n} = (y^{-1}x^{-1})^{-n} = (y^{-1})^{-n}(x^{-1})^{-n} = y^{n}x^{n} = x^{n}y^{n}.$$ (This is also true under the weaker hypothesis that $x$ and $y$ commute, but it is harder to prove.)

Finally, we note that in additive notation, $x^n$ is written $nx$. 