Bijective maps, permutations

The point of this handout is to point out similarities and differences between the set of bijective maps of a given set under the operation of composition and the set of integers under the operation of addition.

$\mathrm{Perm}(X)$ **and** $\circ$	$\mathbb{Z}$ **and** $+$
1. Closure. $f \circ g \in \mathrm{Perm}(X)$, $\forall f, g \in \mathrm{Perm}(X)$.	*1. Closure.* $m + n \in \mathbb{Z}$, $\forall m, n \in \mathbb{Z}$.
2. Associativity. $(f \circ g) \circ h = f \circ (g \circ h)$, $\forall f, g, h \in \mathrm{Perm}(X)$.	*2. Associativity.* $(m + n) + l = m + (n + l)$, $\forall m, n, l \in \mathbb{Z}$.
3. Identity. $\exists \mathbb{I}_X \in \mathrm{Perm}(X)$ such that $f \circ \mathbb{I}_X = \mathbb{I}_X \circ f = f$ for all $f \in \mathrm{Perm}(X)$.	*3. Identity.* $\exists 0 \in \mathbb{Z}$ such that $n + 0 = 0 + n = n$ for all $n \in \mathbb{Z}$.
4. Inverses. $\forall f \in \mathrm{Perm}(X)$, $\exists f^{-1} \in \mathrm{Perm}(X)$ such that $f \circ f^{-1} = f^{-1} \circ f = \mathbb{I}_X$.	*4. Inverses.* $\forall n \in \mathbb{Z}$, $\exists (-n) \in \mathbb{Z}$ such that $n + (-n) = (-n) + n = 0$.
5. Commutativity. Doesn't hold.	*5. Commutativity.* $n + m = m + n$, $\forall m, n \in \mathbb{Z}$.

So we see that, except for commutativity, the set $\mathrm{Perm}(X)$ under composition behaves very much like the set of integers under addition. A set G together with an operation $*$ which satisfies properties 1, 2, 3 and 4 above is called a *group*. If (as in the case of $\mathbb{Z}$ under addition) the group also satisfies property 5, it is called an *abelian group*.

There is a very nice result due to Cayley which states that every group is just a subset of $\mathrm{Perm}(X)$ under composition for some set X. So, if you really know everything about permutations then you know everything about group theory. *You should interpret this as saying that "really knowing everything" about permutations is an impossible task. It's the same way with knowing people!*

So how do you view the group $(\mathbb{Z}, +)$ as a subset of $\mathrm{Perm}(X)$ for some suitable X? Here's the idea. Take the set X to be $\mathbb{Z}$ itself. Now each $n \in \mathbb{Z}$ defines a function

$$\mathrm{Add}_n : \mathbb{Z} \to \mathbb{Z} : m \mapsto m + n$$

That is Add_n simply adds n to each element of $\mathbb{Z}$. You should verify that Add_n is a bijection of $\mathbb{Z}$ with inverse $\mathrm{Add}_{(-n)}$. Furthermore, you should also verify that Add_0 is the identity function $\mathbb{I}_{\mathbb{Z}}$, and that the composition $\mathrm{Add}_m \circ \mathrm{Add}_n$ is exactly Add_{m+n}. So we see that the map

$$\mathbb{Z} \to \mathrm{Perm}(\mathbb{Z}) : n \mapsto \mathrm{Add}_n$$

gives us an exact copy of $\mathbb{Z}$ inside $\mathrm{Perm}(\mathbb{Z})$, with $\circ$ replacing $+$.

It does not take much tweaking of this idea to get the general result of Cayley.