Chapter 2

1 Section 1

1. Let S be a set. Prove that the law of composition defined by $ab = a$ for all a, b in S is associative.

   Solution: use algebra to demonstrate order of groupings doesn't matter We'll show that $a\circ(b\circ c) = (a\circ b)\circ c$. For any $a, b, c \in S$, the composition $a\circ(b\circ c) = a\circ b = a$. Also $(a\circ b)\circ c = a\circ c = a$. Therefore this composition is associative.

   Takeaway: projection is associative.

2. . Prove the properties of inverses that are listed near the end of the section.

   The properties are:

   - If an element a has both a left inverse ℓ and a right inverse r, then the left inverse and the right inverse are equal.

     Solution: use algebra to show equality. We'll use algebra to show that $\ell = r$. Given $a\ell = 1$, multiply both sides by r. This gives $\ell ar = 1r = r$. Using associativity we have $\ell(ar) = r$. But since $ar = 1$, as r is a right inverse, this simplifies to $\ell = r$.

   - If a is invertible, its inverse is unique. **Solution: assume there are multiple inverses and show they are equal.**

     Suppose a is invertible. This means there exists at least one inverse a^{-1}. Let b, c be other, possibly different inverses for a. Then

     $$ca = ba \implies caa^{-1} = baa^{-1} \implies c = b$$

     showing that $b = c$.

   - Inverses multiply in the opposite order: $(ab)^{-1} = b^{-1}a^{-1}$.

     Solution: use algebra to demonstrate the property holds.

     This requires that a and b individually have inverses. Using associativity:

     $$ab(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a1a^{-1} = aa^{-1} = 1$$

   - An element a may have a left inverse or a right inverse, though it is not invertible.

     Solution: show an example

   - Let $\mathbb{N}$ denote the set $\{1, 2, 3, \ldots\}$, and let $s : \mathbb{N} \to \mathbb{N}$ be the *shift* map function defined by $s(n) = n + 1$. Prove that s has no right inverse, but that it has infinitely many left inverses. **Solution: explore the function's properties and form a proof.**

     Suppose s has a right inverse t. Then t must be a function from $\mathbb{N}$ to $\mathbb{N}$ such that $s(t(n)) = n$. We can also write this as $t(n) + 1 = n$. This clearly works if $t(n) = n - 1$. However if $n = 1$ then $n - 1$ is not in the target set $\mathbb{N}$. In this sense s cannot have a right inverse.

     If s has a left inverse then $t(s(n)) = n$ for all n. I.e. $t(n + 1) = n$. We can define $t(n) = n - 1$ and since t can never receive a number lower than 2 as input, we don't have the problem before of $t(n)$ mapping out of $\mathbb{N}$. However, t must still be *defined* on the entire set $\mathbb{N}$, so we can map 1 to any natural number we like. For example we could have t_1 which maps 1 to 1, t_{29} which maps 1 to 29, etc. In this sense each t_k is a left inverse of s and there are infinitely many different ones, one for each natural number.

2 Section 2

2.1 First

2.2 Second

2.3 third

2.4 fourth

2.5 In the definition of a subgroup, the identity element in H is required to be the identity of G. One might require only that H have an identity element, not that it need be the same as the identity of G. Show that if H has an identity at all, then it is the identity of G. Show the analagous statement is true for inverses.

Solution: isolate the essential difference between the objects then show they must be equal. Suppose $H \leq G$ and e is the identity of H. Then for any $h \in H, eh = he = h$. Now take some $g \in G$ that is not in H (if there is no such g then $H = G$ and e is the identity in G, as the group identity is unique). Let $eg = g'$. Perhaps $g \neq g'$ and e is not the identity in G. However, using associativity:

$$\begin{tikzcd}
 & (eh)g \arrow[r, equal] & hg \arrow[d, equal] \\
ehg \arrow[ur, equal] \arrow[dr, equal] & & \\
 & (eh)g = (he)g = h(eg) \arrow[r, equal] & hg'
\end{tikzcd}$$

shows $hg = hg'$. We apply the cancellation law to get $g = g'$. That means $eg = g$ for any $g \in G$ not in H and e is already the identity for H. Therefore e behaves as the identity in G as well, and since group identities are unique, e must be the identity of G.

For inverses, suppose $h \in H$ has an inverse h^{-1} in H but a possibly different inverse $j \in G$. Then in G, $hh^{-1} = hj$ and by the cancellation law $h^{-1} = j$.