THE CHINESE UNIVERSITY OF HONG KONG
DEPARTMENT OF MATHEMATICS

MMAT5510 Foundation of Advanced Mathematics 2017-2018
Supplementary Exercise 3

1. Let $f : A \to B$ be a bijective function.

   (a) Show that there exists unique inverse function $g : B \to A$ of f, i.e. g satisfies $g(f(x)) = x$ for all $x \in A$ and $f(g(y)) = y$ for all $y \in B$.

   (Therefore, the unique inverse function is denoted by f^{-1}.)

   (b) Show that $f^{-1} : B \to A$ is also a bijective function.

   Ans:

   (a) Since f is surjective, let $y \in B$, there exists $x \in A$ such that $f(x) = y$.

   Furthermore, since f is injective, the element $x \in A$ is the unique one such that $f(x) = y$.

   We define $g : B \to A$ by $g(y) = x$. Then we have $g(f(x)) = g(y) = x$ for all $x \in A$ and $f(g(y)) = f(x) = y$ for all $y \in B$, i.e. g is an inverse function.

   Furthermore, suppose that $g_1, g_2 : B \to A$ are inverse functions of f.

   Then for all $y \in B$, we have $f(g_1(y)) = f(g_2(y)) = y$. However, f is an injective function, so $g_1(y) = g_2(y)$. Therefore, $g_1(y) = g_2(y)$ for all $y \in B$ which means they are the same function, i.e. inverse function of f is unique.

   (b) Suppose that $f^{-1}(y_1) = f^{-1}(y_2)$ where $y_1, y_2 \in B$.

   Then, $y_1 = f(f^{-1}(y_1)) = f(f^{-1}(y_2)) = y_2$, and so f^{-1} is injective.

   Let $x \in A$, then $f(x) \in B$. Let $y = f(x) \in B$, then $f^{-1}(y) = f^{-1}(f(x)) = x$ and so f^{-1} is surjective.

   Therefore, f^{-1} is bijective.

2. Let $f : A \to B$ and $g : B \to C$ be two bijective functions.

   Show that $g \circ f : A \to C$ is a bijective function.

   Ans:

   Let $x_1, x_2 \in A$ such that $(g \circ f)(x_1) = (g \circ f)(x_2)$, i.e. $g(f(x_1)) = g(f(x_2))$.

   Since g is injective, $f(x_1) = f(x_2)$. Then, since f is injective, $x_1 = x_2$.

   Therefore $g \circ f$ is injective.

   Let $y \in C$. Since g is surjective, there exists $w \in B$ such that $g(w) = y$.

   Also, since f is surjective, there exists $x \in A$ such that $f(x) = w$.

   Then, we have $(g \circ f)(x) = g(f(x)) = g(w) = y$ and so $g \circ f$ is surjective.

3. Let $f : B \to C$ be a function.

   If A is a subset of B, the restriction of f on A is a function $f|_A : A \to C$ defined by $f|_A(x) = f(x)$ for all $x \in A$.

Show that if f is an injective function, then $f|_A$ is an injective function.

Ans:

Let $x_1, x_2 \in A$ such that $f|_A(x_1) = f|_A(x_2)$.

Then, we have $f(x_1) = f|_A(x_1) = f|_A(x_2) = f(x_2)$.

Since f is an injective function, $f(x_1) = f(x_2)$ implies $x_1 = x_2$.

Therefore, $f|_A$ is an injective function.

4. Let $m, n, p \in \mathbb{N}$. Prove that $m + p = n + p$ if and only if $m = n$.

Ans:

($\Rightarrow$) Prove by mathematical induction on p.

When $p = 0$, if $m + p = n + p$, then it means $m + 0 = n + 0$ and so $m = n$. Assume that if $m, n, p \in \mathbb{N}$ such that $m + p = n + p$, then we have $m = n$.

Then, $m + p^+ = n + p^+$ implies $(m + p)^+ = (n + p)^+$ and so $m + p = n + p$.

By induction assumption, we have $m = n$.

($\Leftarrow$) Prove by mathematical induction on p.

When $p = 0$, if $m = n$, then $m + p = m + 0 = m = n = n + 0 = n + p$.

Assume that if $m, n, p \in \mathbb{N}$ such that $m = n$, then we have $m + p = n + p$.

Then, we also have $(m + p)^+ = (n + p)^+$ and so $m + p^+ = n + p^+$.

(Remark: recall the fact that for any $x, y \in \mathbb{N}$, $x = y$ if and only if $x^+ = y^+$.)

5. Show that for all $p, q \in \mathbb{N}$, $p \leq q$ if and only if there exists $r \in \mathbb{N}$ such that $q = p + r$.

Ans:

($\Rightarrow$) Prove by mathematical induction on p.

When $p = 0$, suppose that $0 = p \leq q$, then $q = 0 + q = p + q$ (i.e. take $r = q$). Assume the $p \in \mathbb{N}$ and if $q \in \mathbb{N}$ with $p \leq q$, then we have $q = p + r$ for some $r \in \mathbb{N}$.

Now, if $p^+ \leq q$, we have $p < q$ and hence $p \leq q$.

By the induction assumption, $q = p + t$ for some natural number t.

However, t cannot be 0. Otherwise, we have $q = p$ which is a contradiction.

Then t is a nonzero natural number, it means that $t = r^+$ for some natural number r.

Therefore, $q = p + r^+ = (p + r)^+ = (r + p)^+ = r + p^+ = p^+ + r$.

($\Leftarrow$) It is sufficient for us to show that for all $p, r \in \mathbb{N}$, we have $p \leq p + r$.

We prove it by induction on r.

When $r = 0$, it is trivial. Assume that $p, r \in \mathbb{N}$ such that $p \leq p + r$.

Then $p + r \leq (p + r)^+ = p + r^+$ and so $p \leq p + r^+$.

(Remark: By the result of question 1, if $p \leq q$, then there exists **unique** r such that $q = p + r$.)

6. (Archimedean Property) Prove that for all $m, n \in \mathbb{N}$ with $n \neq 0$, there exists q such that $m < qn$.

   Ans:

   Prove by mathematical induction on m.

   When $m = 0$, since $n \neq 0$, we have $m = 0 < n = 1 \cdot n$.

   Assume that $m \in \mathbb{N}$ and there exists q such that $m < qn$.

   Then we have $m^+ = m + 1 < qn + 1 \leq qn + n = (q+1)n$.

Well Ordering Property states that every non-empty subset M of $\mathbb{N}$ contains a least element, i.e. there exists $m \in M$ such that $m \leq n$ for all $n \in M$.
Furthermore, the least element m must be unique. Note that if m and m' are both least elements of M, then we have $m \leq m'$ (m is a least element) and $m' \leq m$ (m' is a lease element) and so $m = m'$.

7. (Division Algorithm) If m and n are natural numbers and $n \neq 0$, prove that there exists unique natural numbers q and r such that $m = qn + r$ and $0 \leq r < n$.

   Ans:

   By Archimedean property, $S = \{a \in \mathbb{N} : m < an\}$ is a non-empty subset of $\mathbb{N}$.

   By well ordering property, there exists an unique least element t of S.

   Furthermore, t cannot be 0 (otherwise, we have $m < 0 \cdot n = 0$ which is a contradiction), so $t = q^+$ for a unique $q \in \mathbb{N}$.

   Note that q must not be an element of S, so we have $m \geq qn$.

   There exists unique $r \in \mathbb{N}$ such that $m = qn + r$. (See question 2)

   Note that $r \in \mathbb{N}$, so $0 \leq r$.

   We then claim that $r < n$. Suppose not and $n \geq r$ implies that $r = n + r'$ for some $r' \in \mathbb{N}$.

   Then $m = qn + r = qn + (n + r') = (qn + n) + r' = q^+n + r'$, that means $m \geq q^+$ which contradicts to the fact that $q^+ \in S$. Therefore, $0 \leq r < n$.

8. Prove that every natural number $n > 1$ is divisible by a prime number.

   Ans:

   Let S be the set of all natural numbers $n > 1$ which is not divisible by any prime number.

   Suppose the above statement is false, then S is a non-empty set.

   By the well ordering property, there exists a least natural number $N > 1$ that is not divisible by any prime number.

   Then N cannot be a prime, otherwise, N is divisible by itself which means it is divisible by a prime.

   Therefore, N is a composite number, i.e. $N = ab$ for some natural numbers a and b with $1 < a < N$ and $1 < b < N$.

   Since $1 < a < N$, a is divisible by a prime number p which implies N is also divisible by p (Contradiction).