THE CHINESE UNIVERSITY OF HONG KONG
DEPARTMENT OF MATHEMATICS

MMAT5510 Foundation of Advanced Mathematics 2017-2018
Supplementary Exercise 4

1. Prove that

   (a) If A is a set with m elements and B is a set with n elements and if $A \cap B = \phi$, then $A \cup B$ has $m+n$ elements.

   (b) If A is a set with m elements, where $m \geq 1$, and $C \subseteq A$ is a set with 1 element, then $A \backslash C$ is a set with $m-1$ elements.

   (c) If C is an infinite set and B is a finite set, then $C \backslash B$ is an infinite set.

   Ans:

   (a) By the assumption, there exist bijective functions $f : \mathbb{N}_m \to A$ and $g : \mathbb{N}_n \to B$, where $\mathbb{N}_k = \{1, 2, \ldots, k\}$.
   Then, let $h : \mathbb{N}_{n+m} \to A \cup B$ be a function defined by

   $$h(i) = \begin{cases} f(i) & \text{if} \quad 1 \leq i \leq m; \\ \\ g(i-m) & \text{if} \quad m+1 \leq i \leq m+n. \end{cases}$$

   Then, we are going to show that h is a bijective function.

   - Suppose that $h(i) = h(j)$. Since $h(i) = h(j) \in A \cup B$ and $A \cap B = \phi$, either both $h(i)$ and $h(j)$ are elements A, or both of them are elements of B.
     In case that both of $h(i)$ and $h(j)$ are elements A, by the construction of h, we must have $1 \leq i, j \leq m$ and so $f(i) = h(i) = h(j) = f(j)$. Since f is an injective function, we have $i = j$.
     In case that both of $h(i)$ and $h(j)$ are elements B, by the construction of h, we must have $m+1 \leq i, j \leq m+n$ and so $g(i-m) = h(i) = h(j) = g(j-m)$. Since g is an injective function, we have $i - m = j - m$ and then $i = j$.
     Therefore, h is an injective function.
   - Let $y \in A \cup B$, then we have $y \in A$ or $y \in B$.
     In case that $y \in A$, since f is a surjective function, there exists i with $1 \leq i \leq m$ such that $f(i) = y$. Then, we have $i \in \mathbb{N}_{m+n}$ and $h(i) = f(i) = y$.
     In case that $y \in B$, since g is a surjective function, there exists j with $1 \leq j \leq n$ such that $g(j) = y$. Let $i = m + j$, then we have $m+1 \leq i \leq m+n$ and so $i \in \mathbb{N}_{m+n}$. Also, $h(i) = g(i-m) = g(j) = y$.
     Therefore, h is a surjective function.

   Therefore, h is a bijective function and $A \cup B$ is a set with $m+n$ elements.

   (b) Suppose that $C = \{c\} \subseteq A$.

By assumption there exists a bijective function $f : \mathbb{N}_m \to A$ and we let $f(k) = c$, where $1 \le k \le m$. Note that in particular, f is an injective function, we have $f(i) \ne c$ and so $f(i) \in A \backslash C$ for all $1 \le i \le m$ with $i \ne k$.

Therefore, we can define a function $g : \mathbb{N}_{m-1} \to A\backslash C$ which is given by

$$g(i) = \begin{cases} f(i) & \text{if} \quad 1 \le i \le k-1; \\ \\ f(i+1) & \text{if} \quad k \le i \le m-1. \end{cases}$$

Then, we are going to show that h is a bijective function.

- Suppose that $g(i) = g(j)$. Then either $1 \le i, j \le k-1$ or $k \le i, j \le m-1$. Otherwise, say $1 \le i \le k-1$ and $k \le j \le m-1$, then we have $f(i) = g(i) = g(j) = f(j+1)$. By the injectivity of f, we have $i = j+1$ which is a contradiction.
  Now, if $1 \le i, j \le k-1$, we have $f(i) = g(i) = g(j) = f(j)$ and so $i = j$; otherwise $k \le i, j \le m-1$, we have $f(i+1) = g(i) = g(j) = f(j+1)$ which implies $i+1 = j+1$ and so $i = j$.
  Therefore, g is an injective function.
- Let $y \in A\backslash C$. Firstly, $y \in A$, there exists $1 \le j \le m$ such that $f(j) = y$. Note that $y \ne c$ and so $j \ne k$. If $1 \le j \le k-1$, take $i = j$, then we have $i \in \mathbb{N}_{m-1}$ and $g(i) = f(i) = f(j) = y$; if $k+1 \le j \le m$, take $i = j-1$, then we have $k \le i \le m-1$ and so $i \in \mathbb{N}_{m-1}$ and $g(i) = f(i+1) = f(j) = y$.
  Therefore, g is a surjective function.

Therefore, g is a bijective function and $A\backslash C$ is a set with $m-1$ elements.

Alternative method:

Instead of construction of g, we define a function $h : \mathbb{N}_m \to \mathbb{N}_m$ which is given by $h(k) = m$, $h(m) = k$ and $h(i) = i$ for all $i \ne m, k$. It can be proved that h is a bijective function and so $\tilde{f} = f \circ h : \mathbb{N}_m \to A$ is a also bijective function. Note that $\tilde{f}(m) = f(h(m)) = f(k) = c$ (Sometimes, you may see "Without loss of generality, let $f : \mathbb{N}_m \to A$ be a bijective function with $f(m) = c$", that function f is the $\tilde{f}$ we constructed above.) Then, what remains to show is just the restriction function $\tilde{f}|_{\mathbb{N}_{m-1}} : \mathbb{N}_{m-1} \to A\backslash C$ is a bijective function, which is left as an exercise.

(c) If $B =$, i.e. B has 0 element, the statement is trivially true.

We prove the statement to be true by using mathematical induction on the number of element of B.

- Suppose that C is an infinite set and B has only one element b.
  By assumption there exists a bijective function $f : \mathbb{N} \to C$ and we let $f(k) = b$. Note that in particular, f is an injective function, we have $f(i) \ne b$ and so $f(i) \in A\backslash C$ for all $i \ne k$.
  Therefore, we can define a function $g : \mathbb{N} \to C\backslash B$ which is given by

$$g(i) = \begin{cases} f(i) & \text{if} \quad 1 \le i \le k-1; \\ \\ f(i+1) & \text{if} \quad k \le i. \end{cases}$$

Then, what remains to show is that h is a bijective function and it is left as an exercise.

- Assume that for any infinite set C and for any B with n elements, $C\backslash B$ is an infinite set. Now, if C is an infinite set and B is a set with $n+1$ elements. Suppose that b is an element of B. Note that $C\backslash B = (C\backslash\{b\})\backslash(B\backslash\{b\})$. By the previous part, we know that $C\backslash\{b\}$ is still an infinite set. By part (b), $B\backslash\{b\}$ is a set with n element. Therefore, by the induction assumption, $(C\backslash\{b\})\backslash(B\backslash\{b\})$ is an infinite set.

The result follows by mathematical induction.

2. By writing down an explicit bijective function from the set of all natural numbers $\mathbb{N}$ (i.e. nonnegative integers) onto the set of all integers $\mathbb{Z}$, show that $|\mathbb{N}| = |\mathbb{Z}|$.

Ans:

Let $f : \mathbb{N} \to \mathbb{Z}$ be a function defined by

$$f(n) = \frac{((-1)^n - 1)(n+1)}{4} + \frac{(1+(-1)^n)n}{4}.$$

(When n is even, the first term vanishes and we have $f(0) = 0$, $f(2) = 1$, $f(4) = 2$ and etc; when n is odd, the second term vanishes and we have $f(1) = -1$, $f(3) = -2$, $f(5) = -3$ and etc.) Then, we are going to show that f is bijective.

- If $f(m) = f(n)$, then either both m and n are even or both of them are odd (otherwise, when we compute $f(m)$ and $f(n)$, one is nonnegative while the other one is negative, which is a contradiction.)

  Now, suppose that both m and n are even. Then,

$$\begin{aligned} f(m) &= f(n) \\ \frac{((-1)^m - 1)(m+1)}{4} + \frac{(1+(-1)^m)m}{4} &= \frac{((-1)^n - 1)(n+1)}{4} + \frac{(1+(-1)^n)n}{4} \\ \frac{2m}{4} &= \frac{2n}{4} \\ m &= n \end{aligned}$$

  Suppose that both m and n are odd. Then,

$$\begin{aligned} f(m) &= f(n) \\ \frac{((-1)^m - 1)(m+1)}{4} + \frac{(1+(-1)^m)m}{4} &= \frac{((-1)^n - 1)(n+1)}{4} + \frac{(1+(-1)^n)n}{4} \\ \frac{-2(m+1)}{4} &= \frac{-2(n+1)}{4} \\ m &= n \end{aligned}$$

  Therefore, f is an injective function.

- Let $q \in \mathbb{Z}$.

  Suppose that $q \geq 0$, we take $n = 2q \in \mathbb{N}$. Then,

$$f(n) = f(2q) = \frac{((-1)^{2q} - 1)(2q+1)}{4} + \frac{(1+(-1)^{2q})2q}{4} = \frac{2(2q)}{4} = q.$$

  Suppose that $q < 0$, we take $n = -2q - 1 \in \mathbb{N}$. Then,

$$f(n) = f(2q) = \frac{((-1)^{-2q-1} - 1)((-2q-1)+1)}{4} + \frac{(1+(-1)^{-2q-1})(-2q-1)}{4} = \frac{-2(-2q)}{4} = q.$$

Therefore, f is a surjective function.

Therefore, f is a bijective function and $|\mathbb{N}| = |\mathbb{Z}|$.

3. Let $a, b, c \in \mathbb{Z}$. Show that if $c \mid ab$ and $\gcd(a, c) = 1$, then $c \mid b$.

   Ans:

   Since $\gcd(a, c) = 1$, there exist $m, n\mathbb{Z}$ such that $am + cn = 1$. Then,

$$\begin{aligned} abm + cbn &= b \\ cm + cbn &= b \\ b &= c(m + bn) \end{aligned}$$

   where $m + bn \in \mathbb{Z}$. Therefore, $c \mid b$.

4. Let p, q be positive integers. If $\gcd(p, q) = 1$, then show that $\varphi(pq) = (p-1)(q-1)$, where φ is the Euler's function.

   Ans:

   Without loss of generality, let $p < q$.

   Let $P = \{np : n = 1, 2, \ldots, q-1\}$ and $Q = \{mq : m = 1, 2, \ldots, p-1\}$.

   Claim 1: $P \cap Q = \phi$. If $u \in P \cap Q$, then $u = np = mq$ for some $0 \leq n \leq q-1$ and $0 \leq m \leq p-1$.

   Since $\gcd(p, q) = 1$ and $p \mid mq$, we have $p \mid m$ which contradicts to the fact that $1 \leq m \leq p-1 < p$.
   Claim 2: Let $m \in \mathbb{N}_{pq-1}$. We claim that $m \in \mathbb{N}_{pq-1} \backslash (P \cup Q)$ if and only if $\gcd(m, pq) = 1$.

   Note that $1 \leq m < pq$, $\gcd(m, pq) > 1$ if and only if $\gcd(m, pq) = p$ or $\gcd(m, pq) = q$, while p, q are primes, it means $p \mid m$ or $q \mid m$. Therefore, $\gcd(m, pq) = 1$ if and only if m is not divisible by either p or q, i.e. $m \in \mathbb{N}_{pq-1} \backslash (P \cup Q)$.

   By the above,

$$\begin{aligned} \varphi(pq) &= |\{m \in \mathbb{N}_{pq-1} : \gcd(m, pq) = 1\}| \\ &= |\mathbb{N}_{pq-1} \backslash (P \cup Q)| \\ &= |\mathbb{N}_{pq-1}| - |P| - |Q| \\ &= (pq - 1) - p - q \\ &= (p-1)(q-1) \end{aligned}$$

5. Let n be a positive integer.

   If a and b are integers such that $\gcd(a, n) = \gcd(b, n) = 1$, show that $\gcd(ab, n) = 1$.

   Ans: Suppose that $\gcd(a, n) = \gcd(b, n) = 1$, but $\gcd(ab, n) > 1$.

   Then there exists a prime number p such that $p \mid \gcd(ab, n)$ which implies $p \mid n$ and $p \mid ab$. Since p is a prime number, we have $p \mid a$ or $p \mid b$.

   If $p \mid a$, p is a common divisor of a and n which contradicts to the fact that $\gcd(a, n) = 1$. Similarly, we have contradiction for the case that $p \mid b$.

   Therefore, $\gcd(ab, n) = 1$.