MATH1050 Exercise 7 Supplement

1. Consider each of the statements below. (Do not worry about the mathematical content.) Write down its negation in such a way that the word '*not*' does not explicitly appear.

   (a) *For any* $\varepsilon \in (0, +\infty)$, *there exists some* $\delta \in (0, +\infty)$ *such that for any* $x \in \mathbb{R}$, *if* $0 < |x - a| < \delta$ *then* $|f(x) - \ell| < \varepsilon$.

   (b) *There exists some* $\ell \in \mathbb{R}$ *such that for any* $\varepsilon \in (0, +\infty)$, *there exists some* $\delta \in (0, +\infty)$ *such that for any* $x \in \mathbb{R}$, *if* $0 < |x - a| < \delta$ *then* $|f(x) - \ell| < \varepsilon$.

   (c) *For any* $a \in \mathbb{R}$, *there exists some* $\ell \in \mathbb{R}$ *such that for any* $\varepsilon \in (0, +\infty)$, *there exists some* $\delta \in (0, +\infty)$ *such that for any* $x \in \mathbb{R}$, *if* $0 < |x - a| < \delta$ *then* $|f(x) - \ell| < \varepsilon$.

   (d) *For any* $a \in \mathbb{R}$, *for any* $\varepsilon \in (0, +\infty)$, *there exists some* $\delta \in (0, +\infty)$ *such that for any* $x \in \mathbb{R}$, *if* $|x - a| < \delta$ *then* $|f(x) - f(a)| < \varepsilon$.

   (e) *For any* $\varepsilon \in (0, +\infty)$, *there exists some* $\delta \in (0, +\infty)$ *such that for any* $x, a \in \mathbb{R}$, *if* $|x - a| < \delta$ *then* $|f(x) - f(a)| < \varepsilon$.

   (f)$^\diamondsuit$ *For any* $a \in \mathbb{R}$, *for any* $\varepsilon \in (0, +\infty)$, *there exists some* $\delta \in (0, +\infty)$ *independent of the choice of* a *such that for any* $x \in \mathbb{R}$, *if* $|x - a| < \delta$ *then* $|f(x) - f(a)| < \varepsilon$.

2. Consider each of the statements below. For each of them, determine whether it is true or false. Justify your answer by giving an appropriate argument.

   (a) *Let* $a, b, c, d \in \mathbb{R}$. *Suppose* $a > b$ *and* $c > d$. *Then* $a - c > b - d$.

   (b) *Let* n *be a positive integer. Let* x, y *be distinct positive real numbers.* $x^{2n} + y^{2n} > x^{2n-1}y + xy^{2n-1}$.

   (c) *There exist some* $z, w \in \mathbb{C}$ *such that* $z^4 = w^4 = -1$ *and* $z - w \in \mathbb{R}\backslash\{0\}$.

   (d) *There exist some* $x, y \in \mathbb{R}$ *such that* $(x + y)^2 = x^2 + y^2$.

   (e) *There exist some* $x, y \in \mathbb{R}\backslash\{0\}$ *such that* $x^3 + y^3 = (x + y)^3$.

   (f)$^\diamondsuit$ *There exist some* $x, y \in \mathbb{R}\backslash\{0\}$ *such that* $x^4 + y^4 = (x + y)^4$.

   (g) *There exists some* $x \in \mathbb{R}$ *such that* $x^8 + x^4 + 1 = 2x^2$.

   (h)$^\clubsuit$ *There exist some* $a, b \in \mathbb{R}\backslash\{0\}$ *such that* $\sqrt{a^2 + b^2} = \sqrt[3]{a^3 + b^3}$.

   (i) *There exist some* $x, y \in \mathbb{R}$ *such that* $|x^2 + iy^2| < |xy|$.

   (j) *There exists some* $z \in \mathbb{C}\backslash\{0\}$ *such that* $\left|z + \dfrac{1}{\overline{z}}\right| < \left|z - \dfrac{1}{\overline{z}}\right|$.

   (k) *There exist some* $x, y, p, s, t \in \mathbb{R}$ *such that* $|x - p| \leq s$ *and* $|y + p| \leq t$ *and* $|x + y| > s + t$.

   (l)$^\clubsuit$ *For any* $\alpha \in \mathbb{C}\backslash\{0\}$, *if* $\alpha^2/\overline{\alpha}^2$ *is a positive real number then (*α *is real or* α *is purely imaginary).*

3. (a)$^\diamondsuit$ Prove the **Division Algorithm for Integers**:

   - *Let* $m, n \in \mathbb{Z}$. *Suppose* $n \in \mathbb{Z}\backslash\{0\}$. *Then there exist some unique* $q, r \in \mathbb{Z}$ *such that* $m = qn + r$ *and* $0 \leq r < |n|$.

   Remark. You may take for granted the validity of Division Algorithm for Integers with positive divisors:

   - *Let* $m, n \in \mathbb{Z}$. *Suppose* $n > 0$. *Then there exist some unique* $q, r \in \mathbb{Z}$ *such that* $m = qn + r$ *and* $0 \leq r < n$.

   (b) Let $m, n \in \mathbb{Z}$. Suppose $n \neq 0$. Apply Division Algorithm for Integers to prove that the statements ($\sharp$), ($\flat$) are logically equivalent:

   ($\sharp$) *m is divisible by n.*

   ($\flat$) *The remainder in the division of m by n is zero.*

4. (a)$^\diamondsuit$ Apply Division Algorithm to prove the statement below:

   - *Let* $n \in \mathbb{N}\backslash\{0, 1\}$. *For any* $x \in \mathbb{Z}$, *exactly one of* $x, x + 1, x + 2, \cdots, x + n - 1$ *is divisible by* n.

   (b) Let $p \in \mathbb{N}$. Suppose p is a prime number and $p \geq 5$. Prove the statements below. *Where appropriate and necessary, you may apply Euclid's Lemma.*

   i. $p^2 - 1$ *is divisible by* 8.

   ii.$^\diamondsuit$ $p^2 - 1$ *is divisible by* 3.

   iii.$^\clubsuit$ $p^2 - 1$ *is divisible by* 24.

5. (a) Let $n \in \mathbb{N}$. Let $x, y, u, v \in \mathbb{Z}$. Suppose $x \equiv u (\mathrm{mod}\ n)$ and $y \equiv v (\mathrm{mod}\ n)$. Prove the statements below:
   i. $x + y \equiv u + v (\mathrm{mod}\ n)$.
   ii.$^\diamondsuit$ $xy \equiv uv (\mathrm{mod}\ n)$.

   (b) Let $n \in \mathbb{N}$. Apply mathematical induction to prove each of the statements below:
   i. *Let $t \in \mathbb{N} \backslash \{0, 1\}$. Let $k_1, k_2, \cdots, k_t, \ell_1, \ell_2, \cdots, \ell_t \in \mathbb{Z}$. Suppose $k_i \equiv \ell_i (\mathrm{mod}\ n)$ for each i. Then $k_1 + k_2 + \cdots + k_t \equiv \ell_1 + \ell_2 + \cdots + \ell_t (\mathrm{mod}\ n)$.*
   ii. *Let $t \in \mathbb{N} \backslash \{0, 1\}$. Let $k_1, k_2, \cdots, k_t, \ell_1, \ell_2, \cdots, \ell_t \in \mathbb{Z}$. Suppose $k_i \equiv \ell_i (\mathrm{mod}\ n)$ for each i. Then $k_1 k_2 \cdots k_t \equiv \ell_1 \ell_2 \cdots \ell_t (\mathrm{mod}\ n)$.*

   (c) i. Let $m, n, r \in \mathbb{Z}$. Suppose $n \neq 0$ and $0 \leq r < n$. Prove that r is the remainder in the division of m by n iff $m \equiv r (\mathrm{mod}\ n)$.
   ii. A. What is the remainder in the division of 10^{100} by 7?
   B. What is the remainder in the division of 10^{100} by 13?
   Remark. You can make use of the definition of 'congruence modulo n' and the results of the previous part carefully to obtain the answer very quickly.

6. (a) Prove the statements below:
   i.$^\heartsuit$ *For any $x \in \mathbb{N}$, there exist some $p \in \mathbb{N}$, $a_0, a_1, \cdots, a_p \in [\![0, 9]\!]$ such that $x = \sum_{k=0}^{p} a_k 10^k$ and $a_p \neq 0$.*
   ii.$^\heartsuit$ *For any $x \in \mathbb{N}$, there are at most one $p \in \mathbb{N}$, and for each $j = 0, 1, 2 \cdots, p$, at most one $a_j \in [\![0, 9]\!]$ such that $x = \sum_{k=0}^{p} a_k 10^k$ and $a_p \neq 0$.*

   Remark. So altogether the existence-and-uniqueness statement below holds:
   ($\sharp$) *For any $x \in \mathbb{N}$, there exist some unique $p \in \mathbb{N}$, $a_0, a_1, \cdots, a_p \in [\![0, 9]\!]$ such that $x = \sum_{k=0}^{p} a_k 10^k$ and $a_p \neq 0$.*

   By virtue of this existence-and-uniqueness statement, each natural number x may be presented as the chain of symbols $a_p a_{p-1} \cdots a_1 a_0$, understood as the sum $x = \sum_{k=0}^{p} a_k 10^k$, in which $a_0, a_1, \cdots, a_p$ are the uniquely determined integers amongst $0, 1, \cdots, 9$ according to ($\sharp$). The presentation $x = a_p a_{p-1} \cdots a_1 a_0$ is referred to as the **decimal notation** of the natural number n. $a_0, a_1, \cdots, a_p$ are referred to as the digits of x; a_0 is the last digit, a_1 as the second-last digit, et cetera.

   (b) i. Prove the statements below:
   A. *Let $n \in \mathbb{N}$. Suppose the last digit of n in its decimal notation is divisible by 2. Then n is divisible by 2.*
   B. *Let $n \in \mathbb{N}$. Suppose the number defined as expressed by the last two digits of n in its decimal notation is divisible by 4. Then n is divisible by 4.*
   C. *Let $n \in \mathbb{N}$. Suppose the number defined as expressed by the three digits of n in its decimal notation is divisible by 8. Then n is divisible by 8.*
   ii.$^\diamondsuit$ Can you generalize the above results? Formulate a conjecture for the general situation and prove the conjecture.

   (c)$^\clubsuit$ Prove the statements below.
   i. *Let $n \in \mathbb{N}$. Suppose the sum of the digits of n is divisible by 3. Then n is divisible by 3.*
   ii. *Let $n \in \mathbb{N}$. Suppose the sum of the digits of n is divisible by 9. Then n is divisible by 9.*

7. Prove the statements below. *You may take Euclid's Lemma for granted.*
   (a) *Let $m, n \in \mathbb{Z}$. $m^2 - n^2$ is divisible by 2 iff $m - n$ is divisible by 2.*
   (b) *Let $m, n \in \mathbb{Z}$. $m^3 - n^3$ is divisible by 3 iff $m - n$ is divisible by 3.*
   (c) *Let $m, n \in \mathbb{Z}$. $m^5 - n^5$ is divisible by 5 iff $m - n$ is divisible by 5.*

   Remark. What if $2, 3, 5$ respectively is replaced by 7? Or 11? Or 13? Can you formulate an appropriate conjecture which generalize the statements considered here? How about proving the conjecture?

8. Consider each of the statements below. For each of them, determine whether it is true or false. Justify your answer by giving an appropriate argument.

(a) *Let $x, n \in \mathbb{Z}$. Suppose x is divisible by n. Then for any $y \in \mathbb{Z}$, $(x+y)^3 + (x-y)^3$ is divisible by $2n$.*

(b) *Let $m, n \in \mathbb{Z}$. Suppose $m \equiv 1 (\text{mod } 2)$ and $n \equiv 3 (\text{mod } 4)$. Then $m^2 + n$ is divisible by 4.*

(c) *There exists some $x \in \mathbb{Z}$ such that $x \equiv 5 (\text{mod } 14)$ and $x \equiv 3 (\text{mod } 21)$.*

(d)$^\diamondsuit$ *Let p, q be distinct positive prime numbers. $\dfrac{p+q}{pq}$ is not an integer.*

(e) *There exists some $n \in \mathbb{Z}$ such that $n^3 + n^2 + 2n$ is odd.*

(f) *Let x be a positive real number. Suppose x is an irrational number. Then, for any $n \in \mathbb{N}$, $t \in \mathbb{Q}$, if $n \geq 2$ then $\sqrt[n]{x + t^2}$ is an irrational number.*

(g) *Let $s, t \in \mathbb{R}$. Suppose s, t are distinct irrational numbers. Then st is an irrational number.*

(h) *Let $x, y, z \in \mathbb{N}$. Suppose $x > y > z$ and x is not divisible by y and y is not divisible by z. Then x is not divisible by z.*

(i) *There exist some $a, b \in \mathbb{R}$ such that a is irrational and b, a^b are rational.*

(j) *There exist some $a, b \in \mathbb{R}$ such that b is irrational and a, a^b are rational.*

(k)$^\heartsuit$ *There exist some $a, b \in \mathbb{R}$ such that a, b are irrational and a^b is rational.*

(l) *Suppose $n \in \mathbb{N}$. Then $\gcd(n, n+2) = 2$.*

(m) *Let $x, y, z \in \mathbb{Z}$. Suppose $\gcd(x, y) > 1$ and $\gcd(y, z) > 1$. Then $\gcd(x, z) > 1$.*

(n) *Let $m, n, k \in \mathbb{Z}$. Suppose $m + n$ is divisible by k. Then m is divisible by k or n is divisible by k.*

(o) *There exists some $m, n \in \mathbb{Z}$ such that $m - n$ is divisible by 2 and $m^2 - n^2$ is not divisible by 4.*

(p)$^\diamondsuit$ *There exists some $n \in \mathbb{N} \backslash \{0, 1, 2, 3\}$ such that n is even and $2^n - 1$ is a prime number.*

(q) *Let $x, y, z \in \mathbb{N}$. Suppose $x > yz$ and $y > z$. Further suppose x is divisible by y and x is divisible by z. Then x is divisible by yz.*

(r) *Let $a, b \in \mathbb{Z}$. Suppose a is even and b is odd. Then $a^2 + 2b^2$ is not divisible by 4.*

(s)$^\clubsuit$ There exist some distinct positive prime numbers p, q such that $\sqrt{p} + \sqrt{q}$ is rational.

(t)$^\heartsuit$ *There exists some $n \in \mathbb{N}$ such that n is a prime number and $n > 2^{100}$.*

9.$^\heartsuit$ Let $a, b \in \mathbb{Z}$. Suppose a, b are not both zero. Let $I = \{x \in \mathbb{Z} :$ There exist some $h, k \in \mathbb{Z}$ such that $x = ha + kb\}$. Define $S = I \cap (\mathbb{N} \backslash \{0\})$. Apply the Well-Ordering Principle for Integers on the set S to prove that $\gcd(a, b) \in I$.

Remark. This is a 'clean' argument for '**Bezôut's Identity**'; the trade-off is that it does tell how to perform the calculations. The set I will be referred to as the 'ideal generated by a, b in the commutative ring $\mathbb{Z}$'.

10. (a)$^\diamondsuit$ Prove the statement below:

- *Suppose $a, b, c \in \mathbb{Z}$. Then c is a common divisor of a, b iff $\gcd(a, b)$ is divisible by c.*

(b)$^\clubsuit$ Let $\ell, m, n \in \mathbb{Z}$. Write $g = \gcd(\gcd(\ell, m), n)$. Prove the statements below:

i. *Each of ℓ, m, n is divisible by g.*

ii. *For any $d \in \mathbb{Z}$, if each of ℓ, m, n is divisble by d then $|d| \leq g$.*

iii. *If $\ell = m = n = 0$ then $g = 0$.*

iv. *Suppose $c \in \mathbb{Z}$. Then c is a common divisor of ℓ, m, n iff g is divisible by c.*

Remark. Because of the above, it makes sense to refer to the number $\gcd(\gcd(\ell, m), n)$ as the greatest common divisor of ℓ, m, n, and simply write $\gcd(\gcd(\ell, m), n)$ as $\gcd(\ell, m, n)$. We may further inductively define the greatest common divisor for four, five, six, ... integers. Moreover, to compute the greatest common divisor of n integers $a_1, a_2, \cdots, a_n$, we may iteratively compute $\gcd(a_1, a_2)$, $\gcd(\gcd(a_1, a_2), a_3)$, ..., and $\gcd(... \gcd(\gcd(a_1, a_2), a_3) ..., a_n)$ in succession. The last number will turn out to be $\gcd(a_1, a_2, \cdots, a_n)$.

(c) Prove the statement below:

- *Let $\ell, m, n \in \mathbb{Z}$. There exist some $r, s, t \in \mathbb{Z}$ such that $\gcd(\ell, m, n) = r\ell + sm + tn$.*

Remark. It will turn out that when ℓ, m, n are not all zero, $\gcd(\ell, m, n)$ is the smallest positive integer in the set

$$I = \{x \in \mathbb{N} : \text{There exist some } u, v, w \in \mathbb{Z} \text{ such that } x = u\ell + vm + wn\}.$$

11. Prove the statement $(\star)$ below:

($\star$) *Let $m \in \mathbb{N}$ and $m \geq 2$. Suppose that for any $a, b \in \mathbb{Z}$, if ab is divisible by m then at least one of a, b is divisible by m. Then m is a prime number.*

Remark. Combining the statement ($\star$) with Euclid's Lemma, we obtain this characterization of prime numbers: *Let $p \in \mathbb{Z} \backslash \{-1, 0, 1\}$. p is a prime number iff (for any $a, b \in \mathbb{Z}$, if ab is divisible by p then at least one of a, b is divisible by p).*

12.$^\diamondsuit$ We introduce this definition below:

- *Let $a, b \in \mathbb{Z}$. a, b are said to be* **relatively prime** *if* $\gcd(a, b) = 1$.

Prove each of the statements below without applying the Fundamental Theorem of Arithmetic. Where necessary and appropriate, you may apply Bézout's Identity:

- *Let $m, n \in \mathbb{Z}$. There exist some $s, t \in \mathbb{Z}$ such that $sm + tn = \gcd(m, n)$.*

(a) *Let $a, b, c \in \mathbb{Z}$. Suppose a, c are relatively prime and ab is divisible by c. Then b is divisible by c.*

(b) *Let $a, b \in \mathbb{Z}$. Suppose there exist some $s, t \in \mathbb{Z}$ such that $sa + tb = 1$. Then a, b are relatively prime.*

Remark. According to the Euclidean Algorithm, if a, b are relatively prime (so that $\gcd(a, b) = 1$) then there exist some $s, t \in \mathbb{Z}$ such that $sa + tb = 1$. Hence a, b are relatively prime iff there exist some $s, t \in \mathbb{Z}$ such that $sa + tb = 1$.

(c) *Let $a, b \in \mathbb{Z}$, not both zero. $\dfrac{a}{\gcd(a, b)}, \dfrac{b}{\gcd(a, b)}$ are relatively prime.*

(d) *Let $a, b, c \in \mathbb{Z}$. Suppose a, b are relatively prime and a, c are relatively prime. Then a, bc are relatively prime.*

(e) *Let $a, b \in \mathbb{Z}$. Suppose a, b are relatively prime. Then a^2, b^2 are relatively prime.*

(f) *Let $a, b, c \in \mathbb{Z}$. Suppose a, b are relatively prime and c is divisible by each of a, b. Then c is divisible by ab.*

13.$^\heartsuit$ Apply mathematical induction to justify the statements below:

(a) *For any $n \in \mathbb{N} \backslash \{0, 1\}$, n is a prime number or a product of at least two prime numbers.*

(b) *For any $n \in \mathbb{N} \backslash \{0, 1\}$, if $p_1, p_2, \cdots, p_s$, $q_1, q_2, \cdots, q_t$ are prime numbers, $0 < p_1 \leq p_2 \leq \cdots \leq p_s$, $0 < q_1 \leq q_2 \leq \cdots \leq q_t$, $n = p_1 p_2 \cdot ... \cdot p_s$ and $n = q_1 q_2 \cdot ... \cdot q_t$, then $s = t$ and $p_1 = q_1$, $p_2 = q_2$, ... , $p_s = q_s$.*

Remark. In each part, you have to think carefully which proposition is to be formulated and proved by mathematical induction. The two statements are respectively the 'existence part' and the 'uniqueness part' of the **Fundamental Theorem of Arithmetic**. The theorem itself says that every integer greater than 1 can be 'factorized' into a product of prime numbers in one and only one way, up to re-ordering of the factors in the product.

14.$^\heartsuit$ We introduce the definitions below:

- *Let $a, b, m \in \mathbb{Z}$. We say m is a* **common multiple** *of a, b if m is divisible by each of a, b.*
- *Let $a, b \in \mathbb{Z}$.*
  - *Suppose both of a, b are non-zero. Then the* **least common multiple** *of a, b is defined to be the multiple of a, b of least value amongst all positive common multiples of a, b. It is denoted by* $\mathrm{lcm}(a, b)$.
  - *Suppose $a = 0$ or $b = 0$. Then the least common multiple of a, b is defined to be 0, and we write* $\mathrm{lcm}(a, b) = 0$.

Without applying the Fundamental Theorem of Arithmetic, prove that for any $a, b \in \mathbb{N}$, $\mathrm{lcm}(a, b) \gcd(a, b) = ab$.

15. (a) Prove the statements below:

i. *Let $\zeta \in \mathbb{C}$. Suppose $|\zeta| > \dfrac{1}{\sqrt{2}}$ and $\mathsf{Re}(\zeta) \geq 0$ and $\mathsf{Im}(\zeta) \geq 0$. Then $|\zeta - 1| < |\zeta|$ or $|\zeta - i| < |\zeta|$.*

ii.$^\diamondsuit$ *Let $\eta \in \mathbb{C}$. Suppose $|\eta| > \dfrac{1}{\sqrt{2}}$. Then at least one of $|\eta - 1|$, $|\eta + 1|$, $|\eta - i|$, $|\eta + i|$ is less than $|\eta|$.*

(b)$^\heartsuit$ Recall the definitions below:

- *Let $z \in \mathbb{C}$. z is said to be a* **Gaussian integer** *if both of $\mathsf{Re}(z)$, $\mathsf{Im}(z)$ are integers.*
- *The set of all Gaussian integers is denoted by $\mathbb{G}$.*

Prove the **Division Algorithm for Gaussian integers**:

- *Let $\mu, \nu \in \mathbb{G}$. Suppose $\nu \in \mathbb{G} \backslash \{0\}$. Then there exist some σ, ρ such that $\mu = \sigma\nu + \rho$ and $|\rho| \leq \dfrac{|\nu|}{\sqrt{2}}$.*

Remark. Imitate the argument for the Division Algorithm for natural numbers. Apply the Well-ordering Principle for integers to the set $\{x \in \mathbb{N} : \text{There exists some } \kappa \in \mathbb{G} \text{ such that } x = |\mu - \kappa\nu|^2\}$.

16. (a) Prove each of the statements below 'from first principles', using the definitions of set equality, subset relation, intersection, union, complement, where appropriate.

    i. *Let A, B, T be sets. Suppose $A \subset T$ and $B \subset T$. Then $A \cup B \subset T$.*

    ii. *Let A, B, T be sets. Suppose $A \subset T$ or $B \subset T$. Then $A \cap B \subset T$.*

    (b) Consider each of the statements below. For each of them, determine whether it is true or false. Justify your answer by giving a proof or constructing a counter-example where appropriate.

    i. *Let A, B, T be sets. Suppose $A \cup B \subset T$. Then $A \subset T$ and $B \subset T$.*

    ii. *Let A, B, T be sets. Suppose $A \cap B \subset T$. Then $A \subset T$ or $B \subset T$.*

    iii. *Let A, B, T be sets. Suppose $A \subset T$ or $B \subset T$. Then $A \cup B \subset T$.*

17.$^\diamond$ Consider each of the statements below. In each case, determine whether it is true or false. Justify your answer by giving an appropriate argument.

    (a) *Let A, B, C be sets. Suppose $A \cup (B \cap C) = (A \cup B) \cap C$. Then $A \subset C$.*

    (b) *Let A, B, C be sets. $A\backslash(B\backslash C) = (A\backslash B)\backslash C$.*

    (c) *Let A, B, C be sets. If $A \subset B$ then $C\backslash A \subset C\backslash B$.*

    (d) *Let A, B, C be sets. Suppose $A \subset B$ and $A \not\subset C$. Then $B \not\subset C$.*

    (e) *Let A, B, C be non-empty sets. Suppose $A \subset B$ and $B \not\subset C$. Then $A \not\subset C$.*

    (f) *Let A, B, C be non-empty sets. Suppose $A \subset B$ and $B \not\subset C$. Then $A \not\subset C$.*

    (g) *Let A, B, C be sets. Then $A \cup (B \triangle C) = (A \triangle B) \cup (A \triangle C)$.*

    (h) *Let A, B, C be sets. Then $A \cap (B \triangle C) = (A \triangle B) \cap (A \triangle C)$.*

18. (a)$^\diamond$ Consider each of the statements below. For each of them, determine whether it is true or false. Justify your answer by giving a proof or constructing a counter-example where appropriate.

    i. *Let A, B be sets. $B\backslash(B\backslash A) \subset A$.*

    ii. *Let A, B be sets. $A \subset B\backslash(B\backslash A)$.*

    (b)$^\clubsuit$ Prove the statements below:

    i. *Let A, B be sets. $A \subset B\backslash(B\backslash A)$ iff $A \subset B$.*

    ii. *Let A, B be sets. $B\backslash(B\backslash A) = A$ iff $A \subset B$.*

    iii. *Let A, B be sets. $B\backslash(B\backslash A) \subsetneqq A$ iff $A \not\subset B$.*

19. (a) Consider each of the statements below. For each of them, construct an appropriate counter-example to illustrate that it is false.

    i.$^\heartsuit$ *Let A, B be sets. Suppose $A \cap B = \emptyset$. Then $\mathfrak{P}(A \cup B) \subset \mathfrak{P}(A) \cup \mathfrak{P}(B)$.*

    ii.$^\heartsuit$ *Let A, B be non-empty sets. $\mathfrak{P}(A \cup B) \subset \mathfrak{P}(A) \cup \mathfrak{P}(B) \cup \mathfrak{P}(A \cap B)$.*

    (b)$^\clubsuit$ Prove the statements below:

    i. *Let A, B be sets. Suppose $\mathfrak{P}(A \cup B) \subset \mathfrak{P}(A) \cup \mathfrak{P}(B)$. Then ($A \subset B$ or $B \subset A$).*

    ii. *Let A, B be sets. Suppose ($A \subset B$ or $B \subset A$). Then $\mathfrak{P}(A \cup B) \subset \mathfrak{P}(A) \cup \mathfrak{P}(B)$.*

20. Prove the following statements:

    (a)$^\spadesuit$ *Let A, B be sets. $\mathfrak{P}(A\backslash B) \subset (\mathfrak{P}(A)\backslash\mathfrak{P}(B)) \cup \{\emptyset\}$.*

    (b)$^\spadesuit$ *Let A, B be sets. Suppose ($A \subset B$ or $A \cap B = \emptyset$). Then $\mathfrak{P}(A)\backslash\mathfrak{P}(B) \subset \mathfrak{P}(A\backslash B)$.*

    (c)$^\spadesuit$ *Let A, B be sets. Suppose $\mathfrak{P}(A)\backslash\mathfrak{P}(B) \subset \mathfrak{P}(A\backslash B)$. Then ($A \subset B$ or $A \cap B = \emptyset$).*

21. Dis-prove each of the statements below.

    (a) *Let A, B be sets. $\mathfrak{P}(A \triangle B) \subset (\mathfrak{P}(A) \triangle \mathfrak{P}(B)) \cup \{\emptyset\}$.*

    (b) *Let A, B be sets. $\mathfrak{P}(A \triangle B) \not\subset (\mathfrak{P}(A) \triangle \mathfrak{P}(B)) \cup \{\emptyset\}$.*

Remark. Note that these two statements are not negations of each other. (The statement $\sim((\forall x)(\forall y)P(x, y))$ is not the equivalent to the statement $(\forall x)(\forall y)(\sim P(x, y))$.)

22. Let M be a set, and $\{A_n\}_{n=0}^{\infty}$,$\{B_n\}_{n=0}^{\infty}$ be infinite sequences of subsets of M.

Define

$$G = \{x \in M : x \in A_n \text{ for any } n \in \mathbb{N}\}, \qquad H = \{x \in M : x \in A_n \text{ for some } n \in \mathbb{N}\},$$
$$I = \{x \in M : x \in B_n \text{ for any } n \in \mathbb{N}\}, \qquad J = \{x \in M : x \in B_n \text{ for some } n \in \mathbb{N}\}.$$

Prove the statements below:

(a)♣ *Suppose $A_n \subset B_n$ for any $n \in \mathbb{N}$. Then $G \subset I$ and $H \subset J$.*

(b)♡ *Suppose $K = \{x \in M : x \in A_m \cap B_n$ for some $m, n \in \mathbb{N}\}$. Then $K = H \cap J$.*

(c)♡ *Suppose $L = \{x \in M : x \in A_m \cup B_n$ for any $m, n \in \mathbb{N}\}$. Then $L = G \cup I$.*

23. We introduce the definitions below:

- *Let $\alpha \in \mathbb{C}$ and r be a positive real number. The set $\{z \in \mathbb{C} : |z - \alpha| < r\}$ is called the* **open disc in $\mathbb{C}$ with centre α and radius r**. *It is denoted by $D(\alpha, r)$*
- *Let V be a subset of $\mathbb{C}$. The set V is said to be* **open in $\mathbb{C}$** *if for any $\zeta \in V$, there exists some $\varepsilon > 0$ such that $D(\zeta, \varepsilon) \subset V$.*

(a) Prove the statement below:

For any $\alpha \in \mathbb{C}$, for any $\alpha > 0$, the set $D(\alpha, r)$ is open in $\mathbb{C}$.

(b) Verify that the sets below are open in $\mathbb{C}$:

i. $\mathbb{C}$.

ii. $\emptyset$.

iii. $\{\zeta \in \mathbb{C} : \mathsf{Re}(\zeta) > 0\}$.

iv. $\mathbb{C}\backslash\{0\}$.

v. $\{\zeta \in \mathbb{C} : 0 < \mathsf{Re}(\zeta) < 1 \text{ and } 0 < \mathsf{Im}(\zeta) < 1\}$.

vi. $\{\zeta \in \mathbb{C} : \mathsf{Re}(\zeta) \cdot \mathsf{Im}(\zeta) > 1 \text{ and } \mathsf{Re}(\zeta) > 0\}$.

(c)♢ Prove the statement below:

- *Let U, V be subsets of $\mathbb{C}$. Suppose U, V are open in $\mathbb{C}$. Then $U \cap V$ is open in $\mathbb{C}$.*

(d) Prove the statements below:

i.♢ *Let U, V be subsets of $\mathbb{C}$. Suppose U, V are open in $\mathbb{C}$. Then $U \cup V$ is open in $\mathbb{C}$.*

ii.♣ *Let C be a subset of $\mathfrak{P}(\mathbb{C})$. Suppose U is open in $\mathbb{C}$ for any $U \in C$. Define $W = \{\zeta \in \mathbb{C} : \zeta \in U$ for some $U \in C\}$. Then W is open in $\mathbb{C}$.*

(e) We introduce the definition below:

- *Let V be a subset of $\mathbb{C}$. Define $V^\circ = \{\zeta \in V : D(\zeta, r) \subset V$ for some $r > 0\}$. The set V° is called the* **interior of** *V (with respective to $\mathbb{C}$).*
  Remark. By definition $V^\circ \subset V$.

i.♡ Prove the statements below:

A. *Let S be a subset of $\mathbb{C}$. The interior S° is open in $\mathbb{C}$.*

B. *Let V be a subset of $\mathbb{C}$. The set V is open in $\mathbb{C}$ iff $V^\circ = V$.*

C. *Let U, V be subsets of $\mathbb{C}$. Let $C(V) = \{S \in \mathfrak{P}(\mathbb{C}) : S$ is open in $\mathbb{C}\}$. The statements below are logically equivalent:*

($\sharp$) *$U = V^\circ$.*

($\natural$) *For any subset T of V, if T is open then $T \subset U$.*

($\flat$) *$U = \{\zeta \in \mathbb{C} : \zeta \in S$ for some $S \in C(V)\}$.*

Remark. It is in the sense of this logical equivalence that we refer to V° as the 'maximal subset of V which is open in $\mathbb{C}$'.

ii. Find the respective interiors of the sets below in $\mathbb{C}$. You are not required to justify your answer.

A. $\{0\}$.

B. $\mathbb{C}$.

C. $\{\zeta \in \mathbb{C} : |\zeta| \leq 1\}$.

D. $\{\zeta \in \mathbb{C} : |\zeta| = 1\}$.

E. $\{\zeta \in \mathbb{C} : \mathsf{Re}(\zeta) \geq 0\}$.

F. $\{\zeta \in \mathbb{C} : |\mathsf{Re}(\zeta)| + |\mathsf{Im}(\zeta)| \leq 1\}$.