Numbers and Sets

Shing Tak Lam[*]

April 13, 2021

This document is intended for revision purposes. As a result, it does not contain any exposition. This is based off lectures given by Professor Imre Leader in Michaelmas 2020, but the order of content, as well as some of the proofs have been modified after the fact, primarily to provide simpler proofs for theorems. Note that this also contains theorems from examples sheets, as some are useful elsewhere.

Numbers and Sets is on *Paper 4*.

Contents

1 Number Theory

1.1 Prime Numbers

Definition (Multiples)**.** For a natural number $n \in \mathbb{N}$, the multiples of n are the numbers of the form kn, where $k \in \mathbb{N}$.

Definition (Divisor)**.** For natural numbers m and n, m is a divisor of n, denoted as $m \mid n$ if n is a multiple of m.

Definition (Prime)**.** A natural number $n \geq 2$ is prime if the only divisors of n are 1 and n.

[*] stl45@cam.ac.uk

Proposition. *Every natural number n can be expressed as a product of primes.*

Proof. Note we define the result of the empty product as 1.

Applying strong induction on n, $n = 2$ is true as 2 is prime. Now, given $n > 2$, if n is prime then we are done. Otherwise, n is composite. Say $n = ab$, where $1 < a, b < n$. By the inductive hypothesis, $a = p_1 \dots p_k$ and $b = q_1 \dots q_l$. Then $n = ab = p_1 \dots p_k q_1 \dots q_l$ and we are done. □

Theorem. *There are infinitely many primes.*

Proof. Suppose not. Denote the primes by $p_1, \dots, p_n$. Let $N = p_1 \dots p_n + 1$. Then N has no prime factor, as none of the primes $p_1, \dots, p_n$ divides N. Contradiction. □

1.2 Euclid's Algorithm

Definition (Highest Common Factor)**.** For $a, b \in \mathbb{N}$, a natural number c is a natural number satisfying

- $c \mid a$ and $c \mid b$
- If $d \mid a$ and $d \mid b$, then $c \mid d$.

Definition (Division Algorithm)**.** Given natural numbers n, k, the division algorithm finds integers $q, r \in \mathbb{Z}$ such that $n = qk + r$ and $0 \leq r < k$.

Algorithm. Recursion on n.

- If $n = 1$, then
  - If $k = 1$, then $n = 1 \times 1 + 0$
  - Otherwise, $n = 0 \times k + 1$
- If $n > 1$, we have that $n - 1 = qk + r$.
  - If $r < k - 1$, then $n = qk + (r + 1)$.
  - If $r = k - 1$, then $n = (q + 1)k + 0$.

□

Definition (Euclid's Algorithm)**.** For $a, b \in \mathbb{N}$, $a \geq b$.

Algorithm. By division algorithm, we can find $q_1, \dots$ and $r_1, \dots$ such that

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{n-1} &= q_{n+1} r_n + 0 \end{aligned}$$

Output r_n. □

Proposition. *Euclid's Algorithm Terminates*

Proof. $b > r_1 > r_2 \dots > r_n > 0$. □

Theorem. *The output of Euclid's Algorithm on a, b is the HCF of a, b.*

Proof. Clearly $r_n \mid r_{n-1}$. So $r_n \mid r_{n-2}$. Repeat and we get that $r_n \mid b$ and $r_n \mid a$.

Now suppose if $d \mid a$ and $d \mid b$. Then we have that $d \mid q_1 b$ and $d \mid a$, so $d \mid r_1$. Repeat this and we have that $d \mid r_i$ for $1 \leq i \leq n$. So $d \mid r_n$. □

Theorem (Bézout's Lemma, Bézout's Identity). *For all $a, b \in \mathbb{N}$, there exists $x, y \in \mathbb{Z}$ such that $ax + by = \text{hcf}(a, b)$.*

Proof. Run Euclid's Algorithm on a, b. We get that $r_i = u_i r_{i-1} + v_i r_{i-2}$. Using this, we can show that $r_n = u_n r_{n-1} + v_n r_{n-2} = u_n(u_{n-1}r_{n-2} + v_{n-1}r_{n-3}) + u_n r_{n-2} = (u_n u_{n-1} + v_n)r_{n-2} + u_n v_{n-1} r_{n-3}$. Repeat until we get that $r_n = sr_1 + tr_2 = sr_1 + t(b - q_2 r_1) = (s - tq_2)r_1 + bt = (s - tq_2)(a - bq_1) + bt = (s - tq_2)a + (t - q_1(s - tq_2))b$. □

Alternative Proof. Let h be the least positive linear combination of a and b. We claim that $h = \text{hcf}(a, b)$.

Suppose if $d \mid a$ and $d \mid b$, then clearly $d \mid xa + yb$ for all $x, y \in \mathbb{Z}$.

Now suppose for contradiction if $h \nmid a$. Then let $a = qh + r, 0 < r < h$. So $r = a - qh = a - (xa + yb) = (1 - x)a - yb < h$ is also a positive linear combination of x and y, and is less than h, Contradiction. □

1.3 Fundamental Theorem of Arithmetic

Lemma. *Let p be a prime, $a, b \in \mathbb{N}$. Then if $p \mid ab$, we must have $p \mid a$ or $p \mid b$.*

Proof. Suppose if $p \nmid a$. As $\text{hcf}(p, a) \mid p$, we must have that $\text{hcf}(p, a) = p$ or $\text{hcf}(p, a) = 1$. But as $p \nmid a$, we must have $\text{hcf}(p, a) = 1$. Hence there exists $x, y \in \mathbb{Z}$ such that $ax + py = 1$. Then $p(by) + a(bx) = b$. As $p \mid abx$ and $p \mid pby$, we must have that $p \mid b$. □

Theorem (Fundamental Theorem of Arithmetic). *Every natural number $n \geq 2$ can be expressed uniquely as a product of primes, up to reordering.*

Proof. We have already shown existence. Proceed by strong induction on n. The case for $n = 2$ is trivial.

Now suppose if $n = p_1 \dots p_k = q_1 \dots q_l$. Then as $p_1 \mid n$, $p_1 \mid q_1 \dots q_l$. So we must have that $p_1 \mid q_i$ for some i. Without loss of generality, we may assume $p_1 \mid q_1$. Then $p_1 = q_1$, as they are primes. Dividing through by $p_1 = q_1$, we have that $p_2 \dots p_k = q_2 \dots q_l$. By the inductive hypothesis we are done. □

Corollary. $\text{hcf}(x, y)\,\text{lcm}(x, y) = xy$.

Proof. Suffices to consider prime factors. Suppose if p is a prime factor of x and y, with a factor of p^a in x and p^b in y. The factor of p in $\text{hcf}(x, y)$ is $\min(a, b)$ and the factor in $\text{lcm}(x, y)$ is $\max(a, b)$. As $\min(a, b) + \max(a, b) = a + b$, we are done. □

1.4 Modular Arithmetic

Proposition. *Let p be prime, then every $a \not\equiv 0 \pmod{p}$ is invertible mod p.*

Proof. As $a \not\equiv 0 \pmod{p}$, we have that $\text{hcf}(a, p) = 1$. Thus there exists $x, y \in \mathbb{Z}$ such that $ax + py = 1$. So $ax \equiv 1 - py \equiv 1 \pmod{p}$. □

Proposition. *If $a \in \mathbb{Z}_p$, $a \neq 0$, then $0, a, 2a, \dots, (p-1)a$ are distinct elements of $\mathbb{Z}_p$.*

Proof. If $ia = ja$, then $(i - j)a = 0$. As $a \neq 0$, we must have that $i \equiv j \pmod{p}$. As $0 \leq i, j < p$, we must have that $i = j$. □

Consequently, as $\mathbb{Z}_p$ has p elements, $0, a, 2a, \dots, (p-1)a$ must be $0, 1, \dots, p-1$ in some order.

1.5 Fermat's Little Theorem

Theorem (Fermat's Little Theorem). *Let p be a prime, $a \in \mathbb{Z}_p$, $a \neq 0$. Then $a^{p-1} = 1$.*

Proof. We have already shown that $a, 2a, \dots, (p-1)a$ are distinct, so they are $1, \dots, p-1$ in some order. Multiplying them together, $a^{p-1}(p-1)! = (p-1)!$. As $(p-1)!$ is a product of invertible elements, it is itself invertible. So $a^{p-1} = 1$. □

Definition (Euler Totient Function). For a natural number n, the $\varphi(n)$ is the number x, where $1 \leq x \leq n$ and $\text{hcf}(x, n) = 1$.

Proposition. *If p is prime, then $\varphi(p) = p - 1$.*

Proposition. *If p is prime, then $\varphi(p^2) = p^2 - p$*

Proposition. *If p, q are prime, then $\varphi(pq) = pq - p - q + 1$.*

Proposition. *$\varphi(n)$ is the number of invertible elements in $\mathbb{Z}_n$.*

Theorem (Fermat-Euler Theorem)**.** *Let $n \geq 2$. Then in $\mathbb{Z}_n$, every invertible element $a \in \mathbb{Z}_n$ satisfies*

$$a^{\varphi(n)} = 1$$

Proof. Let the units of $\mathbb{Z}_n$ be $x_1, \dots, x_{\varphi(n)}$. Consider $ax_1, \dots, ax_{\varphi(n)}$. These are distinct (as a is invertible) and also invertible, so they must be $x_1, \dots, x_{\varphi(n)}$ in some order. Hence $a^{\varphi(n)}x_1 \dots x_{\varphi(n)} = x_1 \dots x_{\varphi(n)}$. Cancelling, we get that $a^{\varphi(n)} = 1$. □

1.6 Wilson's Theorem

Lemma. *Let p be prime. Then the only solutions to $x^2 = 1$ in $\mathbb{Z}_p$ are $x = 1$ and $x = -1 = p - 1$.*

Proof.

$$x^2 = 1 \iff x^2 - 1 = 0 \iff (x - 1)(x + 1) = 0$$

As p is prime, we must have $x - 1 = 0$ or $x + 1 = 0$. □

Theorem (Wilson's Theorem)**.** *Let p be prime. Then $(p - 1)! \equiv -1 \pmod{p}$.*

Proof. It is true for $n = 2$. Now let $p > 2$. Consider $1, \dots, p - 1$. We can pair up each a with a^{-1}, when $a^{-1} \neq a$. Note that $a^{-1} = a \iff a^2 = 1 \iff a = 1 \vee a = -1$. Consequently, $(p - 1)! = 1 \cdot (a_1 \cdot a_1^{-1}) \cdot \dots \cdot (a_k \cdot a_k^{-1}) \cdot (p - 1) = p - 1 = -1$. □

Proposition. *Let p be an odd prime. -1 is a square mod p if and only if $p \equiv 1 \pmod{4}$.*

Proof. Suppose for contradiction that $p = 4k + 3$, $x \in \mathbb{Z}_p$ and $x^2 = -1$. By Fermat's Little Theorem, we have that $-1 = (-1)^{2k+1} = (x^2)^{2k+1} = x^{4k+2} = 1$. Contradiction.

Now if $p = 4k+1$, from Wilson's Theorem we have that $(4k)! = -1$. Comparing $(4k)! = (1 \cdot \dots \cdot (2k))((2k+1) \cdot \dots \cdot (4k))$ and $((2k)!)^2 = (1 \cdot \dots \cdot (2k))(1 \cdot \dots \cdot (2k))$, and noting that $2k+n \equiv (2k+n) - (4k+1) \equiv -(2k-n+1) \pmod{4k+1}$. Hence we see that $((2k)!)^2$ and $(4k)!$ differ by $(-)$ signs only, and there are $2k$ $(-)$ signs, so in fact, we have that $((2k)!)^2 = (4k)! = -1$. □

1.7 Chinese Remainder Theorem

Theorem (Chinese Remainder Theorem)**.** *Let m, n be coprime. Then for any a, b, there exists x such that $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$. Moreover, x is unique mod mn.*

Proof. As m and n are coprime, there exists s, t such that $sm + tn = 1$. Then $x = atn + bsm$ satisfies $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$.

Now suppose if x' was also a solution. Then $x' \equiv x \pmod{m}$ and $x' \equiv x \pmod{n}$. So $m \mid x - x'$ and $n \mid x - x'$. As m, n are coprime, we have that $mn \mid x - x'$, so $x \equiv x' \pmod{mn}$. □

1.8 RSA

In this subsection, choose p, q large primes, $n = pq$, e coprime to $\varphi(n) = pq - p - q + 1$.

Definition (RSA)**.** To encode a message $x \in \mathbb{Z}_n$, map x to x^e.

To decode a message, using Euclid's Algorithm/Bézout's Lemma on e and $\varphi(n)$, we find d, k such that $de + k\varphi(n) = 1$. Then $de \equiv 1 \pmod{\varphi(n)}$. Then by Fermat-Euler, $(x^e)^d = x^{de} = x^{1-k\varphi(n)} = x$.

2 Real Numbers

2.1 Completeness

Proposition. *There is no rational $x \in \mathbb{Q}$ such that $x^2 = 2$.*

Proof. Suppose if $x^2 = 2$, $x = \frac{a}{b}$, $a, b \in \mathbb{N}$. Then $a^2 = 2b^2$. The exponent of 2 in the prime factorisation in a^2 is even, but it is odd in $2b^2$. Contradicting unique factorisation. □

Alternative Proof. Suppose if $x^2 = 2$, $x = \frac{a}{b}$, $a, b \in \mathbb{N}$. For any integers c, d, $cx + d$ is of the form $\frac{e}{b}$, for $e \in \mathbb{Z}$. Hence if $cx + d > 0$, we must necessarily have $cx + d > \frac{1}{b}$. As $1 < x^2 < 4$, we must have that $1 < x < 2$ and $0 < x - 1 < 1$. Thus $0 < (x-1)^n < \frac{1}{b}$ if n is large enough. Contradiction as $(x-1)^n$ is of the form $cx + d$, since $x^2 = 2$. □

Axiom (Least Upper Bound Axiom)**.** Every set that is nonempty and bounded above has a least upper bound. We call the least upper bound the supremum.

For the next proposition, consider the canonical map p from $\mathbb{N}$ to $\mathbb{R}$, where $p(1) = 1$ and $p(n+1) = p(n)+1$. We may also refer to $p(\mathbb{N})$, the image of $\mathbb{N}$ under p, as $\mathbb{N}$, as an embedding of the natural numbers into the reals.

Proposition (Axiom of Archimedes)**.** *The natural numbers are not bounded above in $\mathbb{R}$.*

Proof. Suppose not. Clearly $\mathbb{N}$ is nonempty. Let $c = \sup \mathbb{N}$. Then there exists $n \in \mathbb{N}$ such that $c - 1 < n \leq c$. But then $n + 1 \in \mathbb{N}$ and $n + 1 > c$. Contradiction. □

Corollary. *For all $\varepsilon > 0$, there exists $n \in \mathbb{N}$ such that $\frac{1}{n} < \varepsilon$.*

Theorem. *There exists $x \in \mathbb{R}$ such that $x^2 = 2$.*

Proof. Let $S = \{x \in \mathbb{R} : x^2 < 2\}$. S is nonempty, and bounded above. Ler $c = \sup S$.

Suppose if $c^2 < 2$. Then for $0 < t < 1$, and $t < \frac{2-c^2}{5}$, $(c+t)^2 = c^2 + 2ct + t^2 \leq c^2 + 5t < 2$. So $c + t \in S$, $c + t > c$. Contradiction.

Suppose if $c^2 > 2$, then for $0 < t < 2$, $t < \frac{c^2-2}{4}$, $(c-t)^2 = c^2 - 2ct + t^2 \geq c^2 - 4t \geq 2$. So $c - t$ is also an upper bound for S. Contradiction.

Thus, $c^2 = 2$. □

Theorem. *The rationals are dense in the reals.*

Proof. Without loss of generality, assume $0 \leq a < b$. Let $n \in \mathbb{N}$ be such that $\frac{1}{n} < b - a$. Then there must be a $q \in \mathbb{N}$ such that $\frac{q}{n} \leq a$ and $\frac{q+1}{n} > a$, as otherwise, an would be an upper bound to $\mathbb{N}$. Then we have that $a < \frac{q+1}{n} < b$. □

Similarly, the irrationals are dense in the reals.

2.2 Sequences

Definition (Convergence)**.** We say that $x_n \to c$ if for all $\varepsilon > 0$, there exists N, such that for all $n \geq N$, $|x_n - c| < \varepsilon$.

Proposition. *If x_n is increasing and bounded above then it is convergent.*

Proof. Let $c = \sup\{x_1, \dots\}$. Then given $\varepsilon > 0$, there exists N such that $c - \varepsilon < x_N \leq c$. Then for all $n \geq N$, $c - \varepsilon < x_N \leq x_n \leq c$. So $|x_n - c| < \varepsilon$. □

Proposition (Divergence of the Harmonic Series)**.** *The series* $\sum_{n=1}^{\infty} \frac{1}{n}$ *diverges.*

Proof. We have that $\frac{1}{3} + \frac{1}{4} \geq \frac{1}{2}$, and also $\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} \geq \frac{1}{2}$.

In general, we have that $\frac{1}{2^n + 1} + \frac{1}{2^n + 2} + \cdots + \frac{1}{2^{n+1}} \geq \frac{2^n}{2^{n+1}} = \frac{1}{2}$.

Therefore, the partial sums are unbounded. Thus, it can't be convergent, as any convergent series is bounded. □

Proposition (Convergence of the Basel Series)**.** *The series* $\sum_{n=1}^{\infty} \frac{1}{n^2}$ *converges.*

Proof. We have that $\frac{1}{2^2} + \frac{1}{3^2} \leq \frac{2}{2^2} = \frac{1}{2}$, and also $\frac{1}{4^2} + \frac{1}{5^2} + \frac{1}{6^2} + \frac{1}{7^2} \leq \frac{4}{4^2} = \frac{1}{4}$.

In general, we have that $\frac{1}{(2^n)} + \frac{1}{(2^n + 1)} + \cdots + \frac{1}{(2^{n+1} - 1)} \leq \frac{2^n}{(2^n)^2} = \frac{1}{2^n}$.

Hence, the partial sums are bounded above by $1 + \frac{1}{2} + \frac{1}{4} + \cdots = 2$, and increasing. Therefore it is convergent. □

2.3 *e*

Definition (e)**.** .

$$e = \sum_{n=0}^{\infty} \frac{1}{n!}$$

Note this sum converges as it is bounded above by $1 + 1 + \frac{1}{2} + \frac{1}{4} + \cdots = 3$.

Proposition. *e is irrational.*

Proof. Suppose not. Let $e = \frac{p}{q}$, $p, q \in \mathbb{N}$, $q > 1$. Then $q!e = p(q-1)! \in \mathbb{Z}$. Thus $\sum_{n=0}^{\infty} \frac{q!}{n!} \in \mathbb{Z}$.

Then $\frac{q!}{(q+1)!} = \frac{1}{q+1}$ and $\frac{q!}{(q+2)!} = \frac{1}{(q+1)(q+2)} \leq \frac{1}{(q+1)^2}$. In general $\frac{q!}{(q+n)!} \leq \frac{1}{(q+1)^n}$. Clearly, $\sum_{n=0}^{q} \frac{q!}{n!} \in \mathbb{Z}$, which means that $\sum_{n=q+1}^{\infty} \frac{q!}{n!}$ must also be an integer. However, $0 \leq \sum_{n=q+1}^{\infty} \frac{q!}{n!} \leq \sum_{n=q+1}^{\infty} \frac{1}{(q+1)^n} = \frac{1}{q} < 1$. Contradiction. □

2.4 Transcendental Numbers

Definition (Algebraic Numbers)**.** A real number x is algebraic if it is the root of a non-zero polynomial with integer coefficients.

Definition (Transcendental)**.** If x is not algebraic, then it is transcendental.

Theorem. *The number*

$$c = \sum_{n=1}^{\infty} \frac{1}{10^{n!}}$$

is transcendental.

Lemma. *For all polynomials p, there exists k such that for all $0 \leq x, y \leq 1$, $|p(x) - p(y)| \leq k|x - y|$*

Proof. Let $p(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$, then $p(x) - p(y) = a_d(x^d - y^d) + a_{d-1}(x^{d-1} - y^{d-1}) + \cdots + a_1(x - y)$.

Factoring out $(x - y)$, we get that $p(x) - p(y) = (x - y)(a_d(x^{d-1} + x^{d-2}y + \cdots + y^{d-1}) + a_{d-1}(x^{d-2} + x^{d-3}y + \cdots + y^{d-2}) + \cdots + a_1)$

Therefore

$$|p(x) - p(y)| = |x - y|\left|a_d(x^{d-1} + x^{d-2}y + \cdots + y^{d-1}) + \cdots + a_1\right|$$

Using the triangle inequality, we get that

$$\begin{aligned}|p(x) - p(y)| &\le |x - y|\left(\left|a_d(x^{d-1} + x^{d-2}y + \cdots + y^{d-1})\right| + \cdots + |a_1|\right)\\ &\le d(|a_1| + \cdots + |a_d|)|x - y|\end{aligned}$$

□

Lemma. *A polynomial of degree d has at most d roots.*

Proof. Given a polynomial p of degree d, if p has no roots then we are done. If p has a root a, then $p(x) = (x - a)q(x)$ where $q(x)$ is a polynomial of degree $d - 1$. Then every root of p is either a or a root of q. But q has at most $d - 1$ roots (by induction) □

Proof of Theorem. Let $c_n = \sum_{k=1}^{n} \frac{1}{10^{k!}}$. Then $c_n \to c$. Suppose for contradiction that c was algebraic. Then we must have some integer polynomial p such that $p(c) = 0$. From the lemma above, we have some k such that for $0 \le x, y \le 1$, $|p(x) - p(y)| \le k|x - y|$. Suppose further that p has degree d.

Now c_n is of the form $\frac{a}{10^{n!}}$, so $p(c_n)$ is of the form $\frac{b}{10^{d(n!)}}$ for $a, b \in \mathbb{Z}$. For n sufficiently large, c_n is not a root of p, as p has finitely many roots. Then we must have that $p(c_n) \ne 0$, so $|p(c_n)| \ge \frac{1}{10^{d(n!)}}$.

Thus $|p(c_n) - p(c)| = |p(c_n)| \ge \frac{1}{10^{d(n!)}}$.

Now $|c - c_n| = \sum_{k=n+1}^{\infty} \frac{1}{10^{k!}} \le \frac{2}{10^{(n+1)!}}$, so $|p(c_n) - |p(c)|| \le \frac{2k}{10^{(n+1)!}}$. This means that $\frac{1}{10^{d(n!)}} \le \frac{2k}{10^{(n+1)!}}$. Contradiction for n sufficiently large. □

Definition (Liouville Number)**.** A real number x is a Liouville number if for all natural numbers n, there exists infinitely many $(p, q) \in \mathbb{Z}$, $q > 1$ such that

$$0 < \left|x - \frac{p}{q}\right| < \frac{1}{q^n}$$

Intuitively, they are "almost rational" or "has very good rational approximations". The proof above can be modified to show that any Liouville number is transcendental.

3 Sets

3.1 Binomial Coefficients

Definition (Binomial Coefficients)**.** For $n \in \mathbb{N}$, $0 \le k \le n$, we denote by $\binom{n}{k}$ the number of ways to choose k items from n.

Proposition.

$$\binom{n}{k} = |\{S \in \mathcal{P}(\{1, \ldots, n\}) : |S| = k\}|$$

Proposition.

$$\binom{n}{k} = \binom{n}{n-k}$$

Proposition.

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

Proposition.

$$\binom{n}{k} = \frac{n(n-1)\dots(n-k+1)}{k!} = \frac{n!}{k!(n-k)!}$$

Proof. The number of ways to name a k-set is $n(n-1)\dots(n-k+1)$. However, each k-set is named $k\dots 1 = k!$ times, so the number of different k-sets is $\frac{n(n-1)\dots(n-k+1)}{k!}$. □

Theorem (Binomial Theorem)**.**

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}$$

Proof. If we expand $(a+b)^n$ we get terms of the form $a^k b^{n-k}$. We need to choose k of the as and $n-k$ of the bs, so there are $\binom{n}{k}$ ways to do this. □

Theorem (Inclusion-Exclusion)**.** *Define* $S_A = \bigcap_{i \in A} S_i$.

Let $S_1, \dots, S_n$ *be finite sets, then*

$$|S_1 \cup \dots \cup S_n| = \sum_{|A|=1} |S_A| - \sum_{|A|=2} |S_A| + \dots + (-1)^{n+1} \sum_{|A|=n} |S_a|$$

Proof. Let $x \in S_1 \cup \dots \cup S_n$, and suppose that x is in k of the S_i. The number of A with $|A| = 1$ and $x \in S_A$ is k. The number of A with $|A| = 2$ and $x \in S_A$ is $\binom{k}{2}$. In general, the number of A with $|A| = r$ and $x \in S_A$ is $\binom{k}{r}$. Consequently, the number of times x is counted on the right hand side is

$$k - \binom{k}{2} + \binom{k}{3} - \dots + (-1)^{k+1}\binom{k}{k} = 1 - \left(1 + (-1)^k\right) = 1$$

□

4 Functions

Proposition. $f : A \to B$ *is injective if and only if there exists* $g : B \to A$ *such that* $g \circ f = \mathrm{id}$.

Proof. If f is injective, define

$$g(b) = \begin{cases} a & \text{if } f(a) = b \\ \text{arbitrary} & \text{if } b \notin f(A) \end{cases}$$

Note that a must be unique as f is injective. Clearly $gf(a) = a$. On the other hand, if such a g exists, $f(x) = f(y) \implies gf(x) = gf(y) \implies x = y$. □

Proposition. $f : A \to B$ *is surjective if and only if there exists* $h : B \to A$ *such that* $f \circ h = \mathrm{id}$.

Proof. If f is surjective, define $h(b)$ to be an a such that $f(a) = b$, coming from surjectivity of f. Clearly $fh(b) = b$. On the other hand, if such an h exists, then $f(h(b)) = b$, so f is clearly surjective. □

Proposition. *If* f *is bijective, then* $g = h$*, and we denote this by* f^{-1}.

5 Equivalence Relations

Let $\sim$ be an equivalence relation on a set X.

Proposition. *Equivalence classes form a partition.*

Proof. Clearly $x \in [x]$, so equivalence classes are nonempty and they cover X. Now suppose if $t \in [x] \cap [y]$. Then $t \sim x$ and $t \sim y$, so $x \sim y$ and $[x] = [y]$. □

Proposition. *Partitions form an equivalence relation.*

Proof. Define $a \sim b$ for "a and b are in the same partition". This is an equivalence relation. □

Definition (Quotient). Define $X/\sim = \{[x] : x \in X\}$ to be the quotient of X by $\sim$.

Definition (Quotient Map). Define $q : X \to X/\sum$ by $x \mapsto [x]$.

6 Countability

Definition (Countable). A set X is countable if it is finite, or there exists a bijection $X \to \mathbb{N}$.

Proposition. *A set X is countable if and only if its elements can be listed as $x_1, x_2, \ldots$*

Proposition. *$\mathbb{Z}$ is countable.*

Proof. $0, 1, -1, 2, -2, \ldots$ □

Proposition. *A set X is countable if and only if there exists an injection $f : X \to \mathbb{N}$.*

Proof. ($\implies$). Trivial.

($\impliedby$). If X is finite, clearly it is countable. Now suppose if X is infinite. Clearly $f : X \to f(X)$ is a bijection. Suffices to show that $f(X)$ is countable.

Let $a_1 = \min(f(X))$, $a_2 = \min(f(X) \backslash \{a_1\})$, $a_3 = \min(f(X) \backslash \{a_1, a_2\})$ and so on. Then for each $a \in f(X)$, clearly it must be a_n for some $n \leq a$. Thus $f(X) = \{a_1, a_2, \ldots\}$. □

Theorem. *$\mathbb{N} \times \mathbb{N}$ is countable.*

Proof. Define $a_1 = (1, 1)$. Let $a_n = (p, q)$. If $p = 1$, $a_{n+1} = (q + 1, 1)$. If $p > 1$, $a_{n+1} = (p - 1, q + 1)$. Then $\mathbb{N} \times \mathbb{N} = \{a_1, a_2, \ldots\}$. □

Alternative Proof. $f(x, y) = 2^x 3^y$ is an injection. □

Theorem. *Let $(A_n)_{n \in \mathbb{N}}$ be a collection of countable sets. Then $A_1 \cup A_2 \cup \ldots$ is countable.*

Proof. For each A_i, list the elements as $a_{i,1}, a_{i,2}, \ldots$.

Define $f : \bigcup\limits_{n \in \mathbb{N}} \to \mathbb{N}$ by $f(x) = 2^i 3^j$ where $x = a_{i,j}$ and i is minimal. Clearly such an i exists as x must be in (at least) one of the A_i. f is an injection. □

Proposition. *$\mathbb{Q}$ is countable.*

Proof. Define $A_n = \dfrac{1}{n}\mathbb{Z} = \left\{\dfrac{k}{n} : k \in \mathbb{Z}\right\}$. Then $\mathbb{Q} = \bigcup\limits_{n \in \mathbb{N}} A_n$ and is countable. □

Proposition. *The set $\mathbb{A}$ of algebraic numbers is countable.*

Proof. As each integer polynomial has finitely many roots, suffices to show that the set of all integer polynomials is countable.

Define $A_d = \left\{a_d X^d + a_{d-1} X^{d-1} + \cdots + a_0 : a_0, \ldots, a_d \in \mathbb{Z}\right\}$. Then clearly A_d injects into $\mathbb{Z}^{d+1}$. So A_d is countable, and the set of all integer polynomials is countable. □

Theorem. *$\mathbb{R}$ is uncountable.*

Proof. We shall show that $(0,1)$ is uncountable. Suppose not. Let $(0,1) = r_1, r_2, \dots$, and for each r_i, let $r_i = 0.r_{i,1}r_{i,2}\dots$. Now define $s = 0.s_1s_2\dots$ by $s_n = \begin{cases} 5 & \text{if } r_{n,n} \neq 5 \\ 6 & \text{if } r_{n,n} = 5 \end{cases}$. Then clearly for all i, $r_i \neq s$. So we did not list all of the real numbers in $(0,1)$. □

Proposition. *The set of transcendental numbers $\mathbb{R}\backslash\mathbb{A}$ is uncountable.*

Proof. Suppose not. Then $\mathbb{R} = (\mathbb{R}\backslash\mathbb{A}) \cup \mathbb{A}$ would be countable. □

Theorem. *$\mathcal{P}(\mathbb{N})$ is uncountable.*

Proof. Suppose not. Let $\mathcal{P}(\mathbb{N}) = S_1, \dots$. Define $S = \{n \in \mathbb{N} : n \notin S_n\}$. Then for all i, $S \neq S_i$. □

Alternative Proof. Given $x \in (0,1)$, write $x = 0.x_1\dots$ in binary. Define $f(x) = \{n : x_n = 1\}$. Then $f : (0,1) \to \mathbb{N}$ is an injection. Hence if $\mathcal{P}(\mathbb{N})$ is countable, so is $(0,1)$. Contradiction. □

Theorem. *For any set X, there does not exist a surjection $X \to \mathcal{P}(X)$.*

Proof. Given any $f : X \to \mathcal{P}(X)$, define $S = \{x : x \notin f(x)\}$. Then $S \notin f(X)$. □

Theorem (Schröder-Bernstein)**.** *Given sets A and B, with $f : A \to B$ and $g : B \to A$ injections, there exists $h : A \to B$ which is bijective.*

Proof. For each $a \in A$, consider the chain $g^{-1}(a), f^{-1}g^{-1}(a), \dots$, as long as the inverses are well defined. This chain may be empty, may terminate or may be infinite. Define $\chi : a \to \mathbb{N} \cup \{\infty\}$ to be the length of the chain of a.

Define $A_0 = \{a \in A : \chi(a) \text{ even}\}$,$A_1 = \{a \in A : \chi(a) \text{ odd}\}$,$A_\infty = \{a \in A : \chi(a) = \infty\}$. Define similarly B_0, B_1, B_∞. Then $f : A_0 \to B_1$ is a bijection, and $g : B_0 \to A_1$ is a bijection. Furthermore, $f : A_\infty \to B_\infty$ is a bijection.

Hence $h(a) = \begin{cases} f(a) & \text{if } a \in A_0 \text{ or } a \in A_\infty \\ g^{-1}(a) & \text{if } a \in A_1 \end{cases}$ is a bijection. □