Part IA — Numbers and Sets

Theorems

Based on lectures by A. G. Thomason

Notes taken by Dexter Chua

Michaelmas 2014

Introduction to number systems and logic
Overview of the natural numbers, integers, real numbers, rational and irrational numbers, algebraic and transcendental numbers. Brief discussion of complex numbers; statement of the Fundamental Theorem of Algebra.

Ideas of axiomatic systems and proof within mathematics; the need for proof; the role of counter-examples in mathematics. Elementary logic; implication and negation; examples of negation of compound statements. Proof by contradiction. [2]

Sets, relations and functions
Union, intersection and equality of sets. Indicator (characteristic) functions; their use in establishing set identities. Functions; injections, surjections and bijections. Relations, and equivalence relations. Counting the combinations or permutations of a set. The Inclusion-Exclusion Principle. [4]

The integers
The natural numbers: mathematical induction and the well-ordering principle. Examples, including the Binomial Theorem. [2]

Elementary number theory
Prime numbers: existence and uniqueness of prime factorisation into primes; highest common factors and least common multiples. Euclid's proof of the infinity of primes. Euclid's algorithm. Solution in integers of $ax + by = c$.

Modular arithmetic (congruences). Units modulo n. Chinese Remainder Theorem. Wilson's Theorem; the Fermat-Euler Theorem. Public key cryptography and the RSA algorithm. [8]

The real numbers
Least upper bounds; simple examples. Least upper bound axiom. Sequences and series; convergence of bounded monotonic sequences. Irrationality of $\sqrt{2}$ and e. Decimal expansions. Construction of a transcendental number. [4]

Countability and uncountability
Definitions of finite, infinite, countable and uncountable sets. A countable union of countable sets is countable. Uncountability of R. Non-existence of a bijection from a set to its power set. Indirect proof of existence of transcendental numbers. [4]

Contents

0 Introduction

1 Proofs and logic

1.1 Proofs

1.2 Examples of proofs

Proposition. For all natural numbers n, $n^3 - n$ is a multiple of 3.

Proposition. If n^2 is even, then so is n.

Proposition. The solutions to $x^2 - 5x + 6 = 0$ are $x = 2$ and $x = 3$.

Proposition. Every positive number is ≥ 1.

1.3 Logic

2 Sets, functions and relations

2.1 Sets

Theorem. $(A = B) \Leftrightarrow (A \subseteq B \text{ and } B \subseteq A)$

Proposition.

- $(A \cap B) \cap C = A \cap (B \cap C)$
- $(A \cup B) \cup C = A \cup (B \cup C)$
- $A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$

2.2 Functions

Theorem. The left inverse of f exists iff f is injective.

Theorem. The right inverse of f exists iff f is surjective.

2.3 Relations

Theorem. If $\sim$ is an equivalence relation on A, then the equivalence classes of $\sim$ form a partition of A.

3 Division

3.1 Euclid's Algorithm

Theorem (Division Algorithm)**.** Given $a, b \in \mathbb{Z}$, $b \neq 0$, there are unique $q, r \in \mathbb{Z}$ with $a = qb + r$ and $0 \leq r < b$.

Proposition. If $c \mid a$ and $c \mid b$, $c \mid (ua + vb)$ for all $u, v \in \mathbb{Z}$.

Theorem. Let $a, b \in \mathbb{N}$. Then (a, b) exists.

Corollary. (from the proof) Let $d = (a, b)$, then d is the smallest positive linear combination of a and b.

Corollary (Bézout's identity)**.** Let $a, b \in \mathbb{N}$ and $c \in \mathbb{Z}$. Then there exists $u, v \in \mathbb{Z}$ with $c = ua + vb$ iff $(a, b) \mid c$.

Proposition (Euclid's Algorithm)**.** If we continuously break down a and b by the following procedure:

$$\begin{aligned} a &= q_1 b + r_1 \\ b &= q_2 r_1 + r_2 \\ r_1 &= q_3 r_2 + r_3 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} \end{aligned}$$

then the highest common factor is r_{n-1}.

3.2 Primes

Theorem. Every number can be written as a product of primes.

Theorem. There are infinitely many primes.

Theorem. If $a \mid bc$ and $(a, b) = 1$, then $a \mid c$.

Corollary. If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$. (True for all p, a, b)

Corollary. If p is a prime and $p \mid n_1 n_2 \cdots n_i$, then $p \mid n_i$ for some i.

Theorem (Fundamental Theorem of Arithmetic)**.** Every natural number is expressible as a product of primes in exactly one way. In particular, if $p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l$, where p_i, q_i are primes but not necessarily distinct, then $k = l$. $q_1, \cdots q_l$ are $p_1, \cdots p_k$ in some order.

Corollary. If $a = p_1^{i_1} p_2^{i_2} \cdots p_r^{i_r}$ and $b = p_1^{j_1} p_2^{j_2} \cdots p_r^{j_r}$, where p_i are distinct primes (exponents can be zero). Then $(a, b) = \prod p_k^{\min\{i_k, j_k\}}$. Likewise, $\text{lcm}(a, b) = \prod p_k^{\max\{i_k, j_k\}}$. We have $\text{hcf}(a, b) \times \text{lcm}(a, b) = ab$.

4 Counting and integers

4.1 Basic counting

Theorem (Pigeonhole Principle)**.** If we put $mn + 1$ pigeons into n pigeonholes, then some pigeonhole has at least $m + 1$ pigeons.

Proposition.

(i) $i_A = i_B \Leftrightarrow A = B$

(ii) $i_{A\cap B} = i_A i_B$

(iii) $i_{\bar{A}} = 1 - i_A$

(iv) $i_{A\cup B} = 1 - i_{\overline{A\cup B}} = 1 - i_{\bar{A}\cap\bar{B}} = 1 - i_{\bar{A}} i_{\bar{B}} = 1 - (1 - i_A)(1 - i_B) = i_A + i_B - i_{A\cap B}$.

(v) $i_{A\setminus B} = i_{A\cap\bar{B}} = i_A i_{\bar{B}} = i_A(1 - i_B) = i_A - i_{A\cap B}$

Proposition. $|A \cup B| = |A| + |B| - |A \cap B|$

Theorem (Inclusion-Exclusion Principle)**.** Let A_i be subsets of a finite set X, for $1 \leq i \leq n$. Then

$$|\bar{A}_1 \cap \cdots \cap \bar{A}_n| = |X| - \sum_i |A_i| + \sum_{i<j} |A_i \cap A_j| - \cdots + (-1)^n |A_1 \cap \cdots A_n|.$$

Equivalently,

$$|A_1 \cup \cdots \cup A_n| = \sum_i |A_i| - \sum_{i<j} |A_i \cap A_j| + \cdots + (-1)^{n-1} |A_1 \cap \cdots \cap A_n|.$$

The two forms are equivalent since $|A_1 \cup \cdots \cup A_n| = |X| - |\bar{A}_1 \cap \cdots \cap \bar{A}_n|$.

4.2 Combinations

Proposition. By definition,

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{n} = 2^n$$

Theorem (Binomial theorem)**.** For $n \in \mathbb{N}$ with $a, b \in \mathbb{R}$, we have

$$(a+b)^n = \binom{n}{0} a^n b^0 + \binom{n}{1} a^{n-1} b^1 + \cdots + \binom{n}{r} a^{n-r} b^r + \cdots + \binom{n}{n} a^0 b^n$$

Proposition.

(i) $\binom{n}{r} = \binom{n}{n-r}$. This is because choosing r things to keep is the same as choosing $n - r$ things to throw away.

(ii) $\binom{n}{r-1}+\binom{n}{r}=\binom{n+1}{r}$ (Pascal's identity) The RHS counts the number of ways to choose a team of r players from $n+1$ available players, one of whom is Pietersen. If Pietersen is chosen, there are $\binom{n}{r-1}$ ways to choose the remaining players. Otherwise, there are $\binom{n}{r}$ ways. The total number of ways is thus $\binom{n}{r-1}+\binom{n}{r}$.

Now given that $\binom{n}{0}=\binom{n}{n}=1$, since there is only one way to choose nothing or everything, we can construct *Pascal's triangle*:

$$\begin{array}{ccccccccccc} & & & & & 1 & & & & & \\ & & & & 1 & & 1 & & & & \\ & & & 1 & & 2 & & 1 & & & \\ & & 1 & & 3 & & 3 & & 1 & & \\ & 1 & & 4 & & 6 & & 4 & & 1 & \end{array}$$

where each number is the sum of the two numbers above it, and the rth item of the nth row is $\binom{n}{r}$ (first row is row 0).

(iii) $\binom{n}{k}\binom{k}{r}=\binom{n}{r}\binom{n-r}{k-r}$. We are counting the number of pairs of sets (Y,Z) with $|Y|=k$ and $|Z|=r$ with $Z\subseteq Y$. In the LHS, we first choose Y then choose $Z\subseteq Y$. The RHS chooses Z first and then choose the remaining $Y\setminus Z$ from $\{1,2,\cdots n\}\setminus Z$.

(iv) $\binom{a}{r}\binom{b}{0}+\binom{a}{r-1}\binom{b}{1}+\cdots+\binom{a}{r-k}\binom{b}{k}+\cdots\binom{a}{0}\binom{b}{r}=\binom{a+b}{r}$ (Vandermonde's convolution) Suppose we have a men and b women, and we need to choose a committee of r people. The right hand side is the total number of choices. The left hand side breaks the choices up according to the number of men vs women.

Proposition. $\binom{n}{r}=\dfrac{n!}{(n-r)!r!}$.

4.3 Well-ordering and induction

Theorem (Weak Principle of Induction)**.** Let $P(n)$ be a statement about the natural number n. Suppose that

(i) $P(1)$ is true

(ii) $(\forall n)\, P(n)\Rightarrow P(n+1)$

Then $P(n)$ is true for all $n\geq 1$.

Theorem. Inclusion-exclusion principle.

Theorem (Strong principle of induction)**.** Let $P(n)$ be a statement about $n\in\mathbb{N}$. Suppose that

(i) $P(1)$ is true

(ii) $\forall n\in N$, if $P(k)$ is true $\forall k<n$ then $P(n)$ is true.

Then $P(n)$ is true for all $n \in N$.

Theorem. The strong principle of induction is equivalent to the weak principle of induction.

Theorem (Well-ordering principle)**.** $\mathbb{N}$ is well-ordered under the usual order, i.e. every non-empty subset of $\mathbb{N}$ has a minimal element.

Theorem. The well-ordering principle is equivalent to the strong principle of induction.

5 Modular arithmetic

5.1 Modular arithmetic

Proposition. If $a \equiv b \pmod{m}$, and $d \mid m$, then $a \equiv b \pmod{d}$.

Proposition. If $a \equiv b \pmod{m}$ and $u \equiv v \pmod{m}$, then $a + u \equiv b + v \pmod{m}$ and $au \equiv bv \pmod{m}$.

Theorem. There are infinitely many primes that are $\equiv -1 \pmod{4}$.

Theorem. u is a unit modulo m if and only if $(u, m) = 1$.

Corollary. If $(a, m) = 1$, then the congruence $ax \equiv b \pmod{m}$ has a unique solution $\pmod{m}$.

Proposition. There is a solution to $ax \equiv b \pmod{m}$ if and only if $(a, m) \mid b$.

If $d = (a, m) \mid b$, then the solution is the unique solution to $\frac{a}{d}x \equiv \frac{b}{d}x \pmod{\frac{m}{d}}$

5.2 Multiple moduli

Theorem (Chinese remainder theorem)**.** Let $(m, n) = 1$ and $a, b \in \mathbb{Z}$. Then there is a unique solution (modulo mn) to the simultaneous congruences

$$\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases},$$

i.e. $\exists x$ satisfying both and every other solution is $\equiv x \pmod{mn}$.

Proposition. Given any $(m, n) = 1$, c is a unit mod mn iff c is a unit both mod m and mod n.

Proposition.

(i) $\phi(mn) = \phi(m)\phi(n)$ if $(m, n) = 1$, i.e. ϕ is multiplicative.

(ii) If p is a prime, $\phi(p) = p - 1$

(iii) If p is a prime, $\phi(p^k) = p^k - p^{k-1} = p^k(1 - 1/p)$

(iv) $\phi(m) = m \prod_{p|m}(1 - 1/p)$.

5.3 Prime moduli

Theorem (Wilson's theorem)**.** $(p - 1)! \equiv -1 \pmod{p}$ if p is a prime.

Theorem (Fermat's little theorem)**.** Let p be a prime. Then $a^p \equiv a \pmod{p}$ for all $a \in \mathbb{Z}$. Equivalently, $a^{p-1} \equiv 1 \pmod{p}$ if $a \not\equiv 0 \pmod{p}$.

Theorem (Fermat-Euler Theorem)**.** Let a, m be coprime. Then

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Proposition. If p is an odd prime, then -1 is a quadratic residue if and only if $p \equiv 1 \pmod{4}$.

Proposition. (Unproven) A prime p is the sum of two squares if and only if $p \equiv 1 \pmod 4$.

Proposition. There are infinitely many primes $\equiv 1 \pmod 4$.

Proposition. Let $p = 4k + 3$ be a prime. Then if a is a quadratic residue, i.e. $a \equiv z^2 \pmod p$ for some z, then $z = \pm a^{k+1}$.

5.4 Public-key (asymmetric) cryptography

Theorem (RSA Encryption)**.** We want people to be able to send a message to Bob without Eve eavesdropping. So the message must be encrypted. We want an algorithm that allows anyone to encrypt, but only Bob to decrypt (e.g. many parties sending passwords with the bank).

Let us first agree to write messages as sequences of numbers, e.g. in ASCII or UTF-8.

After encoding, the encryption part is often done with RSA encryption (Rivest, Shamier, Adleman). Bob thinks of two large primes p, q. Let $n = pq$ and pick e coprime to $\phi(n) = (p-1)(q-1)$. Then work out d with $de \equiv 1 \pmod{\phi(n)}$ (i.e. $de = k\phi(n) + 1$). Bob then publishes the pair (n, e).

For Alice to encrypt a message, Alice splits the message into numbers $M < n$. Alice sends $M^e \pmod n$ to Bob.

Bob then computes $(M^e)^d = M^{k\phi(n)+1} \equiv M \pmod n$ by Fermat-Euler theorem.

How can Eve find M? We can, of course, factorize n, find e efficiently, and be in the same position as Bob. However, it is currently assumed that this is hard. Is there any other way? Currently we do not know if RSA can be broken without factorizing (cf. RSA problem).

6 Real numbers

6.1 Construction of numbers

Proposition. $\mathbb{Q}$ is a totally ordered-field.

Proposition. $\mathbb{Q}$ is densely ordered, i.e. for any $p, q \in \mathbb{Q}$, if $p < q$, then there is some $r \in \mathbb{Q}$ such that $p < r < q$.

Proposition. There is no rational $q \in \mathbb{Q}$ with $q^2 = 2$.

Axiom (Least upper bound axiom)**.** Every non-empty set of the real numbers that has an upper bound has a least upper bound.

Corollary. Every non-empty set of the real numbers bounded below has an infimum.

Theorem (Axiom of Archimedes)**.** Given $r \in \mathbb{R}$, there exists $n \in \mathbb{N}$ with $n > r$.

Proposition. $\inf\{\frac{1}{n} : n \in \mathbb{N}\} = 0$.

Theorem. $\mathbb{Q}$ is dense in $\mathbb{R}$, i.e. given $r, s \in \mathbb{R}$, with $r < s$, $\exists q \in \mathbb{Q}$ with $r < q < s$.

Theorem. There exists $x \in \mathbb{R}$ with $x^2 = 2$.

6.2 Sequences

Theorem. Every bounded monotonic sequence converges.

Theorem. Every sequence has a monotonic subsequence.

Theorem.

(i) If $a_n \to a$ and $a_n \to b$, then $a = b$ (i.e. limits are unique)

(ii) If $a_n \to a$ and $b_n = a_n$ for all but finitely many n, then $b_n \to a$.

(iii) If $a_n = a$ for all n, then $a_n \to a$.

(iv) If $a_n \to a$ and $b_n \to b$, then $a_n + b_n \to a + b$

(v) If $a_n \to a$ and $b_n \to b$, then $a_n b_n \to ab$

(vi) If $a_n \to a \neq 0$, and $\forall n(a_n \neq 0)$. Then $1/a_n \to 1/a$.

(vii) If $a_n \to a$ and $b_n \to a$, and $\forall n(a_n \leq c_n \leq b_n)$, then $c_n \to a$. (Sandwich theorem)

6.3 Series

6.4 Irrational numbers

Proposition. A number is periodic iff it is rational.

6.5 Euler's number

Proposition. e is irrational.

6.6 Algebraic numbers

Proposition. All rational numbers are algebraic.

Theorem. (Liouville 1851; Non-examinable) L is transcendental, where

$$L = \sum_{n=1}^{\infty} \frac{1}{10^{n!}} = 0.11000100\cdots$$

with 1s in the factorial positions.

Theorem. (Hermite 1873) e is transcendental.

Theorem. (Lindermann 1882) π is transcendental.

7 Countability

Lemma. If $f : [n] \to [n]$ is injective, then f is bijective.

Corollary. If A is a set and $f : A \to [n]$ and $g : A \to [m]$ are both bijections, then $m = n$.

Lemma. Let $S \subseteq \mathbb{N}$. Then either S is finite or there is a bijection $g : \mathbb{N} \to S$.

Theorem. The following are equivalent:

(i) A is countable

(ii) There is an injection from $A \to \mathbb{N}$

(iii) $A = \emptyset$ or there is a surjection from $\mathbb{N} \to A$

Proposition. The integers $\mathbb{Z}$ are countable.

Proposition. $\mathbb{N} \times \mathbb{N}$ is countable.

Proposition. If $A \to B$ is injective and B is countable, then A is countable (since we can inject $B \to \mathbb{N}$).

Proposition. $\mathbb{Z}^k$ is countable for all $k \in \mathbb{N}$

Theorem. A countable union of countable sets is countable.

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

Theorem. The set of algebraic numbers is countable.

Theorem. The set of real numbers $\mathbb{R}$ is uncountable.

Corollary. There are uncountable many transcendental numbers.

Theorem. Let A be a set. Then there is no surjection from $A \to \mathcal{P}(A)$.

Theorem (Cantor-Schröder-Bernstein theorem)**.** Suppose there are injections $A \to B$ and $B \to A$. Then there's a bijection $A \leftrightarrow B$.