# Part IA - Numbers and Sets

## Definitions

Lectured by A. G. Thomason

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. Euclids proof of the infinity of primes. Euclids 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

# 1 Sets, functions and relations

## 1.1 Sets

**Definition** (Set)**.** A *set* is a collection of stuff, without regards to order. Elements in a set are only counted once. e.g. If $a = 2, b = c = 1$, then $A = \{a, b, c\}$ has only two members.

**Definition** (Equality of sets)**.** $A$ is equal to $B$, written as $A = B$, if $\forall x(x \in A \Leftrightarrow x \in B)$, i.e. two sets are equal if they have the same elements.

**Definition** (Subsets)**.** $A$ is a *subset* of $B$, written as $A \subseteq B$ or $A \subset B$, if all elements in $A$ are in $B$. i.e. $\forall x(x \in A \Rightarrow x \in B)$.

**Definition** (Intersection, union, set difference, symmetric difference and power set)**.** Given two sets $A$ and $B$, we define the following:

- Intersection: $A \cap B = \{x : x \in A \text{ and } x \in B\}$
- Union: $A \cup B = \{x : x \in A \text{ or } x \in B\}$
- Set difference: $A \setminus B = \{x \in A : x \notin B\}$
- Symmetric difference: $A \Delta B = \{x : x \in A \text{ xor } x \in B\}$, i.e. the elements in exactly one of the two sets
- Power set: $\mathcal{P}(X) = \{X : X \subseteq P\}$, i.e. the set of all subsets

**Definition** (Ordered pair)**.** An *ordered pair* $(a, b)$ is a pair of two items in which order matters. Formally, it is defined as $\{a, \{a, b\}\}$. We have $(a, b) = (a', b')$ iff $a = a'$ and $b = b'$.

**Definition** (Cartesian product)**.** Given two sets $A, B$, the *Cartesian product* of $A$ and $B$ is $A \times B = \{(a, b) : a \in A, b \in B\}$. This can be extended to $n$ products, e.g. $\mathbb{R}^3 = \mathbb{R} \times \mathbb{R} \times \mathbb{R} = \{(x, y, z) : x, y, z \in \mathbb{R}\}$

## 1.2 Functions

**Definition** (Function/map)**.** A *function* (or *map*) $f : A \to B$ is a "rule" that assigns, for each $a \in A$, precisely one element $f(a) \in B$. We can write $a \mapsto f(a)$. Formally, we say $f \subseteq A \times B$ such that $\forall a \in A$, there exists a unique $b \in B$ such that $(a, b) \in f$.

**Definition** (Injective function)**.** A function $f$ is *injective* if it hits everything at most once, i.e.

$$\forall x, y \in X(f(x) = f(y) \Rightarrow x = y)$$

**Definition** (Surjective function)**.** A function is *surjective* if it hits everything at least once, i.e.

$$\forall y \in Y(\exists x \in X(f(x) = y))$$

**Definition** (Bijective function)**.** A function is *bijective* if it is both injective and surjective. i.e. it hits everything exactly once. Note that a function has an inverse iff it is bijective.

**Definition** (Permutation (function))**.** A *permutation* of $A$ is a bijection $A \to A$.

**Definition** (Composition of functions)**.** The *composition* of two functions is a function you get by applying one after another. In particular, if $f : X \to Y$ and $G : Y \to Z$, then $g \circ f : X \to Z$ with $g \circ f(x) = g(f(x))$. Note that function composition in associative.

**Definition** (Image of function)**.** If $f : A \to B$ and $U \subseteq A$, then $f(U) = \{f(u) : u \in U\}$.

$f(A)$ is the *image* of $A$. We have $f$ is surjective iff $f(A) = B$.

**Definition** (Pre-image of function)**.** If $f : A \to B$ and $V \subseteq B$, then $f^{-1}(V) = \{a \in A : f(a) \in V\}$.

**Definition** (Identity map)**.** The *identity map* $\mathrm{id}_A : A \to A$ is defined as the map $a \mapsto a$.

**Definition** (Left inverse of function)**.** Given $f : A \to B$, a *left inverse* of $f$ is a function $g : B \to A$ such that $g \circ f = \mathrm{id}_A$.

**Definition** (Right inverse of function)**.** Given $f : A \to B$, a *right inverse* of $f$ is a function $g : B \to A$ such that $f \circ g = \mathrm{id}_B$.

**Definition** (Inverse of function)**.** An *inverse* of $f$ is a function that is both a left inverse and a right inverse. It is written as $f^{-1} : B \to A$. It exists if $f$ is bijective.

## 1.3 Relations

**Definition** (Relation)**.** A *relation* $R$ on $A$ specifies that some elements of $A$ are related to some others. Formally, $R \subseteq A \times A$. We write $aRb$ iff $(a, b) \in R$.

**Definition** (Reflective relation)**.** A relation $R$ is *reflective* if $\forall a(aRa)$.

**Definition** (Symmetric relation)**.** A relation $R$ is *symmetric* iff $\forall a, b(aRb \Leftrightarrow bRa)$.

**Definition** (Transitive relation)**.** A relation $R$ is *transitive* iff $\forall a, b, c(aRb \vee bRc \Rightarrow aRc)$.

**Definition** (Equivalence relation)**.** A relation is an *equivalence relation* if it is reflexive, symmetric and transitive. e.g. (i) and (vi) in the above examples are equivalence relations.

**Definition** (Partition of set)**.** A *partition* of a set $X$ is a collection of subsets $A_\alpha$ of $X$ such that each element of $X$ is in exactly one of $A_\alpha$.

**Definition** (Equivalence class)**.** If $\sim$ is an equivalence relation, then the *equivalence class* $[x]$ is the set of all elements that are related via $\sim$ to $x$.

**Definition** (Quotient map)**.** The *quotient map* $q$ maps each element in $A$ to the equivalence class containing $a$, i.e. $a \mapsto [a]$. e.g. $q(8\heartsuit) = \{\heartsuit\}$.

# 2 Division

## 2.1 Euclid's Algorithm

**Definition** (Factor of integers)**.** Given $a, b \in \mathbb{Z}$, we say *a divides b*, *a* is a *factor* of $b$ or $a|b$ if $\exists c \in \mathbb{Z}(b = ac)$. For any $b$, $\pm 1$ and $\pm b$ are always factors of $b$. The other factors are called *proper factors*

**Definition** (Common factor of integers)**.** A *common factor* of $a$ and $b$ is a number $c \in \mathbb{Z}$ such that $c|a$ and $c|b$.

**Definition** (Highest common factor/greatest common divisor)**.** The *highest common factor* or *greatest common divisor* of two numbers $a, b \in \mathbb{N}$ is a number $d \in \mathbb{N}$ such that $d$ is a common factor of $a$ and $b$, and if $c$ is also a common factor, $c|d$.

Clearly if the hcf exists, it must be the largest common factor, since all other common factors divide it, and thus necessarily unique.

## 2.2 Primes

**Definition** (Prime number)**.** $p \in \mathbb{N}$ is a *prime* if $p > 1$ and the only factors of $p$ are $\pm 1$ and $\pm p$.

**Definition** (Coprime numbers)**.** We say $a, b$ are *coprime* if $(a, b) = 1$.

# 3 Counting and Integers

**Definition** (Indicator function/characteristic function)**.** Let $X$ be a set. For each $A \in X$, the *indicator function* or *characteristic function* of $A$ is the function $i_A : X \to \{0, 1\}$ with $i_A(x) = 1$ if $x \in A$, 0 otherwise. It is sometimes written as $\chi_A$.

## 3.1 Combinations

**Definition** (Combination $\binom{n}{r}$)**.** There are $\binom{n}{r}$ subsets of $\{1, 2, 3, \cdots, n\}$ of size $r$. The symbol is pronounced as "$n$ choose $r$".
*Note*: This is a definition of $\binom{n}{r}$, and does not specify the value of it.

## 3.2 Well-ordering and induction

**Definition** (Partial order)**.** A *partial order* on a set is a reflective, antisymmetric $((aRb) \wedge (bRa) \Leftrightarrow a = b)$ and transitive relation.

**Definition** (Total order)**.** A *total order* is a partial order where $\forall a \neq b$, exactly one of $aRb$ or $bRa$ holds.

**Definition** (Well-ordered total order)**.** A total order is *well-ordered* if every non-empty subset has a minimal element, i.e. if $S \neq \emptyset$, then $\exists m \in S$ such that $x < m \Rightarrow x \notin S$.

# 4 Modular arithmetic

**Definition** (Modulo)**.** If $a, b \in \mathbb{Z}$ have the same remainder after division by $m$, i.e. $n|(a-b)$, we say $a$ and $b$ are *congruent modulo* $m$, and write

$$a \equiv b \pmod{m}$$

We can also interpret as $a$ and $b$ have the same last digit when written in base $m$.

**Definition** (Unit (modular arithmetic))**.** $u$ is a *unit* if $\exists v$ such that $uv \equiv 1 \pmod{m}$.

## 4.1 Multiple moduli

**Definition** (Euler's totient function)**.** We denote by $\phi(m)$ the number of integers $a$, $0 \leq a \leq m$, such that $(a, m) = 1$, i.e. $a$ is a unit (mod $m$). Note $\phi(1) = 1$.

## 4.2 Prime moduli

**Definition** (Quadratic residues)**.** The *quadratic residues* are the "squares" mod $p$, i.e. $1^2, 2^2, \cdots, (p-1)^2$.

## 4.3 Public-key (Asymmetric) cryptography

### 4.3.1 RSA encryption

# 5 Real numbers

## 5.1 Construction of natural numbers

**Definition** (Natural numbers)**.** Formally, $\mathbb{N}$ is defined by Peano's axioms. $\mathbb{N}$ is a set with a special element 1 and a map $S : \mathbb{N} \to \mathbb{N}$ that maps $n$ to its "successor" (intuitively, it is $+1$) such that:

(i) $\forall n(S(n) \neq 1)$

(ii) $\forall n, m(n \neq m \Rightarrow S(n) \neq S(m))$

(iii) $\forall A \subseteq \mathbb{N}\{[(1 \in A) \wedge (n \in A \Rightarrow S(n) \in A)] \Rightarrow (A = \mathbb{N})\}$ (Equivalent to weak induction)

Then write $2 = S(1)$, $3 = S(2)$ etc. We can define addition and multiplication recursively and show all rules of arithmetic are satisfied by induction.

This can be explicitly constructed by defining $1 = \emptyset$, $2 = \{1\}$, $3 = \{1, 2\}$ etc. and $S(n) = \{n\} \cup n$ in general.

## 5.2 Construction of integers

**Definition** (Integers)**.** $\mathbb{Z}$ is obtained from $\mathbb{N}$ by allowing subtraction. Formally, we can have $\mathbb{Z}$ to be the equivalence classes of $\mathbb{N} \times \mathbb{N}$ with $(a, b) \sim (c, d)$ iff $a + d = b + c$.

We write $a$ for $[(a, 0)]$ and $-a$ for $[(0, a)]$[1], and define $(a, b)+(c, d) = (a+c, b+d)$ and $(a, b)\times(c, d) = (ac+bd, bd+ad)$ (since $(a-b)(c-d) = (ac+bd)-(bd+ad)$). We can check that these are well-defined.

## 5.3 Construction of rationals

**Definition** (Rationals)**.** $\mathbb{Q}$ is obtained from $\mathbb{Z}$ by allowing division. Formally, we can have $Q$ to be the equivalence classes of $\mathbb{Z} \times \mathbb{N}$ with $(a, b) \sim (c, d)$ iff $ad = bc$.

We write $\frac{a}{n}$ for $[(a, b)]$. We can define $(a, b) + (c, d) = (ad + bc, bd)$ and $(a, b) \times (c, d) = (ac, bd)$. We can check that these are well-defined and satisfies the usual properties.

**Definition** (Totally ordered field)**.** $F$ with $+, \times, \leq$ is a totally ordered field if

(i) $F$ is an additive abelian group with identity 0.

(ii) $F \setminus \{0\}$ is a multiplicative abelian group with identity 1.

(iii) Multiplication is distributed over addition: $a(b + c) = ab + ac$.

(iv) $\leq$ is a total order.

(v) $\forall p, q, r \in F$, $p \leq q \Rightarrow p + r \leq q + r$

(vi) $\forall p, q, r \in F$, $p \leq q, 0 \leq r \Rightarrow pr \leq qr$

[1] Someone pointed out to me that according to the above definition of natural numbers, 0 doesn't exist. This problem can be solved either by defining $\mathbb{N}$ to contain 0, or write $a$ as $[(a + 1, 0)]$ etc. However, for the sake of consistency and clarity of expression, I'll keep the defintions this way.

*Note*: In any ordered field, $0 < 1$, since we know that $0 \neq 1$ by definition and if $1 < 0$, adding $-1$ to both sides, we obtain $0 < -1$. Since $0 < -1$ and $0 < -1$, then $0 < (-1)^2 = 1$. Contradiction.

## 5.4 Construction of real numbers

**Definition** (Least upper bound/supremum and greatest lower bound/infimum)**.** $s \in X$ is a *least upper bound* (or *supremum*) for the set $S \subseteq X$, denoted as $s = \sup X$, if

(i) $s$ is an upper bound for $S$, i.e. $\forall x \in S(x \leq s)$.

(ii) if $t$ is any upper bound for $S$, then $s \leq t$.

Similarly, $s \in X$ is a *greatest lower bound* (or *infimum*) if $s$ is a lower bound and any lower bound $t \leq s$.

**Definition** (Real numbers)**.** The *real numbers* is a totally ordered field containing $\mathbb{Q}$ that satisfies the least upper bound axiom.

**Definition** (Dedekind cut)**.** A *Dedekind cut* of $\mathbb{Q}$ is a set of partition of $\mathbb{Q}$ into $L$ and $R$ such that $\forall l \in L, r \in R(l < r)$ and $R$ has no minimum, i.e. a partition that splits $\mathbb{Q}$ into a "left" and "right" sets.

**Definition** (Closed and open intervals)**.** A *closed interval* $[a, b]$ with $a \leq b \in R$ is the set $\{x \in \mathbb{R} : a \leq x \leq b\}$ n An *open interval* $(a, b)$ with $a \leq b \in R$ is the set $\{x \in \mathbb{R} : a < x < b\}$.

## 5.5 Sequences

**Definition** (Sequence)**.** A *sequence* is a function $\mathbb{N} \to \mathbb{R}$. If $a$ is a sequence, instead of $a(1), a(2), \cdots$, we usually write $a_1, a_2, \cdots$.

**Definition** (Limit of sequence)**.** The sequence $(a_n)_{n=1}^{\infty}$ *tends to* $l \in \mathbb{R}$ as $n$ tends to infinity if and only if

$$\forall \epsilon > 0\{\exists N \in \mathbb{N}[\forall n \geq N(|a_n - l| < \epsilon)]\}$$

If $a_n$ tends to $l$ as $n$ tends to infinity, we write $a_n \to l$ as $n \to \infty$; $\lim\limits_{n\to\infty} a_n = l$; or $a_n$ converges to $l$.

**Definition** (Convergence of sequence)**.** The sequence $a_n$ *converges* if there exists an $l$ such that $a_n \to l$. The sequence *diverges* if it doesn't converge.

**Definition** (Subsequence)**.** A *subsequence* of $(a_n)$ is $a_{g(n)}$ where $g : \mathbb{N} \to \mathbb{N}$ is strictly increasing. e.g. $a_2, a_3, a_5, a_7 \cdots$ is a subsequence of $a_n$.

## 5.6 Series

**Definition** (Series and partial sums)**.** Let $a_n$ be a sequence. Then $s_m = \sum_{n=1}^{m} a_n$ is the *mth partial sum* of the *series* whose $n$th term is $a_n$. We write

$$\sum_{n=1}^{\infty} a_n = \lim_{m\to\infty} s_m$$

If the limit exists.

### 5.6.1 Decimal expansions

**Definition** (Decimal expansion)**.** Let $(d_n)$ be a sequence with $d_n \in \{0, 1, \cdots 9\}$. Then $\displaystyle\sum_{n=1}^{\infty} \frac{d}{10^n}$ converges to a limit $r$ with $0 \leq r \leq 1$ since the partial sums $s_m$ are increasing and bounded by $\sum \frac{9}{10^n} \to 1$ (geometric series). We say $r = 0.d_1 d_2 d_3 \cdots$, the *decimal expansion* of $r$.

## 5.7 Irrational numbers

**Definition** (Irrational number)**.** Numbers in $\mathbb{R} \setminus \mathbb{Q}$ are *irrational.*

**Definition** (Periodic number)**.** A decimal is *periodic* if after a finite number $\ell$ of digits, it repeats in blocks of $k$ for some $k$, i.e. $d_{n+k} = d_n$ for $n > \ell$.

## 5.8 Euler's number

**Definition** (Euler's number)**.**

$$e = \sum_{j=0}^{\infty} \frac{1}{1!} = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots$$

## 5.9 Algebraic numbers

**Definition** (Algebraic and transcendental numbers)**.** An *algebraic number* is a root of a polynomial with integer coefficients (or rational coefficients). A number is *transcendental* if it is not algebraic.

# 6 Countability

**Definition** (Finite set and cardinality of set)**.** The set $A$ is *finite* if there exists some $n \in \mathbb{N}_0$ and a bijection $A \to [n]$. The *cardinality* or *size* of $A$, written as $|A|$, is $n$. By corollary, this is well-defined.

**Definition** (Countable set)**.** A set $A$ is *countable* if $A$ is finite or there is a bijection between $A$ and $\mathbb{N}$. A set $A$ is *uncountable* if $A$ is not countable.