Numbers & Sets - Theorems & Proofs

Lectured by Prof Imre Leader

Michaelmas 2013

1 Elementary Number Theory

1.1 $\mathbb{N}$ and $\mathbb{Z}$

Proposition 1. Every natural number $n \geq 2$ is expressible as a product of primes.

Proof. Induction on n: if n not prime, write $n = ab$ for $1 < a, b < n$ and (by induction) have $a = p_1 p_2 \dots p_k$, $b = q_1 q_2 \dots q_l$, some primes p_i, q_i, thus $n = p_1 \dots p_k q_1 \dots q_l$. □

Theorem 2. There are infinitely many primes.

Proof. Suppose not: let $p_1, p_2 \dots p_k$ be all the primes. Let $n = p_1 p_2 \dots p_k + 1$. Then no p_i divides n. So n has no primes factors, contradicting Prop. 1 (every n expressible as product of primes). □

Proposition 3 (Division algorithm)**.** Let $k, n \in \mathbb{N}$. Then $n = qk + r$, some $q, r \in \mathbb{Z}$ with $0 \leq r \leq k - 1$.

Proof. Induction on n: given $n \geq 1$ can write $n - 1 = qk + r$, some $q, r \in \mathbb{Z}$ with $0 \leq r \leq k - 1$.

If $r < k - 1$, have $n = qk + (r + 1)$. If $r = k - 1$, have $n = (q + 1)k + 0$. □

Proposition 4. The output of Euclid's algorithm on a, b is the hcf of a, b.

Proof. Let c be the output. Show that c divides a and b by following the algorithm backwards. Given $d \mid a$ and $d \mid b$, show that $d \mid c$ by following the algorithm forwards. □

Proposition 5. $\forall a, b \in \mathbb{N}\ \exists x, y \in \mathbb{Z}$ with $ax + by = (a, b)$.

Proof 1. Having run Euclid on a, b with output $c = r_n$: have c a linear combination of r_{n-1} and r_{n-2}, so c a linear combination of r_{n-2} and $_{n-3}$, ..., and c a linear combination of r_i and r_{i-1} for all i (inductively). Hence c a linear combination of a and b. □

Proof 2. Let h be the least positive integer of the form $xa + yb$, some $x, y \in \mathbb{Z}$. Claim: $h = (a, b)$.

If $d \mid a$ and $d \mid b$ then d divides every linear combination of a and b, hence $d \mid h$.

To show $h \mid a$: suppose not, then write $a = qh + r$, some $q, r \in \mathbb{Z}$ with $1 \leq r \leq h - 1$. Then $r = a - qh = a - q(xa + yb)$, so r a linear combination of a and b, contradicting choice of h. So $h \mid a$ and similarly $h \mid b$. □

Corollary 6 (Bezout's Theorem)**.** Let $a, b, c \in \mathbb{N}$. Then $\exists x, y \in \mathbb{Z}$ with $ax + by = c \iff \text{hcf}(a, b) \mid c$.

Proof. Let $h = \text{hcf}(a, b)$.

Left to right: have $h \mid a$ and $h \mid b$, so $h \mid ax + by$ i.e. $h \mid c$.

Right to left: have $h \mid c$ and have $h = ax + by$, some $x, y \in \mathbb{Z}$, so $c = \frac{c}{h}(ax + by)$. □

Proposition 7. Let $a, b \in \mathbb{N}$ and p be prime. Then $p \mid ab \implies p \mid a$ or $p \mid b$.

Proof. Suppose $p \nmid a$, so want $p \mid b$.

Have $(p, a) = 1$ (since p is prime), so $px + ay = 1$ for some $x, y \in \mathbb{Z}$. So, $bpx + bay = b$, hence b is a multiple of p (since ab is a multiple of p). □

Theorem 8 (Fundamental Theorem of Arithmetic)**.** Let $n \geq 2$ be a natural number. Then n can be written as a product of primes, uniquely (up to reordering).

Proof. Existence: Prop. 1.

Uniqueness: Induction on n: True for $n = 2$.

Given $n > 2$: Suppose that $n = p_1 \dots p_k = q_1 \dots q_l$, must show that $k = l$ and (after reordering) $p_i = q_i \ \forall i$.

Have $p_i \mid q_1 q_2 \dots q_l$, so $p_1 \mid q_i$ for some i (Prop. 7). Reordering, we may assume that $p_1 = q_1$. So $p_2 \dots p_k = q_2 \dots q_l$. By induction, have $k = l$ and (after reordering) $p_2 = q_2$, $p_3 = q_3$, … $p_k = q_k$. □

1.2 Modular Arithmetic

Proposition 9. Let p be prime. Then every integer $a \not\equiv 0 \ (p)$ is invertible mod p. (i.e. in $\mathbb{Z}_p$: $a \neq 0 \implies a$ invertible.

Proof 1. Have $(a, p) = 1$, so $ax + py = 1$, some $x, y \in \mathbb{Z}$. Thus $ax \equiv 1 \ (p)$. □

Proof 2. Consider in $\mathbb{Z}_p$ the numbers $a \cdot 0, a \cdot 1, a \cdot 2, \dots a \cdot (p-1)$. They are distinct, as: $ai \equiv aj \ (p) \implies a(i - j) \equiv 0 \ (p) \implies i - j \equiv 0 \ (p)$ (since $a \not\equiv 0 \ (p)$). So $i = j$ (since $0 \leq i, j \leq p - 1$). Thus $a \cdot 0, a \cdot 1, a \cdot 2, \dots a \cdot (p-1)$ are $0, 1, 2, \dots p - 1$ in some order. In particular, $ax = 1$ for some x. □

Proposition 9′. Let a be an integer. Then a is invertible in $\mathbb{Z}_n$ if and only if $(a, n) = 1$.

Proof. a invertible $\iff ax \equiv 1 \ (n)$, some $x \iff ax + ny = 1$, some $x, y \iff (a, n) \mid 1$ (Bezout) $\iff (a, n) = 1$. □

Theorem 10 (Fermat's (little) Theorem)**.** Let p be prime. Then, in $\mathbb{Z}_p$, $a^{p-1} = 1 \ \forall a \neq 0$. (i.e. $a \not\equiv 0 \ (p) \implies a^{p-1} \equiv 1 \ (p)$)

Proof. In $\mathbb{Z}_p$, consider $a \cdot 1, a \cdot 2, \dots, a(p-1)$. Then are distinct (as a is invertible) and non-zero (as $ab = 0 \implies a = 0$ or $b = 0$). So they are $1, 2, \dots, p-1$ in some order. Multiplying, $a^{p-1}(p-1)! = (p-1)!$. So $a^{p-1} = 1$ as $(p-1)!$ is invertible (a product of invertibles is invertible). □

Theorem 10′ (Fermet-Euler Theorem)**.** For a invertible in $\mathbb{Z}_n$, have $a^{\phi(n)} = 1$ (i.e. if $(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \ (n)$).

Proof. Let $x_1, x_2, \dots x_{\phi(n)}$ be the invertibles in $\mathbb{Z}_n$. Then, in $\mathbb{Z}_n$: $ax_1, ax_2, \dots, ax_{\phi(n)}$ are distinct (as a is invertible) and invertible (as a product of invertibles). So they are $x_1, \dots, x_{\phi(n)}$ in some order. Thus $a^{\phi(n)} x_1 x_2 \dots x_{\phi(n)} = x_1 x_2 \dots x_{\phi(n)}$, so $a^{\phi(n)} = 1$ (cancelling each x_i in turn). □

Lemma 11. Let p be prime. Then in $\mathbb{Z}_p$, $x^2 = 1 \implies x = 1$ or -1.

Proof. Have $x^2 = 1 \implies x^2 - 1 = 0 \implies (x+1)(x-1) = 0$. So $x + 1 = 0$ or $x - 1 = 0$ (as p prime). Thus $x = \pm 1$. $\square$

Theorem 12 (Wilson's Theorem)**.** Let p be prime. Then $(p-1)! = -1$ in $\mathbb{Z}_p$ (i.e. $(p-1)! \equiv -1 \ (p)$).

Proof. We may assume that $p > 2$ (it can be easily checked for $p = 2$).

Each $1 \leq a \leq p-1$ can be paired with a^{-1} (in $\mathbb{Z}_p$). We have $a^{-1} \neq a \ \forall a \neq \pm 1$ (Lemma 11). So, in $1 \cdot 2 \cdot 3 \cdot \ldots (p-1)$, terms cancel in pairs a, a^{-1} except for ± 1. Thus $(p-1)! = 1 \cdot 1 \cdot 1 \cdot \ldots 1 \cdot -1 = -1$. $\square$

Theorem 13. Let $p > 2$ be prime. Then -1 is a square mod p if and only if $p \equiv 1 \ (4)$.

Proof. For $p = 4k+3$: suppose $x^2 = -1$ in $\mathbb{Z}_p$. Have $x^{4k+2} = 1$ (by Fermat). But $x^{4k+2} = (x^2)^{2k+1} = (-1)^{2k+1} = -1$, which is a contradiction.

For $p = 4k+1$: have $1 \cdot 2 \cdot 3 \ldots (2k)(2k-1) \ldots (4k-1)(4k) = -1$.

But $4k = -1$, $4k-1 = -2$, ..., $2k-1 = -(2k)$. So, $-1 = (4k)! = (2k)!^2(-1)^{2k} = (2k)!^2$. Thus $x = (2k)!$ has $x^2 = -1$. $\square$

Theorem 14 (Chinese Remainder Theorem)**.** Let m, n be coprime. Then $\forall a, b \in \mathbb{Z} \ \exists x \in \mathbb{Z}$ with $x \equiv a \ (m)$ and $x \equiv b \ (n)$. Moreover, x is unique mod mn.

Proof. Existence: Have $ms + nt = 1$, some $s, t \in \mathbb{Z}$. So $ms \equiv 0 \ (m)$ and $ms \equiv 1 \ (n)$, while $nt \equiv 1 \ (m)$ and $nt \equiv 0 \ (n)$. Hence $a(nt) + b(ms) \equiv a \ (m)$ and $b \ (n)$.

Uniqueness: Having found one solution x, any $x' \equiv x \ (mn)$ is also a solution. Conversely, if x' is a solution, then $m \mid x' - x$ (as $x \equiv x' \ (m)$) and $n \mid x' - x$ (as $x \equiv x' \ (n)$). So $mn \mid x' - x$ (as m, n coprime). $\square$

2 The Reals

Proposition 1. No rational x has $x^2 = 2$.

Proof 1. Suppose $x \in \mathbb{Q}$ has $x^2 = 2$, say $x = \frac{m}{n}$, where $m, n \in \mathbb{N}$ (may assume $x > 0$ as $(-x)^2 = x^2$ and $x \neq 0$ since $0^2 = 0 \neq 2$). So $\left(\frac{m}{n}\right)^2 = 2$ i.e. $m^2 = 2n^2$. But exponent of 2 in prime factorisation of LHS is *even* and exponent of 2 in prime factorisation of RHS is *odd*, which is a contradiction. $\square$

Proof 2. Suppose $x = \frac{m}{n}$ has $x^2 = 2$. Then any $a + bx$ $(a, b \in \mathbb{Z})$ is of form $\frac{c}{n}$, some $c \in \mathbb{Z}$, so $a + bx > 0 \implies a + bx \geq \frac{1}{n}$. But $0 < x - 1 < 1$ (as $1 < x < 2$), so $(x-1)^N < \frac{1}{n}$ for N large. But $(x-1)^N$ is of form $ax + b$ (using $x^2 = 2$). This is a contradiction. $\square$

Proposition 2 (Axiom of Archimedes)**.** $\mathbb{N}$ is not bounded above in $\mathbb{R}$.

Proof. Suppose not: let $c = \sup \mathbb{N}$. Then $c - 1$ is *not* an upper bound for $\mathbb{N}$, so $\exists n \in \mathbb{N}$ with $n > c - 1$. Then $n + 1 > c$, which is a contradiction. $\square$

Corollary 3. Let $t \in \mathbb{R}$ with $t > 0$. Then $\exists n \in \mathbb{N}$ with $\frac{1}{n} < t$.

Proof. Choose $n \in \mathbb{N}$ with $n > \frac{1}{t}$ (Prop. 2). Then $\frac{1}{n} < t$. $\square$

Theorem 4. $\exists x \in \mathbb{R}$ with $x^2 = 2$.

Proof. Let $S = \{x \in \mathbb{R} : x^2 \leq 2\}$. Then S is non-empty (e.g. $1 \in S$), and bounded above ($x \leq 2 \; \forall x \in S$). So let $c = \sup S$.

Claim: $c^2 = 2$.

Proof of claim:

If $c^2 < 2$: Consider $(c+t)^2$, where $t > 0$. Have $(c+t)^2 = c^2 + 2ct + t^2 \leq c^2 + 5t$ (for $t \leq 1$ as $c \leq 2$), which is less than 2 for small t ($t < \frac{2-c^2}{5}$). Hence $c + t \in S$, contradicting c being an upper bound for S.

If $c^2 > 2$: Consider $(c-t)^2$, where $t > 0$. Have $(c-t)^2 = c^2 - 2ct + t^2 \geq c^2 - 4t$ (as $c \leq 2$), which is greater than 2 for small t ($t < \frac{c^2-2}{4}$. Hence $(c-t)^2 > 2$, contradicting c being the *least* upper bound of S.

Therefore, $c^2 = 2$. $\square$

2.1 Convergence

Proposition 5. If $x_n \to c$ and $y_n \to d$ then $x_n + y_n \to c + d$.

Proof. Given $\epsilon > 0$:

$\exists N$ with $|x_n - c| < \frac{\epsilon}{2} \; \forall n \geq N$ and $\exists M$ with $|y_n - d| < \frac{\epsilon}{2} \; \forall n \geq M$. So, $\forall n \geq \max(N, M)$, we have: $|x_n - c| < \frac{\epsilon}{2}$ and $|y_n - d| < \frac{\epsilon}{2}$, so $|(x_n + y_n) - (c + d)| < \frac{\epsilon}{2} + \frac{\epsilon}{2}$. $\square$

Theorem 6. Let $x_2, x_2, \ldots$ be an increasing sequence bounded above. Then $(x_n)_{n=1}^{\infty}$ is convergent.

Proof. Let $c = \sup \{x_2, x_2, \ldots\}$. Claim: $x_n \to c$.

Proof of claim: Given $\epsilon > 0$:

There exists N with $x_N > c - \epsilon$ (since $c - \epsilon$ is not an upper bound), so $\forall n \geq N$: $x_n \geq x_{n-1} \geq \ldots \geq x_N$ (inductively). So $c - \epsilon < x_n \leq c < c + \epsilon$. $\square$

Proposition 7. $\sum_{n=1}^{\infty} \frac{1}{n}$ diverges.

$\sum_{n=1}^{\infty} \frac{1}{n^2}$ converges.

Proof. Have $\frac{1}{3} + \frac{1}{4} \geq \frac{1}{4} + \frac{1}{4} = 2$ and $\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} \geq 4 \cdot \frac{1}{8} = \frac{1}{2}$.

And in general, $\frac{1}{2^n+1} + \frac{1}{2^n+2} + \ldots + \frac{1}{2^{n+1}} \geq \frac{2^n}{2^{n+1}} = \frac{1}{2}$. So the partial sums of $\sum_{n=1}^{\infty} \frac{1}{n}$ are unbounded, so it diverges.

Have $\frac{1}{2^2} + \frac{1}{3^2} \leq \frac{1}{2^2} + \frac{1}{2^2} = \frac{1}{2}$ and $\frac{1}{4^2} + \frac{1}{5^2} + \frac{1}{6^2} + \frac{1}{7^2} \leq 4 \cdot \frac{1}{4^2} = \frac{1}{4}$.

And in general, $\frac{1}{(2^n)^2} + \frac{1}{(2^n+1)^2} + \ldots + \frac{1}{(2^{n+1}-1)^2} \leq \frac{2^n}{(2^n)^2} = \frac{1}{2^n}$. Hence the partial sums of $\sum_{n=1}^{\infty} \frac{1}{n^2}$ are bounded above (by $1 + \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \ldots = 2$). So it converges (by Thm. 6). $\square$

Proposition 8. e is irrational.

Proof. Suppose $e = \frac{p}{q}$, some $p, q \in \mathbb{N}, q \neq 1$ (noting that $2 < e < 3$).

Have $\frac{p}{q} = \sum_{n=0}^{\infty} \frac{1}{n!}$, so $\sum_{n=0}^{\infty} \frac{q!}{n!} \in \mathbb{Z}$. But $\sum_{n=0}^{q} \frac{q!}{n!} \in \mathbb{Z}$. Also, $\frac{q!}{(q+1)!} = \frac{1}{q+1}$, $\frac{q!}{(q+2)!} \leq \frac{1}{(q+1)^2}$, $\frac{q!}{(q+3)!} \leq \frac{1}{(q+1)^3}, \ldots$. So, $\sum_{n=q+1}^{\infty} \frac{q!}{n!} \leq \frac{1}{q+1} + \frac{1}{(q+1)^2} + \ldots = \frac{1}{q} < 1$. Contradicting $\sum_{n=0}^{\infty} \frac{q!}{n!}$ being an integer. $\square$

Proposition 9. The number $\sum_{n=1}^{\infty} \frac{1}{10^{n!}} = 0.110001000000000000000001 0\ldots$ is not algebraic.

Proof. *Non-examinable. $\square$

3 Sets and Functions

Proposition 1. Let A be a set of size n. Then A has exactly 2^n subsets.

Proof. May as well have $A = \{1, \dots, n\}$. To specify a subset B, we must specify:

Is $1 \in B$ or not?

Given that, is $2 \in B$ or not?

$\vdots$

Given that, is $n \in B$ or not?

So, in total, have $2 \times 2 \times \dots \times 2 = 2^n$ subsets.

(Alternatively, do induction on n, in which there are 2 ways to 'extend' a subset of $\{1, \dots, n-1\}$, by including n or not.) $\square$

Theorem 2 (Binomial Theorem)**.** Let $a, b \in \mathbb{R}$ and $n \in \mathbb{N}$. Then

$(a+b)^n = \binom{n}{n}a^n + \binom{n}{n-1}a^{n-1}b + \dots + \binom{n}{1}ab^{n-1} + \binom{n}{0}b^n$.

Proof. Expanding $(a+b)^n = (a+b)(a+b)\dots(a+b)$, we get terms of the form $a^k b^{n-k}$. The number of terms $a^k b^{n-k}$ is $\binom{n}{k}$ since we select k of the brackets for the 'a' terms. $\square$

Proposition 3. $\binom{n}{k} = \frac{n(n-1)(n-2)\dots(n-k+1)}{k!}$.

Proof. The number of ways to specify a k-set is $n \times (n-1) \times \dots \times (n-k+1)$ since you specify an element, then a different element, all the way up to the kth element.

The number of times a given k-set is specified is $k \times (k-1) \times \dots \times 1$ since you name an element from the k-set, then another one and so on.

Thus, the actual number of k-sets is the quotient of the two. $\square$

Theorem 4 (Inclusion-Exclusion Theorem)**.** Let $S_1, \dots S_n$ be finite sets.

Then $|\bigcup_{i=1}^n S_i| = \sum_{|A|=1} |S_A| + \sum_{|A|=2} |S_A| + \sum_{|A|=3} |S_A| - \dots + (-1)^{n+1} \sum_{|A|=n} |S_A|$ where $S_{\{x_1,\dots,x_k\}} = S_{x_1} \cap \dots \cap S_{x_K}$ and the sums are over all $A \subset \{1, \dots, n\}$ of given size.

Proof. Take $x \in$ LHS, and let us show that x is counted exactly once on RHS. Let x belong to k of the S_i.

The number of $S_A, |A| = 1$ that x belongs to is k.

The number of $S_A, |A| = 2$ that x belongs to is $\binom{k}{2}$.

In general, x belongs to $\binom{k}{r}$ of the $S_A, |A| = r$ (for $1 \le r \le k$), and none of the $S_A, |A| > k$.

So the number of times x is counted on RHS is $k - \binom{k}{2} + \binom{k}{3} - \dots + (-1)^{k+1}\binom{k}{k}$. But $(1-1)^k = 1 - k + \binom{k}{2} - \binom{k}{3} + \dots + (-1)^k\binom{k}{k}$. So the number of times x is counted is $1 - (1-1)^k = 1$ (for $k \ge 1$). $\square$

Proposition 5. Let R be an equivalence relation on X. Then the equivalence classes of R partition X.

Proof. Certainly, the equivalence classes have union X, since for any $x \in X$, we have $x \in [x]$. So, we need to check that they are non-empty and disjoint (when not equal).

Non-empty: For any $x \in X$, have $[x] \neq \emptyset$ as $x \in [x]$.

Disjoint: Given $[x] \cap [y] \neq \emptyset$, need $[x] = [y]$. Choose $z \in [x] \cap [y]$. Then zRx and zRy, so xRy (transitivity). So, for any w, $wRx \implies wRy$ and $wRy \implies wRx$. Thus $[x] = [y]$. $\square$

4 Countability

Proposition 1. X is countable $\iff$ $\exists$ injection $f : X \to N$.

Proof. If X is finite, it's trivial, so may assume X is infinite.

Left to right: bijective, so injective.

Right to left: have X bijects with $f(X)$, so enough to show that $f(X)$ is countable. Let $a_1 = \min f(X)$, $a_2 = \min(f(X)\backslash\{a_1\})$ and in general $a_n = \min(f(X)\backslash\{a_1, \ldots, a_{n-1}\})$. Then $f(X) = \{a_1, a_2, a_3, \ldots\}$. Each $k \in f(X)$ is hit, indeed $k = a_n$, some $1 \leq n \leq k$. □

Theorem 2. $\mathbb{N} \times \mathbb{N}$ is countable.

Proof 1. Define $a_1, a_2, \ldots$ by $a_1 = (1, 1)$, and if $a_n = (p, q)$ then $a_{n+1} = (p - 1, q + 1)$ if $p > 1$ or $(q + 1, 1)$ if $p = 1$. Then $\mathbb{N} \times \mathbb{N} = \{a_1, a_2, \ldots\}$ - each point is hit (induction on x and y). □

Proof 2. The function $f : \mathbb{N} \times \mathbb{N} \to \mathbb{N} : (x, y) \mapsto 2^x 3^y$ is an injection. □

Theorem 2′. Let $A_1, A_2, \ldots$ be countable, then $\bigcup_{n\in\mathbb{N}} A_n$ is countable. i.e. 'a countable union of countable sets is countable'.

Proof. Each A_n is countable, so can be listed as $a_{1n}, a_{2n}, a_{3n}, \ldots$ (it might terminate). Then define $f : \bigcup_{n\in\mathbb{N}} A_n \to \mathbb{N} : a_{ij} \mapsto 2^i 3^j$ (use the least such j if a_{ij} is repeated, as the A_j might not be disjoint). Then f is injective. □

Theorem 3. $\mathbb{R}$ is uncountable.

Proof. Will show that $(0, 1)$ is uncountable. Suppose not: have $(0, 1)$ listed as $r_1, r_2, r_3, \ldots$ where: $r_1 = 0.r_{11}r_{12}r_{13}\ldots$

$r_2 = 0.r_{21}r_{22}r_{23}\ldots$

$r_3 = 0.r_{31}r_{32}r_{33}\ldots$

$\vdots$

Construct $s = 0.s_1 s_2 \ldots$ such that $s_n = 5$ if $r_{nn} \neq 5$ and 6 if $r_{nn} = 5$. Then $\forall n : s \neq r_n$ (they differ in the nth place. This is a contradiction (s is not on the list). □

Theorem 4. $\mathcal{P}(\mathbb{N})$ is uncountable.

Proof. Suppose $\mathcal{P}(\mathbb{N})$ is listed as $S_1, S_2, S_3, \ldots$. Let $S = \{n \in \mathbb{N} : n \notin S_n\}$. Then $\forall n : S \neq S_n$. □

Theorem 5 (Schröder-Bernstein)**.** Let A, B be sets. If there exists an injection $f : A \to B$ and there exists an injection $g : B \to A$, then there exists a bijection from $A \to B$.

Proof. For $x \in A$, write $g^{-1}(x)$ for the unique $y \in B$ with $g(y) = x$ (if it exists). Similarly, have $f^{-1}(y)$ for $y \in B$.

For $x \in A$, the *ancestor sequence* of x is $g^{-1}(x), f^{-1}(g^{-1}(x)), g^{-1}(f^{-1}(g^{-1}(x))), \ldots$ (might terminate). Similarly for $y \in B$.

Now let $A_0 = \{x \in A : \text{ancestor sequence has even length}\}$

$A_1 = \{x \in A : \text{ancestor sequence has odd length}\}$

$A_\infty = \{x \in A : \text{ancestor sequence is infinite}\}$

Similarly, have B_0, B_1, B_∞. Note that f bijects A_0 with B_1. Indeed, $x \in A_0 \implies f(x) \in B_1$, and also if $y \in B_1$, then $y = f(x)$, some $x \in A$, so $x \in A_0$. Similarly, g bijects

B_0 with A_1. And f (for example) bijects A_∞ with B_∞. So, we have a bijection h defined such that:

$$h : A \to B : x \mapsto \begin{cases} f(x) & \text{if } x \in A_0 \\ g^{-1}(x) & \text{if } x \in A_1 \\ f(x) & \text{if } x \in A_\infty \end{cases}$$

$\square$