1. Equivalence of Sets

Two sets a and b are said to be *equivalent* if there is some bijection from a onto b. This is obviously an equivalence relation whose domain is the class of all sets. We write $a \approx b$ for equivalent sets a and b. Intuitively, the sets a and b are equivalent if they have the same number of elements. That a has not more elements than b can be formalized by defining: $a \leq_{in} b$ iff there is an injection from a to b; or quite similarly: $a \leq_{pr} b$ iff there is a surjection from b onto a. Both relations are quasi orders (i.e., reflexive and transitive relations) on the class of all sets. Clearly, $\emptyset \leq_{in} a$ for every set $a \neq \emptyset$. (The empty map is injective from $\emptyset$ to a and surjective from a to $\emptyset$) In the following we always assume that $a \neq \emptyset$.

Proposition 1. *Let $f : a \to b$ and $g : b \to a$ be maps. Assume that $g \circ f = id_a$. Then f is injective and g is surjective.*

Proposition 2. *Assume that $f : a \to b$ is injective. Then there is some map $g : b \to a$ such that $g \circ f = id_a$. That is, every injective map has at least one left inverse.*

Proposition 3 (AC)**.** *Assume that $g : b \to a$ is surjective. Then there is some map $f : a \to b$ such that $g \circ f = id_a$. That is, under the assumption of AC, every surjective map has at least one right inverse.*

The proofs are very easy. The map f for Proposition 3 is defined with the help of a choice function on $\mathcal{P}(b) \setminus \{\emptyset\}$ which picks for every $c \in a$ some element $d \in g^{-1}(a) = \{d | g(d) = a\}$.

Hence, $a \leq_{in} b$ always yields $a \leq_{pr} b$ but the converse needs the AC. Thus $a \leq_{in} b$ iff $a \leq_{pr} b$ holds under the assumption of the axiom of choice.

For every map $f : a \to b$ the *equivalence kernel*, or just the kernel, is defined by $c_1 \sim_f c_2$ iff $f(c_1) = f(c_2)$. This is an equivalence relation on the set a where the classes are the largest subsets of a on which the map f is constant. As usual, $a/\sim_f$ denotes the set of equivalence classes and $c \mapsto [c]$ is the *canonical projection* q_f . The map $[c] \mapsto f(c)$ then is the *canonical injection* $\dot{f}$.

Proposition 4. *Every map $f : a \to b$ decomposes into a surjection followed by an injection: $\dot{f} \circ q_f = f$.*

Theorem 5 (Cantor-Bernstein)**.** *$a \leq_{in} b$ and $b \leq_{in} a$ if and only if $a \approx b$.*

Proof. Let $f : a \to b$ and $g : b \to a$ be injections. We need to find a bijection from a to b. We call an element $c_0 \in a$ moving if it allows for an infinite diagram as in figure 1. That is, we can define two sequences $c_\nu = g(d_\nu)$ and $d_\nu = f(c_{\nu+1})$,

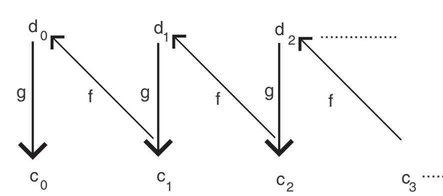

Figure 1. A moving element

$\nu \in \omega$, where c_ν has a (unique) counter image d_ν in b and where d_ν then has a (unique) counter image $c_{\nu+1}$ in a. We call an element $c \in a$ stationary if it is not moving. An element c is stationary if for a first ν we don't have a d_ν , i.e., c_ν is not in the range of the map g (c gets stopped in a) or we don't have a $c_{\nu+1}$, i.e., d_ν is not in the range of f (c gets stopped in b). Let a_1 be the subset of a consisting of all moving elements and the elements which are stopped in b; the set a_2 then is the complement of a_1, i.e., the set of all elements of a which are stopped in a. We define a map $h : a \to b$ by pieces. On a_1 an element c is mapped to d, where $g(d) = c$. This makes sense. If c is moving, then clearly $c \in ran(g)$. If c is not moving, then it got stopped in b, so again we must have that at least $c \in ran(g)$. On a_2 an element c is mapped to $f(c)$.
The map h is injective because f and g are injective, and $g(d_0) = c_0$ and $d_0 = f(c)$ for $c_0 \in a_1$ and $c \in a_2$ cannot happen. If c_0 is moving then $d_0 = f(c_1)$ for some $c_1 \in a_1$. If c_0 is stationary, it is stopped in b; hence again we conclude from $d_0 = f(c)$ that $c = c_1 \in a_1$.
Let $d \in b$. If $g(d)$ is moving, then $h(g(d)) = d$. If $g(d)$ is not moving and got stopped in b, then again $h(g(d)) = d$. If $g(d) = c$ got stopped in a, then we must have some c_1 in a such that $f(c_1) = d$, otherwise c would have been stopped at d in b. Clearly $c_1 \in a_2$ and $h(c_1) = d$. □

Corollary 6. *If $a \leq_{in} b \leq_{in} c$ and $a \approx c$ then $a \approx b$.*

Proof. We have $a \leq_{in} b$ and $b \leq_{in} c \approx a$, yields also $b \leq_{in} a$. The claim follows now from Cantor-Bernstein. □

Theorem 7 (Cantor)**.** *For any set a one has that $a <_{in} \mathcal{P}(a)$. That is $a \leq_{in} \mathcal{P}(a)$ but not $\mathcal{P}(a) \leq_{in} a$.*

Proof. We have that $c \mapsto \{c\}$ establishes an injective map from a into $\mathcal{P}(a)$. We need to show that there is no surjection from a to $\mathcal{P}(a)$. Let $h : a \to \mathcal{P}(a)$ be any map. The set $r = \{c | c \in a, c \notin h(c)\}$ then is not within the range of h: $h(c_0) = r$ yields the Russel Paradox $c_0 \in h(c_0)$ iff $c_0 \in r$ iff $c_0 \notin h(c_0)$. Hence h is not surjective. □

A set a is called *countable* if it is equivalent to ω. Infinite sets which are not countable are called uncountable. The set of all real numbers is an example of an uncountable set.

Let r be the set of real numbers and (a, b) and (c, d) any two (proper) open intervals. Then $(a, b) \approx (c, d)$ by means of a simple linear equation. Clearly $(-1, 1) \leq_{in} [-1, 1] \leq_{in} (-2, 2)$ and $(-1, 1) \approx (-2, 2)$ then yields $(-1, 1) \approx [-1, 1]$. *Hence any two proper intervals, whether open, closed or half-open, are equivalent.* The arctangent function maps r bijectively onto the open interval $(-\pi/2, \pi/2)$. *Hence r is equivalent to any of its proper intervals.* The function $1/x$ maps $(0, 1]$ to $[1, \infty)$ and, as before, any two improper intervals are equivalent. Thus r *is equivalent to any of its intervals.* On the other hand, with the help of the binary representation of real numbers, one easily establishes $[0, 1] \approx 2^\omega$.

Proposition 8. *The set r of real numbers, the continuum, is equivalent to the powerset of the set ω of natural numbers.* □

Proposition 9. *The set ω of natural numbers and the set q of rational numbers are equivalent.*

PROOF. We provide an enumeration of all positive rational numbers. Every positive rational number admits a unique representation in the form m/n where m and n are natural numbers which are relatively prime. For any natural number $k \geq 2$ there are only finitely many rational numbers $q = m/n$ where $n + m = k$. For $k = 2$ there is only one such fraction, namely $1 = 1/1$. For $k = 3$ we have two such numbers, namely $1/2$ and $2/1$. For $k = 4$ we have $1/3, 3/1$. For $k = 5$ we get $1/4, 2/3, 3/2, 4/1$.
This method leads to an enumeration of all rational numbers: $1, 1/2, 2 = 2/1, 1/3, 3 = 3/1, 1/4, 2/3, 3/2, 4 = 4/1, \ldots$ □

The proof actually showed

$$\omega \approx \omega \times \omega$$

It can be shown that the set r of real numbers is equivalent to $\mathcal{P}(\omega)$. Thus $\omega \leq_{in} r$, but ω and r are not equivalent.

The continuum hypothesis states that every subset s of the set r of real numbers is either equivalent to ω or to r. On the basis of the Zermelo Fraenkel axioms, this can neither be proven or disproven.

Problem 1. *An infinite subset s of ω is countable. (Hint: You may use the ordering of ω: $0 < 1 < \ldots$ and that every non-empty subset of ω has a smallest element.)*

Problem 2. *For any sets a and b, one defines a^b as the set of functions from b to a. That is*

$$a^b = \{f | f : b \to a\}$$

(1) *If a has n elements and b has m elements, what is the number of elements in a^b?*
(2) *Let a be any set. Establish an equivalence of the powerset $\mathcal{P}(a)$ of a and the set 2^a. (Hint: For any subset s of a define the characteristic function c_s as $c_s(x) = 1$ if $x \in s$, and $c_s(x) = 0$ if $x \notin s$. For every function $c : a \to 2$ define the support of s_c as $s_c = \{x | c(x) = 1\}$.)*
(3) *Explain how binary representation of numbers can be used to establish the equivalence of the set of real numbers and the powerset of natural numbers.*

Problem 3. (1) *Show that there is a function $f : [0, 1] \to [0, 1]$ such that for every $y \in [0, 1]$ one has exactly two elements $x_1, x_2 \in [0, 1]$ such that $f(x_1) = f(x_2) = y$.*
(2) *Any such function f of the previous problem cannot be continuous. This is a celebrated Intermediate Analysis exercise. (Hint: Use that every continuous function on a closed and bounded interval takes on a maximum and minimum, and use the intermediate value theorem for continuous functions which are defined on an interval.)*