Elements of Computability
Handout 2: Bijections, etc.

G.Bellin

January 25, 2004

Here you find more notions about bijections taken from P. M. Cohn, Algebra, vol. 1, John Wiley and Sons, Second Edintion. Also you find some facts about the cardinality of infinite sets which are essential for our course.

1 Properties of bijections.

Lemma. *Let $f : A \to B$ and $g : B \to A$. If $g \circ f = 1_A$, then f is injective and g is surjective.*

Proof. To see that f is injective, for $x, y \in A$ we have

$$\begin{aligned} f(x) = f(y) \quad &\Rightarrow \quad gf(x) = gf(y) \\ &\Rightarrow \quad 1_A(x) = 1_A(y) \\ &\Rightarrow \quad x = y \end{aligned}$$

To see that g is surjective, given $a \in A$ we have $g(f(a)) = a$, thus there is a $b \in B$, namely, $f(a)$, such that $g(b) = a$.

Theorem. *A function $f : A \to B$ is a bijection if there is a function $g : B \to A$ such that*

$$g \circ f = 1_A \qquad\qquad f \circ g = 1_b.$$

If f is a bijection then it is a surjection and so for every $b \in B$ there is $a \in A$ such that $f(a) = b$. Thus we can define $g : B \to A$ by setting $b \mapsto a$: this association does define a function, because f is injective and therefore to each $b \in B$ we can associate only one $a \in A$ in this way. Clearly $g(f(a)) = a$ and $f(g(b)) = b$.

Conversely, suppose f satisfies the two equations in the statement of the theorem: by the first equation f is injective and by the second surjective.

Theorem. (*Pigeon-hole principle.*) *If A is finite, then an injective function $f : A \to A$ is also surjective.*

Proof. Let $a \in A$, We write $f^n(a)$ for the application of f n times $f \ldots f(n) \ldots$. Since A is finite, for some n and k with $n > k$ we must have $f^n(a) = f^k(a)$. Since f is injective, $f^{n-1}(a) = f^{k-1}(a)$, $f^{n-2}(a) = f^{k-2}(a)$, ..., $f^{n-k}(a) = a$. So there is an element $a' \in A$, namely, $f^{n-k-1}(a)$ such that $f(a') = a$, hence f is surjective.

2 Cardinality.

What does it mean "to count"? Cantor's answer is by abstraction from the operation of establishing a bijection. It is easy to see that the relation

$$A \; R \; B \quad \text{iff} \quad \text{there is a bijection } f : A \to B$$

is an equivalence relation. Given a collection A. the equivalence class $[A] = \{B | A \; R \; B\}$ contains collections B having the same "number" of elements as A, or, as we say, the same *cardinality*. In this view, to count the elements of B is to put B in the equivalence class $[A]$ of a known collection A.

A set A is *finite* if there is a bijection $f : n \to A$. A set A is *countable* if either it is finite or there is a bijection $f : A \to \mathbf{N}$.

Fact. *The integers are countable:* the map $f : \mathbf{N} \to \mathbf{Z}$ given by

$$f(n) = n/2, \quad \text{if } n \text{ is even;} \qquad f(n) = -(n-1)/2, \quad \text{otherwise;}$$

is a bijection.

Fact. *The set of all pairs of natural numbers is countable:* the map

$$J(m, n) = \frac{(m+n)(m+n+1)}{2} + m$$

is a bijection $\mathbf{N} \times \mathbf{N} \to \mathbf{N}$ (including zero) (**Exercise**).

Fact. *The non-negative rationals are countable:* since the rationals are equivalence classes of fractions, i.e., of pairs of integers, the above map J does establish this fact, using the following Lemma, whose proof is left as an exercise.

Lemma. *Let ϕ be a partial function from the set* $\mathbf{N}$ *of natural numbers* onto *the set A. Show that either there is a bijection $f : n \to A$ where $n \in$* $\mathbf{N}$ *or there is a bijection $f :$* $\mathbf{N}$ *$\to A$. In other words, either A is finite or A has the same cardinality as* $\mathbf{N}$. (Exercise).

3 Induction

The *principle of mathematical induction* is the following property:

(I) *Let S be a subset of* $\mathbf{N}$ *such that* $1 \in S$ *and* $n+1 \in S$ *whenever* $n \in S$. *Then* $S = \mathbf{N}$.

It follows immediately from the characterization of $\mathbf{N}$ as the *smallest* inductive set: indeed by hypothesis $S \subseteq \mathbf{N}$ and S is inductive, hence $\mathbf{N} \subseteq S$.

Two other forms of induction are often used:

(I') *Let S be a subset of* $\mathbf{N}$ *such that* $1 \in S$ *and* $n \in S$ *whenever for all* $m < n$ *we have* $m \in S$. *Then* $S = \mathbf{N}$.

(I") *Every non-empty set of positive integers has a least element.*

These three principles are equivalent, see P. M. Cohn, *op. cit.* p. 24-25.

4 Integers and divisibility.

The basic theory of computability can be expressed entirely in terms of functions over the natural numbers $\mathbf{N}$. However, it is useful to consider $\mathbf{N}$ as a subset of the *integers* $\mathbf{Z}$ and exploit the properties of $\mathbf{Z}$ as a *totally ordered ring.* This means that we regard the set $\mathbf{Z}$ together with the operations of addition, subtraction, multiplication and the ordering "<", assuming only that they satisfy the following properties. For all x, y, z, we have

1. (*associativity of the sum and product*) $(x+y)+z = x+(y+z)$, $(xy)z = x(yz)$
2. (*commutativity of the sum and product*) $x+y = y+x$, $xy = yx$;
3. (*existence of neutral elements of sum and of product*) $x+0 = x$, $x1 = x$;
4. (*existence of additive inverse*) $x + (-x) = 0$;
5. (*distributive law*) $x(y+z) = xy + xz$;
6. (*no zero divisors*) if $x \neq 0 \neq y$ then $xy \neq 0$; $1 \neq 0$;
7. (*reflexivity*) $x \leq x$; (*transitivity*) if $x \leq y$ and $y \leq z$, then $x \leq z$; (*totality*) either $x \leq y$ or $x = y$ or $y \leq x$;
8. for all x_1, x_2, y_1, y_2, if $x_1 \leq x_2$ and $y_1 \leq y_2$, then $x_1 + y_1 \leq x_2 + y_2$;

9. if $x \leq y$ and $z \geq 0$ then $zx \leq zy$

To characterize the *integers* $\mathbf{Z}$ among all totally ordered rings we add the condition that the *positive integers* (which we may write as $\mathbf{N}^+$) are precisely the *natural numbers* (without zero): this is achieved by postulating that $\mathbf{N}^+$ satisfies the *Principle of Induction.*

4.1 Divisibility.

For $a, b \in \mathbf{Z}$, we say that *a is divisible by b* (and write $b|a$) if there exists $c \in \mathbf{Z}$ such that $bc = a$. (Notice that $0|a$ iff $a = 0$ and $a|0$ for all a in $\mathbf{Z}$). From the definition it is easy to prove the following facts about divisibility:

D.1 $c|b$ *and* $b|a$ *imply* $c|a$ (transitivity).

D.2 $a|a$ (reflexivity).

D.3 *If* $a|b$ *and* $b|a$ *then* $a = b$ *or* $a = -b$.

D.4 $b|a_1$ *and* $b|a_2$ *imply* $b|(a_1 - a_2)$.

D.5 $b|a$ *implies* $b|ac$ *for all* c.

A *prime number* is an integer p greater than 1 which can be divided only by 1 and by p itself. Please review the proofs of the *fundamental theorem of arithmetic* and of *Euclid's theorem* (*op. cit.* pp.28-29)

Theorem. *Every positive integer a can be written as a product of prime numbers*

$$a = p_1 p_2 \dots p_r$$

and this factorization is unique "modulo commutativity of multiplication".

Euclid's Theorem. *The number of prime numbers is infinite.* (Exercise.)

If $p_0[= 2]$, $p_1[= 3]$, ..., p_n, ... is an enumeration of all the primes in increasing order, then every positive integer can be written uniquely in the form

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n} \qquad (\alpha_i \geq 0, \alpha_n \neq 0)$$

Thus each positive integer a corresponds to one and only one sequence $(\alpha_1, \dots, \alpha_n)$ of non-negative integers. Since $p_i^0 = 1$, we may complete every sequence with infinitely many zeros; thun we obtain a *bijection* between the positive integers $\mathbf{N}^+$ and the set of all sequences of non-negative integers which have only finitely many non-zero elements.