CARDINAL ARITHMETIC 1

Recall that $A \cong B$ means that there is bijection from A to B, and that $A \lesssim B$ means that there is a injection from A to B or, equivalently, that $A \cong S$ for some subset $S \subset B$. (Proof of equivalence: any injective map from A to B is a bijection from A to a subset of B, and vice versa.)

Recall also that

(1) $A \lesssim B$ and $B \lesssim C$ imply that $A \lesssim C$,
(2) $A \lesssim A$,
(3) (Cantor-Bernstein Theorem). $A \lesssim B$ and $B \lesssim A$ imply that $A \cong B$.

Consider the following question: given two sets A and B, can we find sets A^* and $B^\dagger$ such that $A \cong A^*$, $B \cong B^\dagger$, and $A^* \cap B^\dagger = \emptyset$? The answer is "yes". There are many ways one can make such an A^* and $B^\dagger$. One simple and convenient way is to let $A^* = A \times \{0\}$ and $B^\dagger = B \times \{1\}$.

Definition. The **disjoint union** of A and B is $(A \times \{0\}) \cup (B \times \{1\})$.

The disjoint union of A and B is written $A \dot\cup B$, $A \amalg B$, or (occasionally) $A \oplus B$. I'll use $\oplus$ here to emphasize that disjoint union should be thought of as a kind of addition.

Theorem 1. *Let A and B be sets. Then*
(1) *$A \cup B \lesssim A \oplus B$, and*
(2) *If A and B are disjoint, then $A \cup B \cong A \oplus B$.*

Proof. Define a function $f : A \cup B \to A \oplus B$ by

$$f(x) = \begin{cases} (x \times \{0\}) & \text{if } x \in A, \\ (x \times \{1\}) & \text{if } x \in B \times A. \end{cases}$$

Then f is one-to-one (check!), so (1) is true. If A and B are disjoint, then f is a bijection, so (2) is true. □

Theorem 2. *Suppose $A \cong A'$ and $B \cong B'$. Then*
(1) *$A \oplus B \cong A' \oplus B'$.*
(2) *$A \times B \cong A' \times B'$.*
(3) *$\mathcal{P}(A) \cong \mathcal{P}(A')$.*
(4) *$A^B \cong (A')^{B'}$.*

Proof. By hypothesis, there exists injective maps $f : A \to A'$ and $g : B \to B'$. Then (as is easily checked) the map

$$h : A \times B \to A' \times B' \tag{1}$$

$$h(a, b) = (f(a), g(b)) \tag{2}$$

is a bijection from $A \times B$ to $A' \times B'$. This proves (2).

Define a map $\phi : A^B \to (A')^{B'}$ by $\phi(u) = f \circ u \circ g^{-1}$. Then (as is easily checked) ϕ is a bijection. This proves (4).

The proofs of (1) and (3) are similar and are left as exercises. □

In many ways, the set theoretic operations in $A \oplus B$, $A \times B$, and A^B behave like ordinary algebraic addition, multiplication, and exponentiation:

Theorem 3. *For any sets A, B, and C,*
(1) *$A \oplus B \cong B \oplus A$.*
(2) *$A \oplus (B \oplus C) \cong (A \oplus B) \oplus C$.*
(3) *$A \times B \cong B \times A$.*
(4) *$(A \times B) \times C \cong A \times (B \times C)$.*
(5) *$A \times (B \oplus C) \cong (A \times B) \oplus (A \times C)$.*
(6) *$A^{B \oplus C} \cong A^B \times A^C$.*
(7) *$(A^B)^C \cong A^{B \times C}$.*

Date: Feb 1, 2011.

One proves each statement by explicitly giving a bijection. For example, to prove (1), we define a map $\phi : A \oplus B \to B \oplus A$, i.e., a map $\phi : (A \times \{0\}) \cup (B \times \{1\}) \to (B \times \{0\}) \cup (A \times \{1\})$ by

$$\phi((x,0)) = (x,1) \text{ for } x \in A, \text{ and}$$
$$\phi((x,1)) = (x,0) \text{ for } x \in B.$$

It is easy to check that ϕ is a bijection, thus proving (1). Proofs of the other statements are similar and left as exercises.

The sets 0 (i.e, $\emptyset$) and 1 (i.e, $\{0\}$) behave here much as they do in ordinary arithmetic:

Theorem 4. *Let A be any set. Then*

(1) $A \oplus 0 \cong A$.
(2) $A \times 1 \cong A$.
(3) $A \times 0 = 0$.
(4) $1^A \cong 1$.
(5) $A^1 \cong A$.
(6) $A^0 \cong 1$.
(7) $0^A = 0$ *if* $A \neq \emptyset$.

Each of these statements is obviously true (and easy to prove) once you understand figure out what it's saying. For example, to prove (5), note that an element of A^1 is a function $u : 1 \to A$, i.e, a function $u : \{0\} \to A$. Of course u is completely determined by its value at 0. Thus the $u \mapsto u(0)$ gives a bijection from A^1 to A.

Next we state how disjoint unions, products, and set-theoretic exponentials behave with respect to <?:

Theorem 5. *Suppose $A \lesssim A'$ and $B \lesssim B'$. Then*

(1) $A \oplus B \lesssim A' \oplus B'$,
(2) $A \times B \lesssim A' \times B'$,
(3) $A^B \lesssim (A')^B$, *and*
(4) $A^B \lesssim A^{B'}$ *if* $A \neq \emptyset$.

Proof. By hypothesis, A is $\cong$ to some subset of A' and B is $\cong$ to some subset of B', so it suffices to prove the theorem assuming $A \subset A'$ and $B \subset B'$. But if $A \subset A'$ and $B \subset B'$, then $A \oplus B \subset A' \oplus B'$ and $A \times B \subset A' \times B'$. This proves (1) and (2).

To prove (3), note that $A^B \subset (A')^B$ since $A \subset A'$.

To prove (4), let $a \in A$. Given an element $u \in A^B$ (i.e, a function $u : B \to A$), define $\tilde{u} \in A^{B'}$ (that is, define a function $\tilde{u} : B' \to A$) by

$$\tilde{u}(x) = \begin{cases} u(x) & \text{if } x \in B, \text{ and} \\ a & \text{if } x \in B' \setminus B. \end{cases}$$

Then the map $u \mapsto \tilde{u}$ is a one-to-one map (check!) from A^B to $A^{B'}$. □

1. Sets Related to R

The set of real numbers was in the past often referred to as the "continuum". A set A such that $A \cong \mathbf{R}$ is said to "have the cardinality of the continuum".

Recall that $\mathbf{R} \cong 2^{\mathbf{N}} \cong \mathcal{P}(\mathbf{N})$. We can use the basic properties of cardinal arithmetic to prove that many other sets have the cardinality of the continuum.

Theorem 6. $\mathbf{R}^{\mathbf{N}} \cong \mathbf{R}$.

Cantor's colleagues were amazed by this. The set $\mathbf{R}^{\mathbf{N}}$ of infinite sequences of real numbers seems much bigger than the set of real numbers. But this theorem says that the two sets actually have the same size (i.e., cardinality).

Proof. $\mathbf{R} \cong 2^{\mathbf{N}}$ and $\mathbf{N} \times \mathbf{N} \cong \mathbf{N}$, so

$$\mathbf{R}^{\mathbf{N}} \cong (2^{\mathbf{N}})^{\mathbf{N}} \cong 2^{\mathbf{N} \times \mathbf{N}} \cong 2^{\mathbf{N}} \cong \mathbf{R}.$$

□

Corollary 7. $\mathbf{R}^n \cong \mathbf{R}$ *for every* $n \in \mathbf{N}$, $n \neq 0$.

Proof. Since $1 \lesssim n \lesssim \mathbf{N}$,

(*) $$\mathbf{R}^1 \lesssim \mathbf{R}^n \lesssim \mathbf{R}^{\mathbf{N}}$$

But $\mathbf{R}^1 \cong \mathbf{R}$ and $\mathbf{R}^{\mathbf{N}} \cong \mathbf{R}$, so by (*),

$$\mathbf{R} \lesssim \mathbf{R}^n \lesssim \mathbf{R},$$

so $\mathbf{R}^n \cong \mathbf{R}$ by the Cantor-Bernstein Theorem. □

Theorem 8. (1) *If* $1 \lesssim B \lesssim \mathbf{R}$, *then* $\mathbf{R} \times B \cong \mathbf{R}$.
(2) *If* $B \lesssim \mathbf{R}$, *then* $\mathbf{R} \oplus B \cong \mathbf{R}$.

Proof. If $1 \lesssim B \lesssim \mathbf{R}$, then

$$\mathbf{R} \cong \mathbf{R} \times 1 \lesssim \mathbf{R} \times B \lesssim \mathbf{R} \times \mathbf{R} \cong \mathbf{R}^2 \cong \mathbf{R}.$$

This (together with Cantor-Bernstein) proves (1).

If $B \lesssim \mathbf{R}$, then

$$\mathbf{R} \cong \mathbf{R} \oplus 0 \lesssim \mathbf{R} \oplus B \lesssim \mathbf{R} \oplus \mathbf{R} \cong \mathbf{R} \times 2 \cong \mathbf{R}$$

(the last $\cong$ is by part (1)), so (by Cantor-Bernstein) $\mathbf{R} \oplus B \cong \mathbf{R}$. □

[Remark: Why is $\mathbf{R} \oplus \mathbf{R} \cong \mathbf{R} \times 2$? In fact, you should check that for any set A, $A \oplus A$ and $A \times 2$ are actually equal, and not just equipotent.]

Theorem 9. *Let* C *be the set of continuous functions from* $\mathbf{R}$ *to* $\mathbf{R}$. *Then* $C \cong \mathbf{R}$.

Intuitively, C seems much bigger than $\mathbf{R}$, but in fact they have the same cardinality.

Proof. First we prove that $\mathbf{R} \lesssim C$. For each $a \in \mathbf{R}$, let $\phi(a)$ be the constant function from $\mathbf{R}$ to $\mathbf{R}$ that takes the constant value a. (That is, $\phi(a) = \mathbf{R} \times \{a\}$.) Then ϕ is a one-to-one map from $\mathbf{R}$ to C, so $\mathbf{R} \lesssim C$.

Next we prove that $C \lesssim \mathbf{R}$. Define a map $\psi : C \to \mathbf{R}^{\mathbf{Q}}$ as follows. If $f \in C$, then $\psi(f)$ is the restriction of f to $\mathbf{Q}$. I claim that ψ is one-to-one. To see that it is, suppose that $\psi(f) = \psi(g)$. Then (by definition of ψ)

(*) $$f(q) = g(q) \text{ for every } q \in \mathbf{Q}.$$

Now let x be any real number. Then there is a sequence q_i of rationals that converges to x. By (*),

(†) $$f(q_i) = g(q_i)$$

for every i. By continuity of f and of g, $f(q_i)$ converges to $f(x)$ and $g(q_i)$ converges to $g(x)$. Thus letting $i \to \infty$ in (†) gives $f(x) = g(x)$. Since this is true for all x, $f = g$. This completes the proof that ψ is one-to-one, and thus the proof that $C \lesssim \mathbf{R}$.

Since $\mathbf{R} \lesssim C$ and $C \lesssim \mathbf{R}$, in fact $C \cong \mathbf{R}$ by Cantor-Bernstein. □

2. Notation in the Text; Cardinal Numbers

In the text, most of the facts above are stated in a different notation, which I will now explain. The authors make the following assumption:

Assumption. *To each set A we can assign a set $|A|$ (called the cardinality of A) in such a way that $|A| \cong A$ and that $|A| = |B|$ if $A \cong B$.*

At the moment, we cannot prove that such an assignment is possible. (For that reason, I've avoided using the notation $|A|$.) Once we have the axiom of choice, we will be able to make such an assignment. It turns out the cardinality of any finite set is the number of elements in the set, and that the cardinality of any countable set is $\mathbf{N}$.

In general, a set κ is called a **cardinal number** (or simply a **cardinal**) if $\kappa = |A|$ for some set A. It is not hard to show that κ is a cardinal if and only if $|\kappa| = \kappa$. Note that the natural numbers are cardinal numbers, and that $\mathbf{N}$ is a cardinal number.

If, like the authors, we make the assumption above, then we can define arithmetic operations on cardinal numbers as follows:

Definition. Let κ and λ be cardinal numbers. Then

$$\kappa + \lambda = |\kappa \oplus \lambda|$$
$$\kappa \cdot \lambda = |\kappa \times \lambda|$$
$$\kappa^\lambda = |\{f : f \text{ is a function from } \lambda \text{ to } \kappa\}|.$$

The last part of the definition can be written more succinctly as

$$(*) \qquad \kappa^\lambda = |\kappa^\lambda|.$$

But κ^λ means different things on the left and the right. Ideally, we would have different symbols, one symbol to denote the set of functions from λ to κ (we might think of this as "set-theoretic exponentiation") and another symbol to denote the new operation ("cardinal exponentiation") on cardinal numbers we are defining. Thus to remove the ambiguity, we could rewrite (*) as

$$\kappa^\lambda(\text{cardinal exponentiation}) = |\kappa^\lambda(\text{set-theoretic exponentiation})|$$

But in general when we write A^B, we just state which kind of exponentiation we mean, unless it's clear from the context.

Using this new notation, we can restate theorems 3 and 4 as follows:

Theorem 10. *Suppose that κ, λ, and μ are cardinal numbers. Then*
(1) $\kappa + \lambda = \lambda + \kappa$,
(2) $\kappa + (\lambda + \mu) = (\kappa + \lambda) + \mu$,
(3) $\kappa \cdot \lambda = \lambda \cdot \kappa$,
(4) $\kappa(\lambda + \mu) = \kappa \cdot \lambda + \kappa \cdot \mu$,
(5) $\kappa^{\lambda+\mu} = \kappa^\lambda \cdot \kappa^\mu$,
(6) $(\kappa^\lambda)^\mu = \kappa^{\lambda\cdot\mu}$.
(7) $\kappa + 0 = \kappa$,
(8) $\kappa \cdot 0 = 0$,
(9) $\kappa \cdot 1 = \kappa$,
(10) $\kappa^0 = 1$,
(11) $0^\lambda = 1$ *if* $\lambda \neq 0$.

As mentioned above, natural numbers are cardinal numbers. Also $\mathbf{N}$ is cardinal number, but when we think of it as a cardinal number, it is usually denoted to $\aleph_0$. So when you see an expression like $\kappa^{\aleph_0}$ or $\aleph_0^\kappa$, you can assume that the author is using cardinal exponentiation.

Note that $|\mathbf{R}| = |\mathcal{P}(\mathbf{N})| = |2^{\mathbf{N}}| = 2^{\aleph_0}$, so $2^{\aleph_0}$ is the cardinal number of the continuum.

For finite numbers, the cardinal operations agree with the usual arithmetic ones. (This is easy to prove by induction.)

Here are some basic facts about arithmetic of $\aleph_0$ and $2^{\aleph_0}$:

Theorem 11. (1) *If $\kappa \leq \aleph_0$, then $\kappa + \aleph_0 = \aleph_0$.*
(2) *If $1 \leq \kappa \leq \aleph_0$, then $\kappa \cdot \aleph_0 = \aleph_0$.*
(3) *If $1 \leq n < \aleph_0$, then $\aleph_0^n = \aleph_0$.*
(4) *If $\kappa \leq 2^{\aleph_0}$, then $\kappa + 2^{\aleph_0} = 2^{\aleph_0}$.*

(5) *If* $1 \leq \kappa \leq 2^{\aleph_0}$, *then* $\kappa \cdot 2^{\aleph_0} = 2^{\aleph_0}$.

Proof. Statements (1), (2), and (3) are facts (or restatements of facts) about countable sets that we proved earlier. (For instance, (1) is the fact that the union of a countable set and an at most countable set is countable.)

Statements (4) and (5) are essentially restatements of theorem 8. □

We also have

Theorem 12.

$$(2^{\aleph_0})^n = m^{\aleph_0} = \aleph_0^{\aleph_0} = (2_0^{\aleph})^{\aleph_0} = 2^{\aleph_0}$$

for natural numbers $n > 0$ *and* $m > 1$.

Proof. Except for the statements about $m^{\aleph_0}$ and $\aleph_0^{\aleph_0}$, this is a restatement theorem 6 and corollary 7. But we give the whole proof since it is so short:

$$2^{\aleph_0} \leq m^{\aleph_0} \leq {\aleph_0}^{\aleph_0} \leq (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0}$$

so by Cantor-Bernstein these cardinal numbers are all equal. It remains to show that $(2^{\aleph_0})^n$ is equal to the other numbers in the list. Note that

$$2^{\aleph_0} = (2^{\aleph_0})^1 \leq (2^{\aleph_0})^n = 2^{\aleph_0 \cdot n} = 2^{\aleph_0},$$

so $(2^{\aleph_0})^n = 2^{\aleph_0}$ by Cantor-Bernstein. □