Transfinite cardinal arithmetic II

In this interlude between lectures 17 and 18 we shall prove the basic facts about adding and multiplying transfinite cardinal numbers.

Theorem (Idempotent laws for transfinite cardinals). *If A is an infinite set, then we have* $|A| + |A| = |A|$ *and* $|A| \cdot |A| = |A|$.

Corollary (Absorption law for transfinite cardinals). *If* **A** *and* **B** *are nonempty sets and at least one is infinite, then*

$$|A| + |B| = |A| \cdot |B| = |C|$$

where $|C|$ *is the larger of* $|A|$ *and* $|B|$.

The final portion of this statement relies on the fact that cardinal numbers are linearly ordered, which was established in Lecture 16. Of course, the corollary is almost always false if both A and B are finite.

PROOF THAT THE THEOREM IMPLIES THE COROLLARY. Without loss of generality, *we might as well assume that* $|A|$ *is the larger of the two cardinal numbers.* If we can prove the result in this case, the proof when $|B|$ is the larger will follow by interchanging the roles of A and B systematically throughout the argument. Such "without loss of generality" reductions are used frequently in mathematical proofs to simplify the discussion.

Since we are assuming $|A| \geq |B|$, we may combine the conclusion of the theorem with the basic formal properties of cardinal addition and multiplication to conclude that

$$|A| \leq |A| + |B| \leq |A| + |A| = |A|$$

so that $|A| + |B| = |A|$, and similarly

$$|A| \leq |A| \cdot |B| \leq |A| \cdot |A| = |A|$$

so that $|A| \cdot |B| = |A|$.■

PROOF OF THE THEOREM. We begin with the additive identity, both because it is simpler and because it is needed to prove the multiplicative identity. Both arguments are based upon Zorn's Lemma.

Proof that $|A| + |A| = |A|$. Let $\mathfrak{U}_A$ be the set of all pairs (B, f) where $B \subset A$ is a nonempty subset and $f : B \sqcup B \to B$ is a $1-1$ correspondence. If we set $(B, f) \leq (C, g)$ if and only if $g(b, n) = f(b, n)$ for $n = 1$ or 2, then routine calculations show that $\leq$ defines a partial ordering on $\mathfrak{U}_A$.

The set $\mathfrak{U}_A$ is nonempty because A contains a countably infinite subset C and we know that there is a bijection from $C \sqcup C$ to C.

Suppose now that we have a linearly ordered subset of $\mathfrak{U}_A$ whose elements have the form (B_t, f_t), where t lies in some indexing set. For each t let G_t denote the graph of f_t, let B be the union of the sets B_t, and let G be the union of the graphs G_t. We claim that G is the graph of a $1-1$ correspondence from $B \sqcup B$ to B. If so, then we have $(B, f) \geq (B_t, f_t)$ for all t and hence the hypotheses of Zorn's Lemma apply.

Suppose that $z \in B \sqcup B$, and choose t such that $z \in B_t \sqcup B_t$. Then there exists a unique $w \in B_t$ such that $(z, w) \in G_t$; we claim there are no other points in G with first coordinate equal to z. If $(z, x) \in G$, then there is some indexing variable s such that $(z, x) \in G_s$. Choose r so that G_r is the larger of G_s and G_t; then (z, w) and $(z, x) \in G_r$ imply $w = x$ because G_r is the graph of a function. Thus G is also the graph of a function. What is the domain of G? If $(z, w) \in G$, then $z \in B_t \sqcup B_t \subset B \sqcup B$ for some t, and conversely if $z \in B \sqcup B$ then for some t we have $z \in B_t \sqcup B_t$, so there is an ordered pair of the form $(z, w) \in G_t \subset G$.

Next, we need to show that the function f with graph G is a bijection. If $f(x) = f(y)$ then as before one can find a single set B_t such that $x, y \in B_t \sqcup B_t \subset B \sqcup B$ for some t, and conversely if $z \in B \sqcup B$ then for some t we have $z \in B_t \sqcup B_t$. Then we have

$$f_t(x) = f(x) = f(y) = f_t(y)$$

and since f_t is $1-1$ it follows that $x = y$. Also, given $z \in B$, choose t such that $z \in B_t$, so that $z = f_t(w) = f(w)$ for some w and hence f is onto. This completes the proof that linearly ordered subsets of $\mathfrak{U}_A$ have maximal elements.

By Zorn's Lemma there is a maximal element (M, h) of $\mathfrak{U}_A$, and by construction we have $|M| + |M| = |M|$. If $|M| = |A|$ then the proof is complete, so assume the cardinalities are unequal. Since M is a subset of A we must have $|M| < |A|$, and in fact by the rules of cardinal arithmetic it follows that $|A - M|$ must be infinite (if it were finite then we would have $|M| = |A|$). Let $C \subset M$ be a countably infinite set, let $h_0 : C \sqcup C \to C$ be a $1-1$ correspondence, and consider the map

$$k: (M \cup C) \sqcup (M \cup C) \to M \cup C$$

defined as the composite

$$(M \cup C) \sqcup (M \cup C) = (M \sqcup M) \cup (C \sqcup C) \to M \cup C$$

sending $x \in M \sqcup M$ to h(x) and $y \in C \sqcup C$ to $h_0(y)$. It follows immediately that the element $(M \sqcup C, k)$ is strictly greater than (M, h), contradicting the maximilaity of the latter. The problem arises from our assumption that $|M|$ and $|A|$ are unequal, and thus we have $|M| = |A|$ and we have proved the statement about $|A| + |A|$.■

Proof that **$|A| \cdot |A| = |A|$.** Let $\mathcal{V}_A$ be the set of all pairs (B, f) where $B \subset A$ is a nonempty subset and $f : B \times B \to B$ is a $1-1$ correspondence. If we set $(B, f) \leq (C, g)$ if and only if $g(b_1, b_2) = f(b_1, b_2)$ for all $b_1, b_2 \in B \times B$, then routine calculations show that $\leq$ defines a partial ordering on $\mathcal{V}_A$.

The set $\mathcal{V}_A$ is nonempty because A contains a countably infinite subset C, and we know that there is a $1-1$ correspondence from $C \times C$ to C.

Suppose now that we have a linearly ordered subset of $\mathcal{V}_A$ whose elements have the form (B_t, f_t), where t lies in some indexing set. The argument in the previous part of the proof extends to show that this linearly ordered set has an upper bound, whose graph is again the union of the graphs of the functions f_t. Therefore, once again Zorn's Lemma implies the existence of a maximal element (M, h) and once again the conclusion is true if $|M| = |A|$, so suppose the latter is false. It follows that we must have $|M| < |A|$. In this case, if we also have $|A - M| \leq |M|$ then

$$|A| = |M| + |A - M| \leq |M| + |M| = |M|$$

(by the additive identity shown in the first part of the theorem), and therefore we must also have $|M| < |A - M|$. In fact, repeated application of the first part of the theorem also implies that $|M| = 3|M|$ and consequently we also have $3|M| < |A - M|$.

The inequality $|M| < |A - M|$ implies the existence of a subset $N \subset A - M$ such that $|N| = |M|$, and in fact the equation $|M| = 3|M|$ implies that we may write N as a union of pairwise disjoint subsets N_1, N_2, N_3 which have the same cardinality as M and N. Define an extension of $h: M \times M \to M$ to

$$k: (M \cup N) \times (M \cup N) \to M \cup N$$

using the following breakdown by cases:

(1) On $M \times M$, k is given by h.

(2) On $M \times N$, k is given by the composite $M \times N \leftrightarrow N \times N \leftrightarrow M \times M \leftrightarrow M \leftrightarrow N_1$, where the $1 - 1$ correspondences are determined by the standard maps $M \leftrightarrow N$, $N \leftrightarrow N_1$, and $M \times M \leftrightarrow M$.

(3) On $N \times M$, k is given by the composite $N \times M \leftrightarrow N \times N \leftrightarrow M \times M \leftrightarrow M \leftrightarrow N_2$, where the $1 - 1$ correspondences are determined by the standard maps $M \leftrightarrow N$, $N \leftrightarrow N_2$, and $M \times M \leftrightarrow M$.

(4) On $N \times N$, k is given by $N \times N \leftrightarrow M \times M \leftrightarrow M \leftrightarrow N_3$, where the $1 - 1$ correspondences are determined by the standard maps $M \leftrightarrow N$, $N \leftrightarrow N_3$, and $M \times M \leftrightarrow M$.

By construction we again have $(M \cup N, k)$ is strictly greater than (M, h), contradicting the maximilaity of the latter. The problem arises from our assumption that $|M|$ and $|A|$ are unequal, and thus we have $|M| = |A|$ and we have shown the statement of the theorem about $|A| \cdot |A|$.■