SOME CARDINALITY QUESTIONS

PETE L. CLARK

1. On the existence of structures with given cardinality

In this section we address the question, "For which cardinals α does there exist a **Y** of cardinality α?" where Y is some sort of structure.

Example 1: X is a set. Tautologically there is, of course, a set of any given cardinality. For the sake of convenient reference, let X_α denote a given set of cardinality α (for instance, X could be the corresponding von Neumann cardinal).

Example 2: (Posets) It is obvious that there is a partially ordered set of any given cardinality, namely the totally disordered set with $x \leq y$ iff $x = y$. Assuming AC, we saw that there is a well-ordered set of any given cardinality.

Example 3 (Commutative rings): There exists a commutative ring R of any given cardinality α. If $\alpha = n$ is finite, we take $R = \mathbb{Z}/n\mathbb{Z}$. If α is infinite we have many choices, and in particular we can ensure that R is an integral domain, or a field. Consider $R_\alpha := \mathbb{Z}[\{T_i\}_{i \in X_\alpha}]$, the polynomial ring in a set of X_α commuting indeterminates. Indeed this is the union of the polynomial rings in any finite number of indeterminates. For any commutative ring R, the polynomial ring $R[T]$ has cardinality $\aleph_0 \times |R| = \max(|R|, \aleph_0)$, so $|R[T]| = |R|$ if R is infinite. By induction, exactly the same holds for polynomial rings in any finite number of indeterminates, and the polynomial ring in a set $\{X_\alpha\}$ of indeterminates of cardinality α has cardinality at most $|R|$ times the cardinality of all finite subsets of X_α, namely $|R| \times \alpha = \max(|R|, \alpha)$. On the other hand, it clearly has cardinality at least this large, so

$$|R[\{T_i\}_{i \in X_\alpha}]| = \max(|R|, \alpha).$$

In particular, taking $R = \mathbb{Z}$ and α to be any infinite cardinal, we find $|R_\alpha| = \alpha$. Moreover a polynomial ring $\mathbb{Z}_\alpha$ over $\mathbb{Z}$ in α indeterminates is a "versal" commutative ring of cardinality at most α: a commutative ring R has $|R| \leq \alpha \iff R$ is a homomorphic image of $\mathbb{Z}_\alpha$.

Example 4 (Fields): We assume known the fact for any $n \in \mathbb{Z}^+$ there exists a field of cardinality n iff $n = p^r$ is a prime power. On the other hand, for an integral domain R, let $Q(R)$ be its field of fractions. Then $|R| = |Q(R)|$. Indeed, if R is finite, then we have a stronger result: $Q(R) = R$, whereas if R is infinite we have $R \hookrightarrow Q(R)$ and $Q(R) \hookrightarrow R \times R$. Thus combining with Example 3, we get fields of any given infinite cardinality α, namely the field of rational functions in α indeterminates with $\mathbb{Q}$-coefficients.

Example 5 (F-vector spaces): Suppose F is a field. What are the possible cardinalities of F-vector spaces? Up to isomorphism, for every cardinal α, there exists a unique F-vector space of dimension α, say $\bigoplus_{i\in\alpha} F$. Recall that the infinite direct sum is the subgroup of the direct product consisting of tuples all but finitely many of which are zero, so that the cardinality of an α-dimensional F-vector space is equal to $|F|^\alpha$ if F and α are finite, and otherwise $\max(\alpha, |F|)$. In particular, if $F = \mathbb{F}_q$ is finite, then the possible cardinalities of F-vector spaces are all finite numbers q^r ($r \geq 1$) and all infinite cardinals. If F is infinite, there exists an F-vector space of cardinality α iff $\alpha \geq |F|$. In particular, every infinite cardinal is the cardinality of a $\mathbb{Q}$-vector space.

Example 6 (Algebraically Closed Fields): No finite field is algebraically closed (since if $|F| = q$, then every element of F is a root of $T^q - T$, so no element of F is a root of $T^q - T + 1$). Recall that any field F has an algebraic closure $\overline{F}$ (that is, an algebraically closed field which is an algebraic extension over F). The construction of $\overline{F}$ requires Zorn's Lemma: let $\{F_i/F\}$ be the set of all algebraic field extensions of F. To be precise, for each F-algebra isomorphism class of algebraic extensions, we must choose a single representative. We now define a partial ordering on the set, in which $F_i \leq F_j$ if there exists an F-algebra embedding $F_i \hookrightarrow F_j$. (Note that it is incorrect to say that this is inclusion: in general there will be multiple embeddings and there is no distinguished one.) Given any chain in the poset, we take the "union" (more precisely, the direct limit) over all the elements of the chain; this gives an algebraic field extension. So Zorn's Lemma entitles us to a maximal algebraic extension, which is easily seen to be algebraically closed.

Note that if F is finite, $|\overline{F}| = \aleph_0$ (since $\overline{F}$ is a direct limit of countably many finite field extensions of F), and if F is infinite, $|\overline{F}| = |F|$, since we can take the direct limit over all finite extensions F_i of F, each of which is a finite-dimensional F-vector space so has cardinality equal to the cardinality of F, and the number of such finite extensions is at most the number of elements of $F[X]$, i.e., $|F|$. This shows that there exists an algebraically closed field of any infinite cardinality.

Example 7 (nonabelian groups): Of course it follows from Example 3 that there exists a group of any given cardinality α: just take the additive group of the integral domain. Note that these groups are all commutative. One can also ask for nonabelian groups. The issue of which finite n there exists a nonabelian group of order n involves too much group theory to enter into here (but there is a known answer to this). For every infinite cardinal α there exists a nonabelian group of cardinality α, namely the free group on a generating set of cardinality α.

Example 8 (simple groups): Like the case of fields, there are cardinality restrictions on a finite simple group. Moreover the additive group of the finite field $\mathbb{F}_p$ is a (not very exciting) finite simple group, and a moment's thought reveals that these are the only abelian simple groups, finite or otherwise. At this early stage the classification of finite simple groups parts company with the classification of finite fields – for any $i > 1$ there most certainly is *not* a finite simple group of cardinality p^i – and of course the classificiation of finite simple groups, while now complete, is many orders of magnitude more difficult. On the other hand, for any infinite cardinal α there is a finite simple group of cardinality α. For instance, one can take a field F of cardinality α and then a classical matrix group over F, e.g. $PSL_n(F)$ for $n \geq 2$: it is easy to see that if F is infinite, $|PSL_n(F)| = |F|$. (Note that for $n \geq 3$ these also yield finite simple groups, and also for $n = 2$ unless $\#F \leq 3$, but of course not all finite simple groups arise this way.)

Example 9 (topological spaces): For any cardinal α, of course there exists a topological space of cardinality α, namely the discrete topology on α. This discrete space is locally compact, but not compact unless α is finite. Moreover there exists a compact[1] space of every cardinality α: in the infinite case, we may take the one-point compactification X_α^+ of X_α, namely X_α with an extra point ∞ adjoined, so that the open neighborhoods of ∞ are those with finite complement.

Note that X_α^+ is not homogeneous, i.e., the automorphism group does not act transitively. Indeed it is not possible to endow a countably infinite set, say, $\mathbb{Z}^+$ with a homogeneous compact topology. For homogeneity implies that either every point is isolated (i.e., $\mathbb{Z}^+$ is discrete and infinite hence noncompact) or no point is isolated, in which case we could apply the Baire category theorem (which is valid for compact spaces as well as complete metrizable spaces) to deduce its uncountability. In particular we cannot endow a countable set with the structure of a compact topological group.

Example 10 (Polish spaces): By definition a Polish space is a complete metric space with a countable basis (or equivalently, given the metrizability, a countable dense subset). Using the discrete metric, a finite or countable set becomes a Polish space. The real line is, of course, a Polish space of continuum type. However, it can be shown that any uncountable Polish space is of continuum type. (Any separable metric space has cardinality at most that of the continuum. What is more delicate is that, even if the continuum hypothesis is denied, nevertheless there is no Polish space X with $\aleph_0 < |X| < c$.) In particular, the underlying topological space of a product of α Polish spaces (each consisting of at least two points) is itself "Polishable" iff α is at most countable.

[1]Following Bourbaki, a compact space is by definition a quasicompact Hausdorff space.