1.3 Cardinals

Cardinals capture the idea of amount (*five* apples, *seven* oranges,...).

To compare amounts we go back to the following preschool mathematics idea: We are given a picture of kids and apples and want to know whether there are as many apples as kids, but we have not yet learned to count (which pretty much corresponds to our situation before we have cardinal numbers). To solve the problem we try pairing up the apples with the kids and see if it is possible to do so without any being left over of either sort (see Figure).

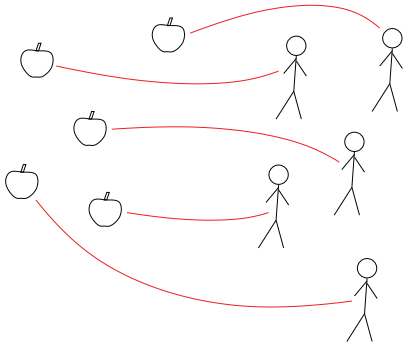

Figure 1: There are as many apples as kids, and we can see this without knowing how many they are.

Using this as our basic idea we define:

Definition 1.17. 1. A set A is *equinumerous* to a set B (written $A \approx B$) if there is a one-to-one function from A onto B.

2. A set A is *dominated* by a set B (written $A \preccurlyeq B$) if there is a one-to-one function from A *into* B.

3. $A \prec B$ means $A \preccurlyeq B$ but not $A \approx B$.

It is easy to see that $\approx$ is an equivalence relation. Not all sets are equinumerous, though:

Theorem 1.18 (Cantor's theorem)**.** *No set is equinumerous to its power set.*

Proof. Exercise, based on the following remark. □

Remark 1.19. Note that the power set $\mathcal{P}(X)$ of a set X is equinumerous to the set of functions $f : X \to 2$.

This is because any subset of X can be coded by its characteristic function and vice versa any function $f : X \to 2$ can be interpreted as the characteristic function of the set $\{x \in X : f(x) = 1\}$.

As for $\preccurlyeq$, it is easy to see that it is reflexive and transitive. One can also (without assuming the axiom of choice) prove that $\preccurlyeq$ is antisymmetric:

Theorem 1.20 (Schröder-Bernstein Theorem)**.** *If $A \preccurlyeq B$ and $B \preccurlyeq A$, then $A \approx B$.*

Proof. Assume $A \preccurlyeq B$ and $B \preccurlyeq A$. Then by definition there are one-to-one functions $f : A \to B$ and $G : B \to A$. Define inductively for each $n \in \mathbb{N}$ sets C_n by

$$\begin{aligned} C_0 &= A \setminus \operatorname{ran}(g) \\ C_{n+1} &= g[f[C_n]], \end{aligned}$$

where $f[X]$ denotes the image of X under f. We then define a function $h : A \to B$ by

$$h(x) = \begin{cases} f(x) & \text{if } x \in C_n \text{ for some } n, \\ g^{-1}(x) & \text{otherwise.} \end{cases}$$

Note that in the second case $x \notin C_0$, so $x \in \operatorname{ran}(g)$ and h is well defined (g was one-to-one).

We then show that h is one-to-one. Define $D_n = f[C_n]$ so that $C_{n+1} = g[D_n]$. Since f and g^{-1} are both one-to-one, problems can only arise when, say, $x \in C_m$ and $x' \notin \bigcup_{n\in\omega} C_n$. In this case $h(x) = f(x) \in D_n$ but $h(x') = g^{-1}(x') \notin D_n$. So $h(x) \neq h(x')$.

It only remains to show that h is onto. Clearly each $D_n \subseteq \operatorname{ran}(h)$, since $D_n = h[C_n]$. So let $y \in B \setminus \bigcup_{n<\omega} D_n$ and consider the element $g(y)$. Now $g(y)$ cannot be in C_0 and neither in any C_{n+1}. So $h(g(y)) = g^{-1}(g(y)) = y$ and we are done. □

So $\preccurlyeq$ is a partial order, but we would of course like it to be total (i.e., be able to compare the size of any sets). This, however, requires us to assume the axiom of choice. The classical form of this axiom states the existence of a choice function:

AC 1 (Choice function)**.** If X is a collection of nonempty sets, there is a function f whose domain is X and which satisfies $f(x) \in x$ for each $x \in X$.

The forms most useful for induction are the well-ordering and enumeration principles.

AC 2 (Well-ordering principle)**.** For any set A, there exists a well ordering on A.

AC 3 (Enumeration principle)**.** Any set is equinumerous to some ordinal number.

Outside logic the most common form is Zorn's lemma.

AC 4 (Zorn's Lemma)**.** Let X be a nonempty partially ordered set, such that each chain in X has an upper bound in X. Then X has a maximal element.

We leave to the reader the proof that all these forms are equivalent.

Assuming the axiom of choice, one can well-order any set. By lemma 1.14 we then have a bijection between an ordinal and the set and can define the size of the set via the ordinals:

Definition 1.21. For any set A the *cardinality* of A is the least ordinal equinumerous to A, i.e., $|A| = \min\{\alpha \in \mathrm{Ord} : \alpha \approx A\}$.

Note that a set may be equinumerous to several ordinals (using different orderings on the set), but given such a set we can of course pick out the least.

Definition 1.22. A *cardinal number* is an ordinal that is not equinumerous to any of its predecessors. Equivalently, a cardinal number is an ordinal that is its own cardinality. Such ordinals are also called *initial ordinals*.

Being able to enumerate sets, we can use transfinite induction on any sets:

Example 1.23. Every vector space has a basis.

Proof. Let V be a vector space over some field F. Using the enumeration principle we can write V as $V = \{v_\alpha : \alpha < \kappa\}$, for some cardinal κ. Then let

$$B = \{v_\alpha : v_\alpha \notin \mathrm{Span}\{v_\beta : \beta < \alpha\}, \alpha < \kappa\},$$

where $\mathrm{Span}(A)$ denotes the linear span of A, i.e. $\mathrm{Span}(A) = \{a_0 v_0 + \cdots + a_{n-1} v_{n-1} : n < \omega, a_i \in F, v_i \in A\}$ and $\mathrm{Span}(\emptyset) = \{0_V\}$ (this is to make sure that the linear span of a set is the intersection of all subspaces containing the set; the empty linear combination is defined to be 0_V).

It remains to show that B is a basis for V. To show this, let $V_\alpha = \mathrm{Span}(\{v_\beta : \beta < \alpha\})$ and $B_\alpha = B \cap \{v_\beta : \beta < \alpha\}$. We show by induction that B_α is a basis for V_α for every $\alpha < \kappa$.

- if $\alpha = 0$, then $B_\alpha = \emptyset$ and $V_\alpha = \{0_V\}$, so B_α spans V_α (via the empty linear combination) and is linearly independent (as there are no vectors in it such that a linear combination with non-zero coefficients would yield 0).

- if $\alpha = \beta + 1$ for some β, and B_β is a basis for V_β, then by definition of B,

  $$v_\beta \in B_{\beta+1} \text{ if and only if } v_\beta \notin V_\beta.$$

  Now, if $v_\beta \in V_\beta$, $V_{\beta+1} = V_\beta$ and $B_{\beta+1} = B_\beta$ is a basis of $V_{\beta+1}$. If $v_\beta \notin V_\beta$, then $B_{\beta+1} = B_\beta \cup \{v_\beta\}$. Now this spans $V_{\beta+1}$: any element of $V_{\beta+1}$ can be written as a linear combination of vectors v_γ, $\gamma < \beta$ and v_β. But since B_β spans V_β all v_γ, $\gamma < \beta$ can be written as linear combinations of elements of B_β. So any element can be written as a linear combination of elements of B_β and v_β, i.e., elements of $B_{\beta+1}$. To show linear independence, let $a_0 v_{i_0} + \cdots + a_{n-1} v_{i_{n-1}} = 0$, with $a_i \in F$, $v_{i_k} \in B_{\beta+1}$. If $v_{i_k} \in B_\beta$, all coefficients must be zero, as B_β is linearly independent. If one of the vectors is v_β and its coefficient is non-zero, then there must be other vectors with non-zero coefficient, as $v_\beta \neq 0$ (because $v_\beta \notin V_\beta$). But then v_β can be written as a linear combination of elements of B_β, a contradiction. So $B_{\beta+1}$ must be linearly independent.

- If α is a limit, let $B_\alpha = \bigcup_{\beta<\alpha} B_\beta$. Note that $V_\alpha = \bigcup_{\beta<\alpha} V_\beta$, as any linear combination of vectors v_γ, $\gamma < \alpha$, already appears in some V_β. Thus B_α spans V_α. For linear independence, note that all vectors in a given linear combination appear already in some B_β, so independence follows from linear independence of the B_β's.

□

In addition to being rather intuitive, transfinite induction is also convenient, when one needs to keep track of sizes during the induction. For this we will first need some cardinal arithmetic.

Definition 1.24. Let κ, λ be cardinals.

1. $\kappa + \lambda := |K \cup L|$, where K and L are any disjoint sets with $|K| = \kappa$ and $|L| = \lambda$.
2. $\kappa \cdot \lambda := |K \times L|$, where K and L are any sets with $|K| = \kappa$ and $|L| = \lambda$.
3. $\kappa^\lambda := |{}^L K|$, where K and L are any sets with $|K| = \kappa$ and $|L| = \lambda$ and ${}^L K = \{f : L \to K \mid f \text{ is a function}\}$.

It is an easy exercise to show that these notions are well-defined, i.e., independent of the choice of sets K and L. Also, they satisfy natural properties:

Lemma 1.25. *For any cardinal numbers κ, λ, μ:*

1. $\kappa + 0 = \kappa$ *and* $\kappa \times 0 = 0$,
2. $\kappa \times 1 = \kappa$,
3. $\kappa^{\lambda+\mu} = \kappa^\lambda \cdot \kappa^\mu$,
4. $(\kappa \cdot \lambda)^\mu = \kappa^\mu \cdot \lambda^\mu$,
5. $(\kappa^\lambda)^\mu = \kappa^{\lambda \cdot \mu}$.

Proof. Exercise. □

Remark 1.26. Note also, that by Remark 1.19, $|\mathcal{P}(X)| = 2^{|X|}$.

Lemma 1.27. *For any cardinal numbers* κ, λ, μ*:*

1. *If* $\kappa \leq \lambda$ *then* $\kappa + \mu \leq \lambda + \mu$.
2. *If* $\kappa \leq \lambda$ *then* $\kappa \cdot \mu \leq \lambda \cdot \mu$.
3. *If* $\kappa \leq \lambda$ *then* $\kappa^\mu \leq \lambda^\mu$.
4. *If* $0 < \kappa \leq \lambda$ *then* $\mu^\kappa \leq \mu^\lambda$.

Proof. Exercise. □

Theorem 1.28. *If* κ *is an infinite cardinal, then* $\kappa \cdot \kappa = \kappa$.

Proof. The proof is by transfinite induction. So assume κ is an infinite cardinal and for all $\alpha < \kappa$ holds, that 'if α is an infinite cardinal, then $\alpha \cdot \alpha = \alpha$'. Then for each $\alpha < \kappa$ we have $|\alpha| \cdot |\alpha| < \kappa$ (if $\kappa = \omega$, use induction on the natural numbers to show that for all $m, n < \omega$, $, \ldots n < \omega$).

Define a well-order $\lhd$ on $\kappa \times \kappa$ by $(\alpha, \beta) \lhd (\gamma, \delta)$ iff

$$\begin{gathered} \max\{\alpha, \beta\} < \max\{\gamma, \delta\} \text{ or} \\ (\max\{\alpha, \beta\} = \max\{\gamma, \delta\} \text{ and } (\alpha, \beta) <_{lex} (\gamma, \delta)) \end{gathered}$$

where $<_{lex}$ is the lexicographic order. It is straightforward to show that $\lhd$ is a well-order (since both $(\kappa, \in)$ and the lexicographic order are). Further, each pair (α, β) has at most $|\max\{\alpha, \beta\} + 1 \times \max\{\alpha, \beta\} + 1| < \kappa$ predecessors in $\lhd$, so $(\kappa \times \kappa, \lhd)$ is isomorphic to an ordinal $\leq \kappa$, showing $|\kappa \times \kappa| \leq \kappa$. Since clearly $\kappa \leq |\kappa \times \kappa|$, we have $|\kappa \times \kappa| = \kappa$. This completes the induction step, so the claim holds for all infinite cardinals. □

Corollary 1.29. *For any infinite cardinals* κ *and* λ, $\kappa + \lambda = \kappa \cdot \lambda = \max\{\kappa, \lambda\}$.

Proof. W.l.o.g. assume $\kappa \leq \lambda$. Then this is seen using Theorem 1.28 and Lemma 1.27 and noting:

$$\lambda = 0 + \lambda \leq \kappa + \lambda \leq \lambda + \lambda = 2 \cdot \lambda \leq \lambda \cdot \lambda = \lambda$$

and

$$\lambda = 1 \cdot \lambda \leq \kappa \cdot \lambda \leq \lambda \cdot \lambda = \lambda.$$

By the Schröder-Bernstein theorem we are done. □

Definition 1.30. By ${}^{<\alpha}X$ we denote the set $\bigcup_{\beta<\alpha} {}^{\beta}X$. Then $X^{<\alpha} := |{}^{<\alpha}X|$.

Corollary 1.31. *For any infinite cardinal κ, $|kappa^{<\omega}| = \kappa$.*

Proof. By induction on n and using Theorem 1.28, one can prove that $\kappa^n = \kappa$. So there are injective functions $f_n : \kappa^n \to \kappa$. Using these define the map $f : \bigcup_{n<\omega} \kappa^n \to \omega \times \kappa$ by $f(g) = (n, f_n(g))$, when $g \in \kappa^n$. f is clearly injective, so $|\kappa^{<\omega}| \leq \omega \cdot \kappa = \kappa$. □

Having cardinal arithmetic we have access to more technical inductions:

Example 1.32. There exists a subset of the plane $\mathbb{R}^2$ that intersects every line exactly twice.

Proof. Denote by $\mathfrak{c}$ the size of the continuum $\mathfrak{c} = |\mathbb{R}|$. At this point all we need to know of $\mathfrak{c}$ is that it is an uncountable cardinal (follows from Cantor's theorem).

Also note that there are $\mathfrak{c}$ many lines in the plane (as the number of lines is $\geq \mathfrak{c}$ and $\leq \mathfrak{c}^2 = \mathfrak{c}$). So we can enumerate the set of lines

$$\mathcal{L} = \{L : L \text{ is a line in } \mathbb{R}^2\} = \{L_\alpha : \alpha < \mathfrak{c}\}.$$

We will construct the desired set inductively. So assume we have constructed sets $X_\beta \subset \mathbb{R}^2$ for all $\beta < \alpha$ satisfying:

- for all $\gamma \leq \beta$, $|L_\gamma \cap X_\beta| = 2$,
- for all $L \in \mathcal{L}$, $|L \cap X_\beta| \leq 2$,
- for $\gamma < \delta \leq \beta$, $X_\gamma \subseteq X_\delta$,
- $|X_\beta| \leq |\beta| + \omega = \max\{|\beta|, \omega\}$.

Now let $Y_\alpha = \bigcup_{\beta<\alpha} X_\beta$ and note that:

- for all $\gamma < \alpha$, $|L_\gamma \cap Y_\alpha| = 2$,

- for all $L \in \mathcal{L}$, $|L \cap Y_\alpha| \leq 2$,
- for $\beta < \alpha$, $X_\beta \subseteq Y_\alpha$,
- $|Y_\alpha| \leq |\alpha| \cdot (|\alpha| + \omega) = |\alpha| + \omega$.

So we only need to take care of intersecting L_α exactly twice. If $|Y_\alpha \cap L_\alpha| = 2$, let $X_\alpha = Y_\alpha$. Otherwise look at the set of lines through two points in Y_α. There are at most $|\alpha| + \omega < \mathfrak{c}$ such lines and each intersects L_α at most once. Thus there are infinitely many points on L_α that do not belong to any of these lines and we can add one or two of those to Y_α to get X_α intersecting L_α exactly twice. The size does not increase. □

It is crucial in the induction to know that the size of X_β is bounded below $\mathfrak{c}$ and not just smaller than $\mathfrak{c}$. We will look closer at why below.

Definition 1.33. The *successor* of a cardinal α, denoted α^+, is the least cardinal greater than α. A cardinal α is said to be a *limit cardinal* if it is not the successor of a cardinal.

The alephs[1] are defined by transfinite recursion:

Definition 1.34. 1. $\aleph_0 = \omega$,

2. $\aleph_{\beta+1} = (\aleph_\beta)^+$,
3. for α a limit, $\aleph_\alpha = \sup\{\aleph_\beta : \beta < \alpha\}$.

Lemma 1.35. *1. Each $\aleph_\beta$ is a cardinal.*

2. Every infinite cardinal is equal to some $\aleph_\beta$.

3. If $\alpha < \beta$, then $\aleph_\alpha < \aleph_\beta$.

4. $\aleph_\alpha$ is a limit cardinal if and only if α is a limit ordinal. $\aleph_\alpha$ is a successor cardinal if and only if α is a successor ordinal.

Proof. Exercise. □

Now we can see that although the union of κ many subsets of size κ has size κ, the same isn't true if we replace 'κ' by 'less than κ': Look at

$$\bigcup_{n<\omega} \aleph_n = \sup\{\aleph_n : n < \omega\} = \aleph_\omega.$$

Here $\aleph_\omega$ is written as a union of ω (i.e., $< \aleph_\omega$) sets of size $< \aleph_\omega$. Not all infinite cardinals have this property, though, but only the singular ones, defined below.

[1] Aleph, $\aleph$, is the first letter in the Hebrew alphabet

Definition 1.36. Let $f : \alpha \to \beta$ be a function. It is said to map α *cofinally* into β if $\mathrm{ran}(f)$ is unbounded in β.

Definition 1.37. The *cofinality of* β, $\mathrm{cf}(\beta)$, is the least α such that there is a map from α cofinally into β.

Note that clearly $\mathrm{cf}(\beta) \leq \beta$.

Definition 1.38. A cardinal κ is *regular* if $\mathrm{cf}(\kappa) = \kappa$. A cardinal is *singular* if it is not regular.

Now singular cardinals can be written as 'unions of fewer smaller sets', which is the reason for the warning after example 1.32. So is $\mathfrak{c}$ singular? The peculiar situation is that we don't know. In fact, we know we cannot know, since this is independent of the axioms of set theory (ZFC or similar) (however, $\mathfrak{c}$ cannot be $\aleph_\omega$, since $\mathrm{cf}(\mathfrak{c}) > \omega$).

Definition 1.39 (Continuun Hypothesis, CH)**.** The Continuum Hypothesis is the statement $2^\omega = \aleph_1$. The Generalized Continuum Hypothesis, GCH, is the statement 'for all α, $2^{\aleph_\alpha} = \aleph_{\alpha+1}$'.