Well-orderings, ordinals and well-founded relations.

An ancient principle of arithmetic, that *if there is a non-negative integer with some property then there is a least such,* is useful in two ways: as a source of proofs, which are then said to be "by induction" and as as a source of definitions, then said to be "by recursion."

An early use of induction is in Euclid's proof that every integer $\geqslant 2$ is a product of primes, (where we take "prime" to mean "having no divisors other than itself and 1"): if some number is not, then let $\bar{n}$ be the least counter-example. If not itself prime, it can be written as a product $m_1 m_2$ of two strictly smaller numbers each $\geqslant 2$; but then each of those is a product of primes, by the minimality of $\bar{n}$; putting those two products together expresses $\bar{n}$ as a product of primes. Contradiction !

An example of definition by recursion: we set $0! = 1; (n+1)! = n! \times (n+1)$. A function defined for all non-negative integers is thereby uniquely specified; in detail, we consider an *attempt* to be a function, defined on a finite initial segment of the non-negative integers, which agrees with the given definition as far as it goes; if some integer is not in the domain of any attempt, there will be a least such; it cannot be 0; if it is $n+1$, the recursion equation tells us how to extend an attempt defined at n to one defined at $n+1$. So no such failure exists; we check that if f and g are two attempts and both $f(n)$ and $g(n)$ are defined, then $f(n) = g(n)$, by considering the least n where that might fail, and again reaching a contradiction; and so, there being no disagreement between any two attempts, the union of all attempts will be a well-defined function, which is familiar to us as the factorial function.

So far, only the natural numbers have been needed for indexing the stages of an iterative process. Cantor discovered that there are phenomena which go further, leading him to the concept of a *well-ordering*: a linear ordering for which every non-empty subset has a least element. Every natural number is either 0 or a successor, $n+1$; but in longer well-orderings there will be *limit points*, which have predecessors but no largest one.

Some properties of well-orderings and ordinals. No well-ordering can be order-isomorphic to a strict initial segment of itself; for suppose to the contrary that $(A, <_A)$ is a non-empty well-ordering, that $a \in A$ and that $F : A \longrightarrow \{x \in A \mid x <_A a\}$ is order-preserving, and therefore injective. Then $a >_A F(a)$, so $F(a) >_A F(F(a)), \ldots$; and so the set $\{a, F(a), F^2(a), \ldots\}$ will form a non-empty subset of A with no minimal element.

On the other hand, given two well-orderings, $(A, <_A)$, $(B, <_B)$, one is order-isomorphic to an initial segment of the other: in short, any two well-orderings are comparable.

In fact, working within Zermelo-Fraenkel set theory, von Neumann identified a certain class of well-orderings, called the class of ordinals, with the useful property that every well-ordering is isomorphic to exactly one ordinal; and, further, given any two ordinals one *is* actually an initial segment of the other, and not just isomorphic to one.

If η is an ordinal, there is an immediate successor, $\eta \dotplus 1$ so that every ordinal ξ is either $\leqslant \eta$ or $\geqslant \eta \dotplus 1$; every set A of ordinals has a least upper bound, $\sup A$; every non-empty set B of ordinals has a least member, $\inf B$.

The natural numbers $\mathbb{N}$, may be identified with the finite ordinals; if A is the empty set, $\varnothing$, $\sup A = 0$; on the other hand $\sup \mathbb{N}$ will be the smallest limit ordinal, which is called ω. The ordinals continue: $\omega \dotplus 1$, $(\omega \dotplus 1) \dotplus 1$; in fact the sum $\eta + \xi$ of two ordinals is easily defined by recursion on the second variable:

$$\eta + 0 = \eta; \quad \eta + (\zeta \dotplus 1) = (\eta + \zeta) \dotplus 1; \quad \eta + \lambda = \sup_{\nu < \lambda} (\eta + \nu) \text{ for limit } \lambda$$

so the next limit ordinal will be $\omega + \omega$. Since this definition makes $\eta \dotplus 1 = \eta + 1$, we may henceforth write $+1$ instead of $\dotplus 1$.

An example of the use of ordinals to index an iterative process whose length is not known at the outset. Suppose that $\langle X, <_X\rangle$ is a countable linear ordering. We shall define, by recursion on ν, a series of equivalence relations, $\sim_\nu$, on X, with the property that $x <_X y <_X z \;\&\; x \sim_\nu z \implies x \sim_\nu y$, so that each equivalence class, $[x]_\nu$ is a convex subset of X, so that the ordering $<_X$ naturally induces a linear ordering of the set $X/{\sim_\nu}$ of $\sim_\nu$-equivalence classes.

The first definition is easy: $x \sim_0 y \iff_{\mathrm{df}} x = y$, so $[x]_0 = \{x\}$.

Given $\sim_\nu$, the next equivalence relation will be defined by

$$x \sim_{\nu+1} y \iff_{\mathrm{df}} \text{ there are only finitely many } \sim_\nu \text{ classes between } [x]_\nu \text{ and } [y]_\nu.$$

Thus $x \sim_\nu y \implies x \sim_{\nu+1} y$, and so the equivalence classes are nested.

For a limit ordinal λ, we define $x \sim_\lambda y$ to hold if for some $\nu < \lambda$, $x \sim_\nu y$; so

$$[x]_\lambda = \bigcup_{\nu<\lambda} [x]_\nu.$$

Now, (with some care, if we wish not to use the Axiom of Choice), we may show that there will be some countable ordinal, η say, for which $\sim_\eta \,=\, \sim_{\eta+1}$; at that point, either all points in X have become $\sim_\eta$-equivalent—in which case the original set is said to be *scattered*; or else the set of $\sim_\eta$-classes is infinite and densely ordered, like the rationals though possibly with end-points—in which case by choosing one point in each $\sim_\eta$-class we obtain an order-preserving embedding of $\mathbb{Q}$ into the original ordered set X.

For example, applied to the rationals $\mathbb{Q}$ with their usual ordering, the process stops at stage 0; applied to $\mathbb{Z}$, it stops at stage 1. Applied to the set of rationals $\{1, 2, 3\} \cup \{1 + \frac{1}{n} \mid n = 1, 2, \ldots\} \cup \{3 - \frac{1}{n} \mid n = 1, 2, \ldots\}$, $[1]_0 = [1]_1 = \{1\}$, $[3]_0 = [3]_1 = \{3\}$, but $1 \sim_2 2 \sim_2 3$, so the process stops at stage 2.

This analysis yields a useful description of all scattered countable linear orderings.

How many countable ordinals are there ? Any one countable linear ordering will only need countably many countable ordinals to index the above process; but given a countable ordinal θ, we may design a countable linear ordering such that the above process stops at stage θ. Thus to cover all cases, we shall need all the countable ordinals; so naturally we ask how many there are.

We can get an upper bound by considering those relations on $\mathbb{N}$ which are well-orderings. The class of such relations will be a set W, being a subclass of the set of all subsets of $\mathbb{N} \times \mathbb{N}$; each such relation is isomorphic to a countable ordinal and hence the collection of ordinals isomorphic to members of W will be a set, using the axiom of replacement; hence the class of countable ordinals is a set. But given the properties mentioned above, it will itself be a well-ordering and thus isomorphic to an ordinal, which is called ω_1. Every countable ordinal is isomorphic to an initial segment of ω_1, and given the way the ordinals are nested, any strict initial segment of ω_1 will be some countable ordinal; but ω_1 itself cannot be countable, for if it were, $\omega_1 + 1$ would also be a countable ordinal; but as we have seen, $\omega_1 + 1$ cannot be isomorphic to an initial segment of ω_1. Putting our remarks together, we see that ω_1 is the first uncountable ordinal, and the set of countable ordinals is uncountable.

Well-founded relations. A binary relation R on a set X is *well-founded* if every non-empty subset of X has an R-minimal element. The well-founded relations on X are those for which there is a mapping ϖ_R of X into the class of ordinals such that for all x and y in X with xRy, $\varpi(x) < \varpi(y)$. Further, in Zermelo-Fraenkel set theory, an ordinal-valued rank function ϱ is definable for all sets, such that $y \in x \implies \varrho(y) < \varrho(x)$. Indeed ϱ satisfies the following equation for all x:

$$\varrho(x) = \sup\{\varrho(y) + 1 \mid y \in x\}$$

and the above equation may be regarded as defining ϱ by recursion on the membership relation $\in$, which in Zermelo Fraenkel set theory is indeed well-founded.

A well-ordering may be thought of as a well-founded relation which is also a linear ordering, but it is the well-foundedness that enables definitions and proofs by recursion to be carried out, not the linearity, which is merely a simplifying influence.

For example, if one thinks of the well-formed formulæ of a formal language, the sub-formula relation is well-founded but not linear; it is easy to find two formulæ neither a sub-formula of the other; but proofs of properties of a formal system often proceed by induction on the sub-formula relation.

Codes for Borel sets. The above idea of recursion on a well-founded relation illuminates the concept of a *Borel set*, which is of pivotal importance in the study of measure and probability. The collection of Borel subsets of $\mathbb{R}$ is often defined to be the smallest family containing the open intervals with rational end-points and closed under taking complements and countable unions: but that definition comes adrift in a certain model of set theory in which the Axiom of Choice fails very badly, and indeed, in that model, that smallest family contains every set of reals.

A better definition may be given by introducing the idea of a *Borel code*, which is a countable well-founded labelled tree. Think of it as a root system, starting from a unique top point, growing downwards and branching as it goes, but with no infinite descending paths. Each of the bottom points bears a label on which is written the name of some rational open interval, such as $(\frac{1}{3}, \frac{2}{3})$. To determine whether a point p is in the set coded by the tree, start at the bottom points and see which of the rational intervals named there contain the point; then work upwards using the labels, which tell you to take unions or take complements, to track the membership of p in the sets defined at the intermediate stages; and see whether p is stated to be "in" when the computation reaches the unique top point of the tree.

The computation for a given p is done by recursion on the tree, and is uniquely determined by p; so p will be in the coded set if some computation respecting at every stage the information contained in the tree says that it is, or, equivalently, if every such computation says that it is.

Then one defines a *Borel set* to be the set described by some Borel code. A weak form of the Axiom of Choice is needed to prove that the collection of Borel sets is closed under countable union: for a set with a code will actually have many different codes, and therefore to build a Borel code for the union $\bigcup_i B_i$ of Borel sets B_i, one must start by choosing a code for each B_i.

Borel codes were developed by Solovay for his celebrated paper on the measure problem; he defines the set $BC_{\mathcal{X}}$ of Borel codes for any topological space $\mathcal{X}$ with a countable basis $(\mathcal{O}_i)_{i\in\mathbb{N}}$ of open sets as being generated by these rules:

$$\langle 0, i\rangle \text{ codes } \mathcal{O}_i;$$
$$\langle 1,\, s\rangle \text{ codes } \mathcal{X} \setminus B \text{ if } s \text{ codes } B;$$
$$\text{if } h : \mathbb{N} \to BC_{\mathcal{X}} \text{ and } \forall n \in \mathbb{N}\ h(n) \text{ codes } A_n \text{ then } \langle 2,\, h\rangle \text{ codes } \bigcup_{n\in\mathbb{N}} A_n.$$

Analytic and co-analytic sets. Lebesgue made a famous (and as he later happily acknowledged, highly fruitful) mistake in 1905, when he said that if B is a Borel subset of the plane $\mathbb{R}^2$, its projection onto the line $\mathbb{R}^1$ will also be Borel. The error was detected a decade later by Suslin, a young member of the Moscow group of set theorists led by Lusin, and led to the discovery and study of the class of *analytic sets*. They are indeed the projections of Borel subsets of the plane, but the class can be defined in other interesting ways which make the link with well-orderings much more evident. For example, let S be a closed subset of $\mathbb{R} \times \mathbb{Q}$: for $r \in \mathbb{R}$, let $S_r = \{q \in \mathbb{Q} | (r,\, q) \in S\}$, so that S_r will be a set of rationals; and write $<_r^{\mathbb{Q}}$ for the restriction of the usual ordering of the rationals to S_r.

Then the set $\{r \in \mathbb{R} \mid (S_r, <_r^{\mathbb{Q}})$ is not a well-ordering$\}$ is analytic, and every analytic set of reals is of this form for some S as above. Put very abstractly, the criterion for membership of a given analytic set is that the tree of finite partial stages in the construction of a witness to some statement be ill-founded, so that such a witness, which typically will be an infinite sequence of integers, does in fact exist.

A *co-analytic set* is the complement of an analytic set. It is easily seen, using Borel codes, that every Borel set is both analytic and co-analytic; a landmark result of Suslin is the converse, that a set which is both analytic and co-analytic is Borel, and a definition of analytic sets in terms of well-orderings is central to that proof.

An analytic set which is not Borel. Indeed, well-orderings have proved crucial in *descriptive set theory*, which is the study of definable sets of reals; it transpires that a more convenient setting than $\mathbb{R}$ is *Baire space* $\{\alpha \mid \alpha : \mathbb{N} \longrightarrow \mathbb{N}\}$, often called $\mathcal{N}$. We use this setting for our example.

Let $\mathfrak{s} : \mathcal{N} \longrightarrow \mathcal{N}$ be the shift function defined by $\mathfrak{s}(\alpha)(n) = \alpha(n+1)$. We iterate this function according to the definition $\mathfrak{s}^0(\alpha) = \alpha$, $\mathfrak{s}^{k+1}(\alpha) = \mathfrak{s}(\mathfrak{s}^k(\alpha))$.

For α and β in $\mathcal{N}$ we say that α *attacks* β, written $\alpha \curvearrowright_{\mathfrak{s}} \beta$, if β is an accumulation point of the sequence $\{\mathfrak{s}^k(\alpha) \mid k = 0, 1, 2, \ldots\}$ of successive images of α by the shift function. A *recurrent* point is a point that attacks itself. Then the set $\{\alpha \in \mathcal{N} \mid \exists \rho \; \alpha \curvearrowright_{\mathfrak{s}} \rho \curvearrowright_{\mathfrak{s}} \rho\}$ of points in $\mathcal{N}$ that attack at least one recurrent point is analytic but not Borel.

The proof of that fact, which we do not give, depends on determining the well-foundedness or otherwise of certain trees having a point of $\mathcal{N}$ at each node, chosen so that each point in the tree attacks those points above it in the tree. So ordinals and well-foundedness are embedded in the discussion of concepts arising in symbolic dynamics.

The Axiom of Choice is equivalent to the *Well-Ordering Principle* that every set can be wellordered. But how easily definable is, say, a well-ordering of the continuum ? It is known to be impossible that an analytic subset of the plane should be the graph of such a well-ordering; and to be consistent that the continuum is well-orderable but that no such well-ordering is definable even allowing as parameters in the definition finitely many ordinals and finitely many real numbers. On the other hand it is known to be consistent that the continuum has a well-ordering whose graph is the continuous image of a co-analytic set. So well-orderings of uncountable sets of reals are hard to come by; if one exists, then by a celebrated theorem of Shelah, for which Raisonnier has given a simpler proof, there is a set of reals which is not Lebesgue measurable.

Conclusion. In this brief *tour d'horizon* we have seen that Cantor's discovery of well-orderings has led to substantial insights into constructions in many parts of mathematics. Well-orderings and well-founded relations can be expected to be present, even if only in the background, whenever there is a sense that an ongoing computation, though possibly a very abstract one, is involved. Strange attractors, for instance, are analytic sets, and analytic sets are highly computational objects.

For further reading:

the classic *Abstract Set Theory* by A. A. Fraenkel has an excellent introduction to the concept of a well-ordering;

for a modern introduction to the work of Lusin, his school and their successors, I suggest *Classical Descriptive Set Theory* by A. S. Kechris.

A. R. D. Mathias