Nilpotent[*]

Graeme Taylor

March 16, 2003

> *When an expression raised to the square or any higher power vanishes, it may be called nilpotent; but when, raised to a square or higher power, it gives itself as the result, it may be called idempotent*[1]

To be mathematically vague, an object is nilpotent if some power of it 'is' zero. Clearly, such vagueness won't do, but can only be cleared up by a mathematical framework within which objects, powers and zero all have meaning. For the non-mathematician, a friendly environment might be the integers. Then zero is a very familiar concept, and power has its 'usual' meaning of repeated multiplication. So, a nilpotent integer is one which when multiplied together a magical number of times (its order of nilpotency) becomes zero.

With a little thought it becomes clear that the only such integer is zero itself- all the others grow in magnitude during the multiplication process, so cannot end up at zero. How exotic, then, does the mathematics have to become before the nilpotent definition becomes interesting? There are many mathematical playgrounds out there within which nilpotency is meaningful, and I'm certainly no master of them all. So we'll settle for a tour of a couple of the more accessible (for, at least, an undergraduate) areas in which interesting behaviour can be found.

Nilpotency in Modular mathematics

We observed that the problem with the integers was that multiplication always made things bigger (in absolute value- for a negative integer it would alternate between positive and negative values, but those continue to get further from zero at each step). So a solution might be to throw in numbers which, when multiplied by, give smaller results: values less than 1, such as fractions. (That is, we can start working in $\mathbb{Q}$, the set of rational numbers). This turns out not to help- whilst $(\frac{1}{2})^{n+1}$ is half the size of $(\frac{1}{2})^n$, there is still no value k such that $(\frac{1}{2})^k$ is zero. That is, it approaches

[*] First appeared on Everything2, at *http://www.everything2.com/index.pl?node_id=1442774*

[1] from "Linear Associative Algebra", Benjamin Peirce, 1870. Source: Earliest Known Uses of Some of the Words of Mathematics - *http://members.aol.com/jeff570/mathword.html.*

but never attains its limit. So adding in more numbers to play with wasn't useful in getting an integer-like playground with non-zero nilpotent values.

Instead, therefore, we'll throw most of the integers away. A structure that allows this is modular mathematics- where all calculations are done modulo some value n- meaning that n is identified with zero, and at any intermediate step of a calculation, multiples of n can be safely discarded. Those with more than a passing interest in cryptography will probably have come across it; otherwise, you may have encountered it as ”clock arithmetic”- where you add and multiply on a clock face, resetting to zero every time you reach 12 (so 17:00 hours is $17 - 12 = 5$ o'clock in the afternoon).

Why can this give nilpotent elements? Well, some experimentation will show that working in the integers modulo n (an algebraic structure known as a ring; although choosing a prime number for n gives a ”better” structure, a field) multiplication will wrap around and so can give smaller values. For instance, working modulo 7, we can start taking multiples of two: $2 \times 2 = 4$, $2 \times 2 \times 2 = 8 = 8 - 7 = 1$ which is less than two. Two then locks into this pattern $(2 \rightarrow 4 \rightarrow 1 \rightarrow 2)$ so isn't nilpotent. But any multiple of 7 is trivially nilpotent, as $7^1 = 7 = 7 - 7 = 0$. Can we get rings where values other than n and its multiples are 0? That's possible too, if we pick an n which is some power of a number. As an example, two is nilpotent in the integers modulo 8, since $2^3 = 8 = 8 - 8 = 0$ in that setting.

What's happened here is that we've made the definition of nilpotent go further by giving ourselves more zeros to play with. Before moving on to break the power bit instead of the zero bit, I'll take a quick detour into some related algebra for those more versed in the notions and notation. Feel free to skip this bit.

A ring is said to be reduced if it has no nilpotent operators: that is, there exists no non-zero f and natural m such that $f^m = 0$. If the ring R is of the form $R = k[X_1, ..., X_n]/I$ for some ideal I, then R is reduced if and only if I is a radical ideal (that is, I is its own radical). In particular, $k[V]$, the co-ordinate ring, is reduced for any affine variety V.

Nilpotent Operators

A mathematical operator/function/map is a rule which takes values in a space and assigns to them values in a new space. If the operation actually always assigns a value from the original space, then it makes sense to think of applying the function multiple times. So if $T : V \rightarrow V$ is a map such that $v \rightarrow f(v)$ for all v in V, then we can think of the map $T^2 : V \rightarrow V$ as being $v \rightarrow f(f(v))$. In this way, we can build up T^n for any natural number n. If we take maps as our objects, and this layering process as our 'power', then we are in a position to think about nilpotent operators. (The natural candidate for a 'zero' here is the zero map, which cheerfully sends anything you throw at it to zero.)

In analysis, as ariels[2] observes, the nilpotent operators on finite dimensional spaces V reduce dimension. Since infinite dimensional functional analysis is not something I easily grasp, we'll ignore that (even though other interesting things can apparently happen) and restrict our attention to finite dimension (which can be arbitrarily large if you're feeling cheated!).

A structure theorem for nilpotent operators

f $\beta : W \to W$ is a nilpotent operator, then there is a basis $w_1 ... w_n$ of W for which $\beta(w_i)$ is either w_{i-1} or 0; and in particular $\beta(w_1)$ is zero.

Proof of the above was considered beyond the scope of my undergrad studies, but the complication arises in showing that all nilpotent operators can be considered in this form. Clearly, any operator with this structure will be nilpotent. If this isn't obvious because the terminology is meaningless to you, here's what that part of the theorem is saying. Any object in our space can be built up using some but not necessarily all of a collection of building blocks (the basis $w_1 ... w_n$). So the input to β and its output can both be thought of as such a sum. Let's simplify further, and suppose that we're working in the familiar three dimensions and have a basis w_1, w_2, w_3. We start with a point t, which we write as $aw_1 + bw_2 + cw_3$ for some constants. When we apply β we get an answer out which by our rule simply erases some coefficients and shifts others. For instance, for the rule $w_3 \to w_2 \to w_1 \to 0$ the result is $bw_1 + cw_2$. Note that this is of only 2 dimensions compared to the three of the point t. Applying β to that object gives us cw_1. A final application erases our last coefficient and takes us to zero: β was nilpotent of order 3.

[2] An everything2 user, *http://www.everything2.com/index.pl?node=ariels*