Cubes in Fields

PETER FREYD
pjf@upenn.edu

September 26, 2019

I have an awful proof of the following:

In any field, any sum of four cubes is a sum of just three cubes.

That is, the first-order axioms for fields imply the first-order consequence:

$$\forall_{a,b,c,d}\ \exists_{x,y,z}\ \ a^3+b^3+c^3+d^3 = x^3+y^3+z^3$$

By "awful proof," I mean a correct proof but one that's quite awful.

It is an immediate corollary of:

In any field at least one of the following two alternatives must hold:

1) Every element is a sum of three cubes;

2) The sum of any two cubes is a cube.

That is:

$$\left[\forall_a\ \exists_{x,y,z}\ \ a = x^3+y^3+z^3\right]\ \ \vee\ \ \left[\forall_{a,b}\ \exists_x\ \ a^3+b^3 = x^3\right]$$

This, in turn, is an immediate consequence of an even-better result:

For any field at least one of the following three alternatives must hold:

1) Every element in the field is a sum of three cubes;

2) The field is of characteristic = 3;

3) The field has exactly four elements.

(In the last two alternatives, cubes are closed under addition: in the characteristic = 3 case we have, of course, $x^3+y^3 = (x+y)^3$; and the only cubes in the field with four elements are 0,1, which—should a formula be demanded—implies $x^3+y^3 = (x^3+y^3)^3$.)

The awful proof rests on the following polynomial identity that holds in any commutative unital ring:

$$x\left(3^2x^2y^7+3^4xy^4+3^6y\right)^3 \;=\; \left(x^3y^9-3^6\right)^3+\left(-x^3y^9+3^5xy^3+3^6\right)^3+\left(3^3x^2y^6+3^5xy^3\right)^3$$

Given x, if we can find a value for y such that $3^2x^2y^7+3^4xy^4+3^6y \neq 0$ then we may divide both sides by its cube to obtain a representation of x as a sum of three cubes. In any field of characteristic other than 3 there can be at most 7 values for y for which $3^2x^2y^7+3^4xy^4+3^6y = 0$, hence if any such field has more than 7 elements we know that every element is a sum of three cubes. Direct inspection suffices for fields of order $2, 5$ and 7. [1]

Can anyone find a nice proof? And are there similar theorems for larger powers?

As bad as this proof is, there is, alas, an even worse one. I'll get to it below. The origin of both proofs is this one-variable polynomial identity:

$$x\left(3^2x^2+3^4x+3^6\right)^3 \quad = \quad \left(x^3-3^6\right)^3+\left(-x^3+3^5x+3^6\right)^3+\left(x^2+3^4x\right)^3$$

To obtain the two-variable version simply replace x with xy^3.

I was first aware of this one-variable identity from Yuri Manin's book on cubic forms.[2] He uses it to give an "unenlightening" proof that every rational number is a sum of three rationals cubed (he dates the proof to 1825).

Several weeks after first seeing Manin's book it occurred to me that the mere writing of an equal sign between polynomials was not, in fact, a proof.

It is a fond position of mine that mathematical proofs exist only in their performance—what is written is akin to a score thereof. (Necessarily, then, when one says he can prove that there is an elementary proof of the non-existence of 16 dimensional division algebra over the algebraic reals he is using the word "proof" in two different ways.) An experienced prover can imagine performing a proof while reading the score and—just as is the case for an experienced musician—the imagining only whets the appetite: he will want to perform the proof.

But note that even without saying that proofs exist in their performance, the mere assertion of a polynomial identity certainly fails to constitute an actual proof. So one day—it must have been a very strange mood that day—I sat myself down with paper and pencil to see if I could, in fact, perform a proof of the identity.

And it would not verify.

There were too many places that a careless arithmetic error could destroy the verification. The date was in the early 80s. If there were good symbolic-program packages, I didn't know of their existence. (Would a machine verification really constitute a proof? Well, certainly not in the strongest sense. But it would, at least, constitute very good evidence of the truth of the assertion.) I did have a newly acquired programmable pocket calculator by Hewlett-Packard. It would suffice to show that

$$x\left(3^2x^2+3^4x+3^6\right)^3-\left(x^3-3^6\right)^3-\left(-x^3+3^5x+3^6\right)^3-\left(x^2+3^4x\right)^3$$

evaluates to zero for 10 different integral values for x. That I could do with my calculator. And I could program it so that it would detect numerical overflow. So that I did.

And the identity failed. (You don't need a calculator: it fails even modulo 3; even for $x = 1$.)

You must forgive me. I pulled a switch here. The polynomial identity in Manin's book was not actually the one that dates to 1825. It had an error (not present in the two-variable

[1] The fields of order 4 and 7 are the only finite fields in which it is not the case that every element is a sum of *two* cubes. A proof appears below in Appendix 2.

[2] Manin, Yu. I. *Cubic forms: algebra, geometry, arithmetic.* Translated from Russian by M. Hazewinkel. North-Holland Mathematical Library, Vol. 4. North-Holland Publishing Co., Amsterdam-London; American Elsevier Publishing Co., New York, 1974.

polynomial at the opening of this paper). I corrected for the “awful proof” but faithfully copied the error in the above one-variable polynomial expressions.

Assuming that the error was a single misprint, my little pocket calculator could find just where the misprint was. And, presto, it didn’t take long to determine that the values of

$$x\left(3^2x^2+3^4x+3^6\right)^3-\left(x^3-3^6\right)^3-\left(-x^3+3^5x+3^6\right)^3$$

were integers cubed for integral values of x. Taking the cube roots and doing a little curve-fitting quickly yielded the correct identity. (There were actually two wrong numbers—as can be observed from the correct two-variable equation and the incorrect one-variable equation—but fortunately they were in the same clause.)[3]

There was the wonderful possibility that these errors had been perpetrated for over 150 years. After checking with the translator that he had not introduced the errors, I wrote to Manin and he traced them to his first notes on the subject—no one had actually performed the proof in decades. Even mod 3. Even $x = 1$.

Before we get to the even-worse proof let me pause to improve the “even-better result” by inserting a bunch of *skew*s:

For any skew-field at least one of the following three alternatives must hold:

1) Every element in the skew-field is a sum of three cubes;

2) The skew-field is of characteristic = 3;

3) The skew-field has exactly four elements.

The proof is mostly just a hitchhike on what we already have. Suppose that x is an element of a skew-field of characteristic other than 3. Let C be its center and $C(x)$ the sub-skew-field generated by C and x. If $C(x)$, which is, of course, commutative, has other than 4 elements we’re done. For the case that it has exactly 4 elements it suffices, obviously, to find any larger commutative sub-ring. If there is no such sub-ring, finish with:

If R is a unital ring without non-zero nilpotents, if K is maximal among its commutative unital sub-rings and if K has exactly four elements, then $R = K$.

(The hypothesis, of course, is much weaker than what we are given.) Since $(1+1)^2 = 4 = 0$ the absence of nilpotents forces K, hence all of R, to be of characteristic 2. Let $a \in K$ be other than 0 or 1. The fourth element is necessarily $a + 1$. We know that $a^2 \neq 0$. If $a^2 = 1$ then $(a+1)^2 = 0$ and the absence of nilpotents would force $a = 1$. Hence $a^2 = a + c$ where c is either 0 or 1 and in either case c is central. Define a function $f : R \to R$ by $f(x) = x+ax+xa$. Then $af(x) = ax+(a+c)x+axa = cx+axa$ and similarly $f(x)a = xc+axa$, that is, the values of f commute with a, hence lie in K. Moreover $f|K$ is the identity function hence f is an idempotent transformation of the additive group structure of R with K as its image. What we need to prove, therefore, is that f is the identity function and for that it suffices to show that its kernel is trivial (the only monomorphic idempotent is the identity function). Accordingly let x be such that $f(x) = 0$. We may rewrite that as $ax = x(a+1)$ and $(a+1)x = xa$. Hence $axx = x(a+1)x = xxa$ forcing $x^2 \in K$. There are only four possibilities for x^2. If $x^2 = 1$ then $(x+1)^2 = 0$ forcing $x \in K$. If $x^2 = a + c$ for c either 0 or 1 then x and $a+c$ clearly commute,

[3] In this day, of course, everyone has access to symbolic programs. Paste

```
x*(9*x^2+81*x+729)^3-(x^3-729)^3-(-x^3+243*x+729)^3-(27*x^2+243*x)^3
```

into the box on the top of `http://www.numberempire.com/simplifyexpression.php`
(Test the work by changing any integer, for example, by tacking `.0000000000001` onto its end).

again forcing $x \in K$. The fourth possibility, that $x^2 = 0$, also forces $x \in K$ (no non-trivial nilpotents). But $\operatorname{Ker}(f) \cap \operatorname{Image}(f) = \{0\}$ for any idempotent.[4]

Now for the even-worse proof. It is scored by the identity

$$a^3 + b^3 + c^3 + d^3 \quad = \quad X^3 + Y^3 + Z^3$$

where X, Y, and Z are as described below, in which s denotes $a^3 + b^3 + c^3 + d^3$ and brackets denote "pseudo-inverses", that is,

$$[x] = \begin{cases} 0 & \text{if } x = 0 \\ x^{-1} & \text{if } x \neq 0 \end{cases}$$

$$\begin{gathered}
X = (s^3 - 3^6)[3^2s^2 + 3^4s + 3^6] + (1 - 3[3])(a + b + c + d) + \\
(1 - (3s^2 + 3^3s + 3^5)[3s^2 + 3^3s + 3^5])((-s^3 - 3^6)[-3^2s^2 + 3^4s - 3^6] + \\
(1 - 2[2])((a^9s^3 + 1)[a^7s^2 + a^4s + a] + \\
(1 - (a^7s^2 + a^4s + a)[a^7s^2 + a^4s + a])((b^9s^3 + 1)[b^7s^2 + b^4s + b] + \\
(1 - (b^7s^2 + b^4s + b)[b^7s^2 + b^4s + b])((c^9s^3 + 1)[c^7s^2 + c^4s + c] + \\
(1 - (c^7s^2 + c^4s + c)[c^7s^2 + c^4s + c])((d^9s^3 + 1)[d^7s^2 + d^4s + d] + \\
(1 - (d^7s^2 + d^4s + d)[d^7s^2 + d^4s + d])((1 - a[a])b + a))))))
\end{gathered}$$

$$\begin{gathered}
Y = (-s^3 + 3^5s + 3^6)[3^2s^2 + 3^4s + 3^6] + \\
(1 - (3s^2 + 3^3s + 3^5)[3s^2 + 3^3s + 3^5])((s^3 - 3^5s + 3^6)[-3^2s^2 + 3^4s - 3^6] + \\
(1 - 2[2])((-a^9s^3 + 3^5a^3s + 3^6)[a^7s^2 + a^4s + a] + \\
(1 - (a^7s^2 + a^4s + a)[a^7s^2 + a^4s + a])((-b^9s^3 + 3^5b^3s + 3^6)[b^7s^2 + b^4s + b] + \\
(1 - (b^7s^2 + b^4s + b)[b^7s^2 + b^4s + b])((-c^9s^3 + 3^5c^3s + 3^6)[c^7s^2 + c^4s + c] + \\
(1 - (c^7s^2 + c^4s + c)[c^7s^2 + c^4s + c])((-d^9s^3 + 3^5d^3s + 3^6)[d^7s^2 + d^4s + d] + \\
(1 - (d^7s^2 + d^4s + d)[d^7s^2 + d^4s + d])((1 - a[a])c + a[a]((1 - b[b])c + b)))))))
\end{gathered}$$

$$\begin{gathered}
Z = (3^3s^2 + 3^5s)[3^2s^2 + 3^4s + 3^6] + \\
(1 - (3s^2 + 3^3s + 3^5)[3s^2 + 3^3s + 3^5])((3^3s^2 - 3^5s)[-3^2s^2 + 3^4s - 3^6] + \\
(1 - 2[2])((3^3a^6s^2 + 3^5a^2s)[a^7s^2 + a^4s + a] + \\
(1 - (a^7s^2 + a^4s + a)[a^7s^2 + a^4s + a])((3^3b^6s^2 + 3^5b^2s)[b^7s^2 + b^4s + b] + \\
(1 - (b^7s^2 + b^4s + b)[b^7s^2 + b^4s + b])((3^3c^6s^2 + 3^5c^2s)[c^7s^2 + c^4s + c] + \\
(1 - (c^7s^2 + c^4s + c)[c^7s^2 + c^4s + c])((3^3d^6s^2 + 3^5d^2s)[d^7s^2 + d^4s + d] + \\
(1 - (d^7s^2 + d^4s + d)[d^7s^2 + d^4s + d])((1 - a[a])d + a[a]((1 - b[b])d + b[b]((1 - d[d])c + d))))))))
\end{gathered}$$

[4] If K has fewer than 8 elements and other than 4 elements it's even easier to prove this last italicized lemma (with a little work needed when it has 6 elements). At this writing I have neither a proof nor counterexample when K has 8 elements. If the lemma is true for all finite K, I suspect that it's an anciently known fact.

There's a well-known metatheorem that says that when such an equation holds for all fields then it is a consequence of the equational theory of commutative von Neumann regular rings, that is, the theory of commutative rings together with a unary operation—here denoted with brackets—that satisfies the two further equations, $x[x]x = x = [[x]]$. The worse proof would start with the term $X^3 + Y^3 + Z^3$ and by a sequence of substitutions—each justified by one of the defining equations of commutative von Neumann regular rings—eventually reach the term $a^3 + b^3 + c^3 + d^3$.

A machine could find it.

I don't believe that any human will ever perform it.

Appendix 1

The two-variable polynomial in the awful proof provides another (but ancient) result:

In every subfield of the reals each positive element is the sum of three cubes of the subfield's positive elements.

What we need, given positive x, is a y such that the four terms,

$$3^2x^2y^7 + 3^4xy^4 + 3^6y, \qquad x^3y^9 - 3^6, \qquad -x^3y^9 + 3^5xy^3 + 3^6, \qquad 3^3x^2y^6 + 3^5xy^3,$$

are each positive. Since any subfield is a dense subset of $\mathbb{R}$ it suffices to find a non-empty open interval of ys on which all four terms are positive. The 1st and 4th terms are positive on the entire positive half-line. The 2nd term is positive on the open half-line starting at $\sqrt[3]{3^2/x}$. At the beginning of that half-line the 3rd term is equal to 3^7. So we finish by taking the right-hand endpoint of the open interval to be the first place where the 3rd term is equal to 0.[5]

Appendix 2

In all finite fields of order other than 4 or 7 every element is a sum of two cubes.

I assume this result is ancient. But here's the proof I found.

Let F be a field of order q and let $F^\star$ be the multiplicative group of non-zero elements in F. If 3 doesn't divide the order of $F^\star$ then, of course, the "cubing" function that sends x to x^3 is an endomorphism with a trivial kernel, hence a multiplicative automorphism—every element in F is a cube. We will assume, therefore, that 3 divides $q-1$.

Let $C \subset F$ be the set of cubes and $C^\star = C \cap F^\star$. The order of $C^\star$ is $(q-1)/3$. Note that C (no star) has slightly more than one third the number of elements in F.

$F^\star$ is partitioned into the three cosets of $C^\star$. We will use two facts: if any element of a $C^\star$-coset is a sum of two cubes then so are all elements of that coset and if y and z are in the same coset different from $C^\star$ then $xyC^\star$ is the remaining coset.

[5] The result can fail in the non-Archimedean case. (Any Archimedean ordered field, of course, is isomorphic to a unique subfield of the reals.) Order the polynomial ring $\mathbb{R}[X]$ "at infinity," that is by taking the positive elements to be all those polynomials with positive leading coefficients. The degree of an nth-power of a polynomial is, of course, divisible by n. In this ordering the sum of any number of nth-powers of positive polynomials still has a degree divisible by n. Thus for any integer $n > 1$ no such sum can be equal to $XP^n(X) > 0$. Restated: for any integer $n > 1$ the element X in the ring of rational functions $\mathbb{R}(X)$ when ordered by the functions' behavior "at infinity" is not the sum of any number of positive nth-powers.

The hypothesis says that we may assume that $q > 7$, hence we may choose $a \in F$ such that $a(a^3-1)(a^3+1) \neq 0$. Using that neither a, a^3+1 nor a^3-1 is zero, one of three possibilities holds:

Case 1: Either a^3+1 or a^3-1 is in $C^\star$.

Case 2: Neither a^3+1 nor a^3-1 is in $C^\star$ but they are in the same $C^\star$-coset.

Case 3: Neither a^3+1 nor a^3-1 is in $C^\star$ but they are in different $C^\star$-cosets.

In the 3rd case we are done: every $C^\star$-coset contains a sum of two cubes.

In the 2nd case we know that the product of a^3+1 and a^3-1 is in the remaining $C^\star$-coset hence that coset contains the sum of two cubes, to wit, $(a^2)^3 + (-1)^3$. We are done since all three cosets contain a sum of two cubes.

In the 1st case we may replace a with $-a$, if necessary, to reduce to the case that a^3+1 is a cube. Let b be such that $1 = b^3 - a^3$. Note that neither a nor b is zero.

Let $x \in F$ be arbitrary. If $xa^3 + C$ meets C then x is a sum of two cubes. Similarly if $xb^3 + C$ meets C. If both $xa^3 + C$ and $bx^3 + C$ are disjoint from C, then since $xa^3 + C$, $xb^3 + C$ and C each have slightly more than one third of the elements of F it must be the case that $(xa^3 + C) \cap (xb^3 + C)$ is non-empty. Let c, d be such that $xa^3 + c^3 = xb^3 + d^3$. Then $x = x(b^3 - a^3) = c^3 + (-d)^3$.

(Similar calculations tell us, further, that when 3 divides $q-1$ the average number of ways a non-zero element of a field of order q is a sum of two cubes is $(q+5)/18$ when q is odd and $(q+2)/18$ when q is even. Yes, the fields of order 2, 13 and 16 are the only fields in which each non-zero element has a *unique* representation as a sum of two cubes.)

Available at
`http://www.math.upenn.edu/~pjf/cubes.pdf`