Examples and simplifications related to the Fermat equation.

Introduction

For Let a, b, c be pairwise coprime integers and p an odd prime, and $a^p + b^p + c^p = 0$. What we will call the 'different element' is a particular element of a locally free module over the coordinate ring of the fiber in the Fermat curve over the rational j value corresponding to the numbers $a, b, c.$. That module embeds into the normalization of the coordinate ring of the fiber; the image of the different element in the normalization corresponds to a rational integer times a root of unity, and the rational integer, along with another rational integer for the fiber over a rational lambda value, provide a guide for how to assemble the components of the fiber, first putting together the components in the fiber over each of the six lambda value separately, and then attaching the partly-assembled pieces together to make the fiber over one j value. In each case, the rational integer indicates, on each irreducible component of the relevant fiber, the locus where that component meets the union of all the other components.

In general, once the discriminants of the irreducible components are inverted, a necessary and sufficient condition for a fiber to consist of smooth rational points of a curve is that the different element can be reduced to zero in an ambient resolution of singularities of the fiber. We obtain the different element by restricting a section of a line bundle of isomorphism type $\mathcal{O}(13p - 3)$ on the integer projective plane to an element of a locally free module over the coordinate ring of a fiber. The same one section of $\mathcal{O}(13p - 3)$ works for all fibers.

When the different element required fibers over separate rational λ values to intersect I first thought there was a contradiction; I'd expected only fiber and cusp components to meet. We now understand something else. The requirement of two generators in a finite residue algebra yields a tensor decomposition when their valuations are comparable, which is a residue of the pullback structure one would see analytically if such intersections were not empty, inconsistent with the differentials being locally principal.

The tensor indecomposability holds even if we do not assume that the Fermat equation is true, only that the fiber occurs in *some* smooth curve, and as we vary a, b, c over integers, we see that the non-reduced coordinate ring at the four-fold intersection point merges, the tensor decomposition disappears, when the valuation of a and of $b + c$ become incompatible, for the simple reason that in the finite residue algebra the order of nilpotency is finite, one or the other must be zero. This same finite order is present in the ordinary completion or in the local ring, because of Nakayama's lemma (an ordinary fact about radicals and ordered sets). When one of the generators shifts out of range, the tensor decomposition which would contradict the known smoothness for the Fermat curve and other curves degenerates, the tensor factors merge, and this then makes a place where a smooth rational point can come into existence.

1. Theorem. (under revision)

Preliminary results

We still assume $a^p + b^p + c^p = 0$ with a, b, c pairwise coprime and p an odd prime. Let q be a prime divisor of a, so the order $m = v_q(a) \geq 1$. from the formula $-a^p = b^p + c^p$ we have $1 + (c^{-1}b)^p$ is congruent to zero modulo q^{pm} where c^{-1} refers to the inverse of c modulo q^{pm}. Thus

$$(-c^{-1}b)^p \equiv\ 1\ mod\ q^{p\cdot v_p(a)}.$$

and we arrive at $-c^{-1}b$ one of the (possibly trivial) p'th roots of unity modulo q^{mp}. The units modulo q^{mp} is cyclic when q is odd, and the p-primary component is the trivial group when $q = 2$ since p is odd. There are at most p p'th roots of unity in the group of units of the integers modulo q^{mp}, that is, there are p if $q \equiv\ 1\ mod\ p$ and just 1 otherwise. If $p \neq q$ they can be described by first choosing any integer which represents a p'th root of unity modulo q and raising to a sufficiently high p'th power. There are two cases, still with $p \neq q$. If $-c^{-1}b\ \equiv\ 1\ modq^{p\cdot v_q(a)}$ then $q^{p\cdot v_q(a)}$, the highest power of q to divide a^p, is a divisor of $b + c$ and therefore q is not a divisor of the difference quotient $\frac{-a^p}{b+c} = \frac{b^p+c^p}{b+c} = b^{p-1} - cb^{p-2}... + c^{p-1}$. This is consistent with what we see if we just use the congruence $b + c \equiv\ 0\ mod\ q$ to replace c with $-b$ in the formula for the difference quotient, all terms are equal and we obtain $b^{p-1} + b^{p-1} + ... + b^{p-1} = pb^{p-1}$, the derivative of b^p with respect to p, which is indeed coprime to q since $q \neq p$ and $p|a$ which is coprime to b.

On the other hand, if $-c^{-1}b \not\equiv\ 1\ modq^{p\cdot v_q(a)}$ then q is not a divisor of $b+c$, and all of $q^{p\cdot v_q(a)}$ must be a divisor of the difference quotient $p^{p-1} - cb^{p-2}... + c^{p-1}$.

Moreover then it must be a nontrivial p'th root of unity, this requires there to be nontrivial p'th roots of unity modulo $q^{pv_q(a)}$, equivalently modulo q, so $q \equiv\ 1\ mod\ p$

When $q = p$ the p'th roots of unity in the units of the integers modulo $p^{p\cdot v_p(a)}$ are the cyclic group under multiplication generated by $(1+p)^{p\cdot v_p(a)-1}\ mod\ p^{p\cdot v_p(a)}$. When $-c^{-1}b \equiv\ 1\ mod\ p^{p\cdot v_p(a)}$ then again the full power of q divising into $-a^p = b^p + c^p$ also divides into $b + c$ so p is not a divisor of the difference quotient $b^{p-1} - cb^{p-2}... + c^{p-1}$.

Now we see a little inconsistency, because now using $b + c \equiv\ 0\ mod\ q^2$ and replacing c by $-b$ in the formula for the difference quotient again gives us pb^{p-1} the derivative, but the formula says the difference quotient *is* divisible by p, precisely the first power and not the second. The contradiction implies that we can remove this case: that when $q = p$ is a divisor of a it never happens that the root of unity $-c^{-1}b\ mod\ p^{p\cdot v_p(a)}$ is the trivial root of unity, but always nontrivial. When p is a divisor of a, the factorization of a^p into its greatest common divisor with $b + c$ and its greatest common divisor with $b^{p-1} - cb^{p-2}... + c^{p-1}$ would never quite be be a division into a pair of coprime p'th powers. It would be when p is not a divisor of a, with the prime divisors in the second factor required to be congruent to 1 modulo p, and for which the $p'th$ root of unity $-c^{-1}b\ mod\ q^{p\cdot v_q(a)}$ is a nontrivial p'th root of unity, and those primes q in the first factor allowed to have any congruence class $1, 2, 3, .., p-1$ modulo p being the ones for which the root of unity $-c^{-1}b\ mod\ q^{p\cdot v_q(a)}$ is the trivial root of unity.

But when the divisor q of a is congruent to 0 modulo p since $p \cdot v_p(a)$ is never equal to 1, the prime $q = p$ occurs on both sides of the factorization, exactly once in the second factor, and $p \cdot v_p(a) - 1$ times in the first factor, and the root of unity $-c^{-1}b\ mod\ p^{p\cdot v_p(a)}$ is never the trivial root of unity.

These facts merely restate the truth of the equation $a^p + b^p + c^p = 0$ when a, b, c are pairwise coprime and p odd reduced modulo a^p. The equation is equivalent, of course, to the more precise equation where we consider $= c^{=1}b^p = 1 - a^p$ modulo arbitrarily high powers of a, or in the completion of the integers at a, and also of course the same conditions apply after permuting a, b, c. In any case we will restate the weak version

2. Lemma. Let a, b, c be pairwise coprime and p an odd prime. The equation $a^p + b^p + c^p = 0$ implies that a^p factorizes into two parts, its greatest common divisor with $b + c$ and, if a is coprime to p, its greatest common divisor with the difference quotient $b^{p-1} - cb^{p-2}... + c^p$, otherwise the second part is this divided by p. That is, each prime divisor q of a besides p occurs with multiplicity $p \cdot v_q(a)$ in one factor or the other. The factor p if it occurs, occurs with multiplicity 1 in the second factor and multiplicity $p \cdot v_p(a) - 1$ in the first. For $q \neq p$ the prime q belongs to the first factor if and only if the p'th root of unity $-c^{-1}b\ mod\ q^{p\cdot v_q(a)}$ is the trivial root of unity, and in the second factor if it is a primitive p'th root of unity. The primes q besides p which belong to the second factor are all congruent to 1 modulo p while the primes q besides p in the first factor can have any congruence class modulo p. If p is a divisor of a the root p'th root of unity $-c^{-1}b\ mod\ p^{p\cdot v_p(a)}$ is always a primitive p'th root of unity. The same conditions remain true under permuting a, b, c of course, and more precise conditions are true if one completes at a instead of just reducing modulo a^p.

Remark. For fixed p we can interpret the equation $x^p + y^p + z^p = 0$ as saying that on the locus where yz is invertible $1 + (y/z)^p = -z^{-p}x^p$ where $-z^{-p}$ is a unit, and we can lift $(-y/z)$ to a Teichmuller root of unity in the completion at x, or we can write

$$1 + (z/y)^p = -y^{-p}x^p$$

and lift $(-z/y)$ to the reciprocal Teichmuller unit. A more general equation in four variables $x^p + y^p + z^p + w(xyz)^p = 0$ and note whenever this has an integer solution so does the original equation, as $w = (x^p + y^p + z^p)/(xyz)^p$ has small absolute value. The more general equation just asserts $x^p + y^p + z^p \equiv 0\ mod(xyz)^p$, and it is this which is equivalent to compatibility of the Teichmuller roots of unity.

Thus consistency of the Teichmuller roots of unity (the conclusion of Lemma 2) would imply the existence of an actual solution of $x^p + y^p + z^p = 0$.

Another way of saying this is, any proof of of the Fermat theorem implies that the assignment of Teichmuller roots of unity, which underlie the structure of the fiber over a lambda value and controls the tensor decompositions at meeting points of fiber components over different lambda values, actually is internally inconsistent in the fiber, and so the phenomenon of tensor decompositions which are residual of the analytic structure can be in a meta-mathematical sense 'proven' to be the reason why the theorem is true.

That word 'proven' can be made rigorous in the one easy step; a solution in the three separate completions, meaning, a solution of $x^p + y^p + z^p \equiv\ 0\ mod(xyz)^p$ really does lift to a solution of the precise equation, therefore a strategy to 'homotop' the existing proof into one aims to establish that an inconsistency in the Teichmuller roots of unity implies the existence of a tensor decomposition at the intersection of components of two fibers over separate lambda values, cannot be defeated by someone saying, "yes, but an assignment of Teichmuller roots being inconsistent with there being no such tensor decomposition only produces *fake* solutions of the Fermat equation! Is there a Hasse principle completing this picture by converting fake solutions into actual Fermat olutions? The answer to this question is provably "yes" because of the archimedian magnitude of the integer w.

In the remainder of the paper we will continue to look at difference quotients. We will initially work in the integers with $2, 3, p$ inverted so that the only ramification we will encounter is due to intersections.

We will see that we will be able to re-deduce Lemma 2 only from indirect properties such as symmetry of the different element and smoothness of the Fermat curve.

Definitions

When we write $\mathbf{Z}$ this will mean the ring $\mathbb{Z}[\frac{1}{2}, \frac{1}{3}, \frac{1}{p}]$. The ring $\mathbf{Z}[\omega]$ will denote $\mathbb{Z}[\frac{1}{2}, \frac{1}{3}, \frac{1}{p}]$ also adjoined a primitive p'th root of unity ω.

We will be interested in finite index subrings of cartesian products $R \subset A_1 \times ... \times A_m$ where each A_i is a copy of either $\mathbf{Z}$ or $\mathbf{Z}[\omega]$. The trace dual of such a ring R (within the corresonding cartesian product of copies of $\mathbb{Q}$ and $\mathbb{Q}[\omega]$) will be called R' and the normalization, which is merely $A_1 \times ... \times A_m$, may be also called $\overline{R}$.

We will say that the *different ideal* of R is the set of $r \in R$ such that $rR' \in R$.

When we speak of a direct sum of two rings, these are considered to be rings with identity element, and the direct sum ring has as its identity element the sum of the two separate identity elements for the subrings. Thus the inclusions and projections are not “homomorphisms of rings with identity element.”

At times, we may be concerned with the cases when R has a locally principal differentials module, thus we sate

Definition. the differentials module of a ring R is the R-module generated by a symbol dr for each $r \in R$ with relations that $d(ab) = adb + bda$ for all pairs $a, b \in R$.

If $R \subset A_1 \times ... \times A_m$ is such a subring, for any subset $S \subset \{1, 2, .., .m\}$ we will abbreviate by A_S the same cartesian product in which the factors A_i for $i \notin S$ are just ignored. The image of R in A_S will be called *the projection of R into A_S* , it is a homomorphic image of R and we will denote it by the symbol R_S.

Orbit representatives

Here is a set of orbit representatives for the action of $\mathrm{Aff}(F_p)$ on F_p^3 which we will need later. These will be the elements

$$(0, 0, 0), (0, 0, 1), (0, 1, 0), (0, 1, 1), ..., (0, 1, p - 1).$$

These comprise all tuples for which the first entry is 0, the second entry is 0 or 1 and if the second entry is 0 the last entry is 0 or 1.

Using these, and choosing or remembering our primitive p'th root of unity $\omega \in \mathbf{Z}[\omega]$, we may make three particular elements of $\mathbf{Z} \times \mathbf{Z}[\omega]^{p+1}$ depending on numbers a, b, c, which we call

$$\begin{gathered} x = (a, a, a, a, ..., a) \\ y = (b, b, b\omega, b\omega, ...b\omega) \\ z = (c, c\omega, c, c\omega, ..., c\omega^{p-1}). \end{gathered}$$

I hope that the pattern is clear, if we think of x, y, z as three rows of a matrix, each column consists of a, b, c with each term multiplied by the power of ω indicated by the entries of the corresponding three-tuple of elements of F_p, one for each of our choseen $\mathrm{Aff}(F_p)$ orbit representatives. In other words, if our orbit representatives are $v_1, ..., v_{p+2}$, our elements are

$$\begin{gathered} (a\omega^{v_i(1)})_i \\ (b\omega^{v_i(2)})_i \\ (c\omega^{v_i(3)})_i \end{gathered}$$

.

Define Λ (the reason for the notation will become clear later), to be the subring of $\mathbf{Z} \times \mathbf{Z}[\omega]^{p+1}$ which is spanned as a $\mathbf{Z}$-module by all monomials in x, y, z whose total degree in x, y, z is a multiple of p.

The next algebra will describe is Λ^6, the cartesian product of six copies of Λ within $(\mathbf{Z} \times \mathbf{Z}[\omega])^{p+1})^6$. We will index the cartesian factors by the six elements of the symmetric group S_3 writing $\Lambda^6 = \prod_{\sigma \in S_3} \Lambda_\sigma$. Likewise we will index the factors in the normalization, where each factor is a copy of $A_1 \times ... \times A_{p+2}$, by the elements of S_3 in the same way, so when we write A_σ we are referring to a cartesian product of $p+2$ factors, the first a copy of $\mathbf{Z}$ and the others copies of $\mathbf{Z}[\omega]$, so we may write

$$\Lambda^6 = \prod_{\sigma \in S_3} \Lambda_\sigma \subset \prod_{\sigma \in S_3} A_\sigma.$$

Define J to be the subalgebra of Λ^6 spanned by all monomials of degree a multiple of $6p$ in the three six-tuples which we will call

$$\begin{aligned} X &= (x, y, x, z, y, z) \\ Y &= (y, x, z, y, z, y) \\ Z &= (z, z, y, x, x, x) \end{aligned}$$

The columns result by applying each of the six possible permutations of $\{x, y, z\}$ to the first column, therefore the rows are also described

$$\begin{aligned} X &= (\sigma(x))_{\sigma \in S_3} \\ Y &= (\sigma(y))_{\sigma \in S_3} \\ Z &= (\sigma(z))_{\sigma \in S_3} \end{aligned}$$

Note that Λ is just the sum of the six projections of J on six summands of its normalization.

Examples of components in a fiber

Let a, b, c now be any three pairwise coprime numbers, and p an odd prime number. We construct the corresponding coordinate ring Λ. of the fiber of the Fermat curve over the corresponding lambda value. $Spec(\Lambda)$ has 1 irreducible component which is a copy of $Spec(\mathbb{Z})$ and $p+1$ irreducible components which are copies of $Spec(\mathbb{Z}[\omega]$. The components are indexed by the following triples of elements of $\mathbf{F}_p^3$ which are orbit representatives for the $\text{Aff}(F_p)$ action

$$(0,0,0), (0,0,1), (0,1,0), (0,1,1), (0,1,2), ..., (0,1,p-1).$$

Let q be a divisor of a. The tensor product of Λ over $\mathbb{Z}$ with the local ring $\mathbb{Z}_q$ of $\mathbb{Z}$ at q is a semilocalization. The corresponding semilocalization of the normalization is such that the first component is local and the others each have as many maximal ideals as the index in the units of $\mathbb{F}_p$ of the subgroup generated by $q \ mod \ p$. These maximal ideals in the localization of each component, direct sum the unit ideal of other components, comprise maximal ideals in the normalization $\overline{\Lambda}$, but they are allowed to coalesce when they are intersected with the subring Λ.

We will show that this semilocalization of Λ decomposes as a cartesian product of two rings, one is the projection on the first and fourth component, the other is the projection on the other components.

The first component corresponds to a copy of $Spec(\mathbb{Z}_q$ which has the prime residue field F_q. The corresponding maximal ideal in the fourth component must also be one with the prime residue field F_q therefore, however the fourth component is a semilocal ring allowed to have more than one maximal ideal.

We have been looking at $\Lambda = \Lambda_1$. When we look at the semilocalization at q of Λ_s for s the transposition fixing a, we will find that the components indexed by $(0,0,0),(0,1,1)$ there are disjoint from the corresponding components in $Spec(\Lambda_1)$ and do each meet all of the remaining $p-1$ components.

The different element

Let me preface this section by saying that there are many languages it could be written in, the language of bimodules, of dualizing sheaves, or of differential forms. The fact they are equivalent is explained in the Stacks project [3]. We will use the language of differential forms.

Here is what we will establish. Let $\mathcal{L}$ be the locally free J-module of rank one which consists of the values at the specific elements $X, Y, Z \in \overline{J}$ of all homogeneous polynomials of degree congruent to 1 modulo $6p$. The tensor power $\mathcal{L}^{\otimes i}$ depends only on the residue class of i modulo $6p$, and we may write $\mathcal{L}^{6p} = \mathcal{L}$ with an equality sign once we interpret the tensor power as representing polynomial multiplication.

In this section we'll consider a particular element of $d_J(X,Y,Z) \in \mathcal{L}^{\otimes(p-3)}$ which we've called the 'different element,' it is expressed as a particular homogeneous polynmial of degree $13p-3$ in X, Y, Z, and which is a restriction of a section of $\mathcal{O}(13p-3)$ on the integer projective plane which can be described by the same polynomial multiplied by, for example, $\frac{s}{X^{13p-3}}$ where s is a section of a line bundle with divisor of zeroes of degree $13p-3$ where $x=0$, so that the product is s times a rational function and the product is a section without poles.

We will also describe a rational integer. It will be the value at a, b, c of the polynomial $d_J(X,Y,Z)$ which we will call $d_J(a,b,c)$. The way they will be related is, there will be a root of unity $\alpha_J \in \overline{J}$ and the rational integer times a root of unity in the normalization, that is, the product $d_J(a,b,c)\alpha_J$ is equal to the image in the normalization of an embedded copy of the locally free module, such that the image of $d_J(X,Y,Z)$ under the embedding is $d_J(a,b,c)\alpha$.

We begin with the global picture.

Let $s_1 = X^p+Y^p+Z^p$, $s_2 = X^pY^p+Y^pZ^p+Z^pX^p$, $s_3 = X^pY^pZ^p$. To specialize the Frey j-invariant to a rational point we choose a matrix $\begin{pmatrix} A & B \\ C & D \end{pmatrix} \in Sl_2(\mathbb{Z})$

and consider the residue of $d\ log\ \frac{A+Bj}{C+dj}$ on the Fermat curve $s_1 = 0$ restricted to the fiber where $A + Bj = 0$. We will arrive at the element $d_J(X, Y, Z) =$

$6(XYZ)^{p-1} \cdot p^2(X^pY^p - Y^pZ^p)(Y^pZ^p - Z^pX^p)(Z^pX^p - X^pY^p)(X^pY^p + Y^pZ^p + Z^pX^p)(X^pZ^p + Z^pY^p + Y^pX^p)$

of $\mathcal{L}^{\otimes(13p-3)} = \mathcal{L}^{\otimes(p-3)}$.

To relate this to the different ideal of J, we will apply E. Noether's notion of the different [1], in the context of multilinear algebra and projective geometry [2],[3]. The overall picture is this: if we had defined the Noether different ideal of the affine cone of the fiber, it would have been generated by a size three Jacobian determinant. The value of this is our homogeneous polynomial of degree $13p-3$. Associated to the homogeneous polynomial is a section of $\mathcal{O}(13p-3)$ on the integer projective plane. The scheme where the section meets the zero section is defined locally by a size two Jacobian determinant. Thus when the line bundle is trivialized on affine charts the zero scheme agrees with the Noether different of the fiber.

Here are our conventions about projective geometry and first principal parts. In projective geometry, considering differentials like dx and dy when you care about the ratio $[x : y]$ if you allow yourself to write $[x : y] = [1 : y/x]$ then there should be some way to make sense of $d1$ and $d(y/x)$.

The trick is to understand that you are on a line bundle, the disjoint union of the lines through the origin, and you can think of x and y as linear functionals on each *line.* You imagine, the coordinate ratio is telling you which line to look at, one of x or y is a nontrivial linear functional on that line. If f is a section of the dual bundle, it induces a functional on any one of the lines. Working locally, we consider *df* and also f times the differential of a coordinate specifyng which line we are on, such as y/x. So we consider *df* and $fd(y/x)$; For example, when we take $f = x$ we have dx and $x(xdy - ydx)/x^2$ which is dx and $dy - (y/x)dx$, and by a change of basis this is the same as dx and dy again.

It is said that the rational function y/x, which makes sense at every point of the integer projective line, is a 'nome.' If we interpret it as the ratio $[y : x]$ it is defining an isomorphism, but a question is, if we instead interpret y/x as an element of the quotient field of a function ring, or as a function with a simple pole, how can we identify that it is a nome? We can consider the differential $d(y/x)$ and this is nonzero wherever it is defined, but fails to make sense at one point. Crucially, if y, x are sections of a line bundle on some other manifold, giving a map to the projective line, how do we find the 'critical locus' which if there were no denominator would be the locus of zeroes of the pullback of $d(y/x)$?

The clearest way of answering this will be to say that the deRham differential d in exactly this setting extends to a connection ∇ with values in first principal parts, and we may rigorously write $d\ log\ (y/x) = \nabla\ log(y/x)$ and then follow this with

$$\nabla\ log(y/x) = \nabla\ log(y) - \nabla\ log(x)$$

Each of $\nabla(x)$ and $\nabla(y)$ is the rigorous manifestation of what earlier I called dx and dy, they are global sections of a rank two vector bundle over $\mathbb{P}^1$ which is the prinicpal parts bundle of $\mathcal{O}(1)$, and becauses principal parts is suitably functorial if $\mathcal{L}$ is the line bundle pullback of $\mathcal{O}(1)$ under the morphism underlying our rational function, whose domain is the complement of the indeterminacy locus, the same symbols describe the corresponding global sections of the rank two pullback vector bundle. This principal part is a rigorous and meaningful interpretation for what should be the residue of the logarithmic derivative, that is

$$y \cdot \nabla \ log(y) = \nabla(y)$$
$$x \cdot \nabla \ log(x) = \nabla(x)$$

The wedge product $\nabla(x) \wedge \nabla(y)$ is, up to sign, the unique generator for the second exterior power of the first principal parts of $\mathcal{O}(1)$ on the projective line, the global sections sheaf is a free module of rank one over the rational integers.

Next let's talk about a very general principle under which we can generalize the expression $xdy - ydx$ to higher dimensions and explain how it is related to logarithmic differential forms. First we work in affine space in three dimenisions. Here, consider

$$xdy \wedge dz - ydx \wedge dz + zdx \wedge dy$$

It is very interesting that the value of such an expression, as a differential form, is unaffected by multiplying each of x, y, z by the same differentiable function of x, y, z. For example in this case of three variables

$$(fx)d(fy) \wedge d(fz) - (fy)d(fx) \wedge d(fz) + fzd(fx) \wedge d(fy)$$

$$= f^3(xdy\wedge dz - ydx\wedge dz + zdx\wedge dy) + f^2(xzdy\wedge df + xydf\wedge dz - yzdx\wedge df - xydf\wedge dz + xzdf\wedge dy + yzdx\wedge df)$$

in which the second term is zero. We can use this differential n form – the contraction of $dx_0 \wedge ... \wedge dx_n$ along the vector-field $\sum x_i \frac{\partial}{\partial x_i}$ – to describe a global section of differential n-forms on projective space $\mathbb{P}^n$ tensored with a line bundle $\mathcal{O}(n+1)$. On $\mathbb{P}^2$, we may choose our function f to be $\frac{1}{x_0}$ so that the left side of the equation in the calculation above is

$$(fx)d(fy) \wedge d(fz) - (fy)d(fx) \wedge d(fz) + fzd(fx) \wedge d(fy) = d\frac{y}{x} \wedge d\frac{z}{x} - 0 + 0$$

and we have arrived at the standard volume two-form on the affine plane with coordinates $\frac{y}{x}, \frac{z}{x}$. The fact that the patching when we change from one of the standard coordiante charts to the other involves homogeneity of degree three explains why this is not describing a differential two-form, but a global section of the two-forms tensored by $\mathcal{O}(3)$.

We are going to give a better explanation of that standard form on affine space by pulling it back to the line bundle. First we need a tutorial about line bundles and vector bundles.

We can interpret line bundles two separate ways. To construct a line bundle we might call $\mathcal{O}(3)$ we first imagine that we have a line bundle $\mathcal{L}$ with a global section s whose divisor of zeroes is some curve or divisor, for example the divisor described by x^3. Then we may obtain other global sections by multiplying by rational functions which have poles no worse than the zeroes of x^3 so that the product will have no poles. These are the $\frac{1}{x^3}x^iy^jz^ks$ such that $i+j+k=3$ with $i,j,k \geq 0$. It is sometimes a convention to erase the symbol $\frac{1}{x^3}$ and the symbol s and to state that global sections of $\mathcal{O}(3)$ have as a basis the actual monomials $x^iy^jz^k$ for $i+j+k=3$, but this would be misleading and confusing.

Now that we are done with the tutorial about vector bundles, let's talk about logarithmic forms. We usually consider those differential one-forms on the total space V of a line bundle which are allowed logarithmic poles on the zero section E, and twisted by $-E$. These are the one-forms which restrict to zero on E in the forms sense, and when we restrict to E in the coherent sheaf sense we arrive at the first principal parts bundle of the dual line bundle $\mathcal{L}$. This is just copying what we have said already, if f is a nonzero section of the dual bundle $\mathcal{L}$, we have a local basis $df, fdx_1, ..., fdx_n$ We may consider one local section to be fixed, and imagine that $\nabla(f) = df + 0fdx_1 + ... + 0fdx_n$ is the deRham differential on the line bundle of f, which is our section of the dual bundle Then any other nonzero local section is a multiple gf and working on the total space of the line bundle $\nabla(fg) = d(fg) = gdf + \frac{\partial g}{\partial x_1}fdx_1 + ... + \frac{\partial g}{\partial x_n}fdx_n$. in the original basis. So the sequence of coordinates of the coherent sheaf restriction of dg is $(g, \frac{\partial g}{\partial x_1}, ..., \frac{\partial g}{\partial x_n})$. We are describing the firt principal parts sheaf – or vector bundle – of the dual line bundle, and except for questions of naturality it would be OK to say that it is spanned by formal direct sums $g \oplus dg$. Note also that we can formalize the rule above as the rule of a connection, $\nabla(gf) = g\nabla(f) + f \otimes dg$, section of $\mathcal{L} \otimes \Omega_{\mathbb{P}^2}$. where $\mathcal{L}$ is our dual line bundle.

Questions of naturality explain why we are not describing a direct sum bundle, but rather we are describing a vector bundle $\mathcal{P}(\mathcal{L})$ and an exact sequence $0 \to \Omega \otimes \mathcal{L} \to \mathcal{P}(\mathcal{L}) \to \mathcal{L} \to 0$. This sequence makes sense even on singular varieties, and remains exact if one reduces Ω and $\mathcal{P}(\mathcal{L})$ modulo torsion. It is the same as $(\mathcal{O} \otimes \mathcal{O})/I^2 \otimes \mathcal{L}$ with its coherent sheaf structure on the left, where $\mathcal{O}$ is the structure sheaf, and it can be geometrically understood as sections of $\mathcal{L}$ keeping track of an infinitesimal neighbourhood.

Just on general principles, the exact sequence shown above induces a long exact sequence involving exterior powers of $\mathcal{P}(\mathcal{L})$, but it makes more sense to go to the conceputal origin. If V is a line bundle and $\mathcal{L}$ its dual, the sheaf $\mathcal{O}(-E)$ on V pulls back to $\mathcal{L}$ itself, and as $\mathcal{O}(-E)\Omega_V(log(E))$ pulls back to $\mathcal{P}(\mathcal{L})$ the sheaf $\Omega_V(log(E))$ just pulls back to $\mathcal{L}^{\otimes(-1)} \otimes \mathcal{P}(\mathcal{L})$.

For the logarithmic differential forms of all degrees, contracting against the Euler derivation gives a long exact sequence of vector bundles on V

$$0 \to \Lambda^{r+1}\Omega_V(log\ E) \to \Lambda^r\Omega_V(log\ E) \to,,,, \to \mathcal{O}_V \to 0$$

This pulls back on the zero section E to a long exact sequence

$$0 \to \mathcal{L}^{\otimes(-r-1)} \otimes \Lambda^{r+1}\mathcal{P}(\mathcal{L}) \to \mathcal{L}^{\otimes(-r)} \otimes \Lambda^{r}\mathcal{P}(\mathcal{L}) \to ...$$

In the case when E is the projective plane and V is the disjoint union of the lines through the origin in three space, this becomes

$$\mathcal{O}(-3) \otimes \Lambda^3\mathcal{P}(\mathcal{O}(1)) \to \mathcal{O}(-2) \otimes \Lambda^2\mathcal{P}(\mathcal{O}(1)) \to ...$$

The sheaf $\mathcal{P}(\mathcal{O}(1))$ is just a trivial vector bundle of rank 3 with basis $\nabla(x), \nabla(y), \nabla(z)$. Tensoring with $\mathcal{O}(3)$ gives

$$0 \to \Lambda^3\mathcal{P}(\mathcal{O}(1)) \to \mathcal{O}(1) \otimes \Lambda^2\mathcal{P}(\mathcal{O}(1)) \to ...$$

I apologize if this was a lengthy development, it is something trivial. The sheaf on the left, $\Lambda^3\mathcal{P}(\mathcal{O}(1))$ is a trivial sheaf of rank one, it has a unique generating section up to sign which is $\nabla(x) \wedge \nabla(y) \wedge \nabla(z)$. So the first sheaf is

$$\Lambda^3\mathcal{P}(\mathcal{O}(1)) = \mathcal{O} \cdot \nabla(x) \wedge \nabla(y) \wedge \nabla(z).$$

When we wrote that form on affine space which is 'homogeneous' of degree three with respect to function multiplication, can now describe the phenomenon rigorously. The image of $\nabla(x) \wedge \nabla(y) \wedge \nabla(z)$ under the embedding shown is

$$x \otimes (\nabla(y) \wedge \nabla(z)) - y \otimes (\nabla(x) \wedge \nabla(z)) + z \otimes (\nabla(x) \wedge \nabla(y))$$

It spans the image of the first map from $\mathcal{O}$ in the exact sequence

$$0 \to \mathcal{O} = \Lambda^3\mathcal{P}(\mathcal{O}(1)) \to \mathcal{O}(1) \otimes \Lambda^2\mathcal{P}(\mathcal{O}(1))$$
$$\to \mathcal{O}(2) \otimes \Lambda^1\mathcal{P}(\mathcal{O}(1)) \to \mathcal{O}(3) \to 0$$

which comes from the action of contracting the exterior algebra on the differentials of the total space of $\mathcal{O}(-1)$ with log poles on the zero section along its Euler vector field, and tensoring with $\mathcal{O}(3)$. This global section is a natural image of the triple wedge product $\nabla(x) \wedge \nabla(y) \wedge \nabla(x)$ which bases $\Lambda^3\mathcal{P}(\mathcal{O}(1))$.

If we allow ourselves to write down *rational* sections of the prinicpal parts sheaf we can simplify this natural image section as

$$= xyz(\nabla\ log(y) \wedge \nabla\ log(z) - \nabla\ log(x) \wedge \nabla\ log(z) + \nabla\ log(y) \wedge \nabla\ log(z)).$$

Using the valid rules like

$$\nabla(x) = \nabla(y\frac{x}{y}) = \frac{x}{y}\nabla(y) + y \otimes d\frac{x}{y}$$

and so

$$\nabla\ log(x) = \frac{1}{x}\nabla(x) = \frac{1}{y}\nabla(y) + \frac{1}{(x/y)}d(x/y)$$

giving

$$d\ log\ (x/y) = \nabla\ log(x) - \nabla\ log(y).$$

Using this, our invariant expression can be rewritten without needing to use ∇, it is

$$(xyz)d\ log(y/x) \wedge d\ log(z/x)$$

and this expression is invariant under even permutations of the variables.

First let's include formal details of this, and then make it more rigorous. For the formal details, we have

$$\begin{aligned} xyz\nabla\ log(y/x) \wedge \nabla\ log(z/x) &= xyz(\nabla\ log\ y - \nabla\ log\ x) \wedge (\nabla\ log\ z - \nabla\ log\ x) \\ &= xyz(\frac{\nabla(y)}{y} - \frac{\nabla(x)}{x}) \wedge \frac{\nabla(z)}{z} - \frac{\nabla(x)}{x}) \\ &= (xz\nabla(y) - yz\nabla(x)) \wedge (\frac{\nabla(z)}{z} - \frac{\nabla(x)}{x} \\ &= x\nabla(y) \wedge \nabla(z) - y\nabla(x) \wedge \nabla(z) - z\nabla(y) \wedge \nabla(x) \end{aligned}$$

To be more rigorous we should rewrite xyz as a rational function like $\frac{yz}{x^2}$ times a section s of $\mathcal{O}(3)$ which takes a zero of order three on the hyperplane defined by x. So a more correct expression is

$$\frac{y}{x}\frac{z}{x}s \otimes d\ log\ \frac{y}{x} \wedge d\ log\ \frac{z}{x}.$$

As a sanity check, since we are talking about rational sections we are allowed to move the first two factors past the tensor sign and this just becomes

$$s \otimes d\frac{y}{x} \wedge d\frac{z}{x}$$

the tensor product with the most obvious two-form in coordinates y/x and z/x, with our section of the line bundle $\mathcal{O}(3)$.

This too can be totally explained. From the exact sequence $0 \to \mathcal{L} \otimes \Omega_E \to \mathcal{P}(\mathcal{L}) \to \mathcal{L} \to 0$ we obtain when E is dimension two

$$\begin{gathered} \Lambda^3\mathcal{P}(\mathcal{L}) \cong \mathcal{L} \otimes \Lambda^2(\mathcal{L} \otimes \Omega_E) \\ 0 \to \Lambda^2(\mathcal{L} \otimes \Omega_E) \to \Lambda^2\mathcal{P}(\mathcal{L}) \to \mathcal{L} \otimes \Lambda^1(\mathcal{L} \otimes \Omega_E) \to 0 \\ 0 \to \Lambda^1(\mathcal{L} \otimes \Omega_E) \to \Lambda^1\mathcal{P}(\mathcal{L}) \to \mathcal{L} \otimes \Lambda^0(\mathcal{L} \otimes \Omega_E) \to 0 \end{gathered}$$

and tensoring each with the next higher power of $\mathcal{L}$ gives the short exact sequences which splice together to give the long exact sequence. Just splicing the first with the twist of the second gives

$$0 \to \Lambda^3\mathcal{P}(\mathcal{L}) \to \mathcal{L} \otimes \Lambda^2\mathcal{P}(\mathcal{L}) \to \mathcal{L}^{\otimes 3} \otimes \Omega_E \to 0.$$

On each local chart where we trivialize $\mathcal{L}$ this yields an actual presentation of Ω_E with generators pairwise wedge products of $\nabla(x), \nabla(y), \nabla(z)$ and with one relation which is the image of the triple wedge product $\nabla(x)\wedge\nabla(y)\wedge\nabla(z)$ under our map, which had been induced on logarithmic differentials by the Euler flow.

In our setting, we have a rational function given by the j invariant we wish to calculate the residue of $d\ log\ \frac{A+Bj}{C+dj}$ or, to remove some prejudice, let us say, $d\ log\ \frac{As_2^3+Bs_3^2}{Cs_2^3+Ds_3^2}$ at the locus of the Fermat curve where the numerator is zero and the denominator is 1, and where s_1, s_2, s_3 are the degree two and three elementary symmetric polynomials in X^p, Y^p, Z^p (the Fermat equation asserts $s_1 = 0$).

We had shown on the projective plane that when s is a section of $\mathcal{O}(3) = \mathcal{L}^{\otimes 3}$ which vanishes to degree three on the hyperplane defined by x, the expression

$$\frac{y}{x}\frac{z}{x}s \otimes d\ log\ \frac{y}{x} \wedge d\ log\ \frac{z}{x}.$$

describes a section of $\mathcal{L} \otimes \Lambda^2 \mathcal{P}(\mathcal{L})$ which spans the kernel of the map to $\mathcal{L}^3 \otimes \Omega_E$ and here E is the integer projective plane.

Although it is not quite the right thing to do, if we just choose a homogeneous polynomial P of degree $5p$ in X, Y, Z then we can consider a rational map to $\mathbb{P}^2$ with the role of x being played by $Cs_2^3 + Ds_3^2$, the role of y being played by $As_2^3 + Bs_3^2$, the role of z being played by s_1P as all three have degree $6p$, and we arrive at

$$\frac{As_2^3 + Bs_3^2}{Cs_2^3 + Ds_3^2}\ \frac{s_1P}{Cs_2^3 + Ds_3^2}s \otimes d\ log(\frac{s_1P}{Cs_2^3 + Ds_3^2}) \wedge d\ log(\frac{As_2^3 + Bs_3^2}{Cs_2^3 + Ds_3^2})$$

Let us take some time to explain what this formula represents. To the left of the tensor sign, the symbol s is a global section of $\mathcal{O}(18p)$ and the rational functions multiplying it just mean the symbol to the left of the tensor sign is a rational section of $\mathcal{O}(18p)$ on the integer projective plane.

The symbols to the right of the tensor sign are a wedge product the differentials of two ordinary rational functions, thus a rational section of the two-forms, which we could if we wish interpret as a rational section of $\mathcal{O}(-3)$.

Because of the rule in affine space $d(s_1P) = s_1dP + Pds_1$ where we have $s_1 = 0$ the sheaf spanned by these sections for all choices of P is just $\mathcal{O}(5p)$ times the single section of $\mathcal{O}(13p - 3)$ coming from the Jacobian matrix with P replaced by 1.

This means, the actual calculation which we want is the same as we have done, setting $P = 1$ and taking the determinant of the affine size three Jacobian determinant to obtain a homogeneous polynomial of degree $13p - 3$.

An easy way of remembering what that homogeneous polynomial is, if we had merely calculated the Noether different of the affine cone of a fiber over a j value, we would have obtained a homogeneous polynomial of degree $13p - 3$ as a generator, and it is this same homogeneous polynomial which, when viewed as a section of the line bundle $\mathcal{O}(13p-3)$, defines the different subscheme of the fiber by its intersection with the zero-section of that line bundle.

To be very clear, there are three ways of rewriting our vector bundle section. If we write it

$$\frac{As_2^3+Bs_3^2}{Cs_2^3+Ds_3^2}s\otimes d\frac{s_1P}{Cs_2^3+Ds_3^2}\wedge d\ log(\frac{As_2^3+Bs_3^2}{Cs_2^3+Ds_3^2})$$

we could view it as the residue of $d\ log\ j$ for a particular j value, restricted to the curve by wedging with the differential of its defining relation, and then tensored with our rational section.

If we write it

$$s\otimes d\frac{s_1P}{Cs_2^3+Ds_3^2}\wedge d\frac{As_2^3+Bs_3^2}{Cs_2^3+Ds_3^2}$$

and similarly on other coordinate charts, we see the Noether different tensored with the section s and with the ambient two-forms. This is what proves that the different section as we have defined it locally agrees with the Noether different.

For the analogous different element of the fiber over a λ value one can repeat the calculation but instead of the polynomials s_2 and s_3 just using X^p and Y^p.

We also need a tutorial about Noether's different. If a $\mathbf{Z}$-algebra R were built from generators ω_1,ω_2 and relators

$$\begin{cases} f(\omega_1,\omega_2)=0 \\ g(\omega_1,\omega_2)=0 \end{cases}$$

then we might repeat the construction, adjoining variables x_1,x_2 subject to the same relations, building $R\otimes_{\mathbf{Z}}R$. Then

$$0=f(x_1,x_2)-f(\omega_1,\omega_2)$$

$$=f(x_1,x_2)-f(\omega_1,x_2)+f(\omega_1,x_2)-f(\omega_1,\omega_2)$$

$$=\frac{f(x_1,x_2)-f(\omega_1,x_2)}{x_1-\omega_1}(x_1-\omega_1)+\frac{f(\omega_1,x_2)-f(\omega_1,\omega_2)}{x_2-\omega_2}(x_2-\omega_2)$$

and likewise

$$0=g(x_1,x_2)-g(\omega_1,\omega_2)$$

$$=\frac{g(x_1,x_2)-g(\omega_1,x_2)}{x_1-\omega_1}(x_1-\omega_1)+\frac{g(\omega_1,x_2)-g(\omega_1,\omega_2)}{x_2-\omega_2}(x_2-\omega_2)$$

Here, what are written as difference-quotient fractions should really be thought of as polynomials (and the same thing is familiar in analysis using Weierstrass preparation theorems) with a degree-one divisor removed. We obtain that the two-by-two matrix of difference quotients annihilates the column $(x_1-\omega_1,x_2-\omega_2)$, from the calculation of adjoint matrices its determinant annihilates the diagonal ideal I in $R\otimes R$, the kernel of multiplication $R\otimes R\to R$ which introduces the relations $x_i=\omega_i$. In general, Noether defines the different ideal to be the image in R of the annihilator of I, a special case being the determinant of a square Jacobian matrix of partial derivatives. We do not yet have this situation four our size three determinant, but the definition applies locally (this precise identity involving a size two determinant).

The relation between Noether's notion of different and the trace element is that the annihilator of $I \subset R \otimes R$ can be interpreted as bimodule homomorphisms $Hom(R, R \otimes R)$ and there is a general principle that bimodule maps from R to $Hom_{\mathbf{Z}}(A, B)$ for R modules A, B gives $Hom_R(A, B)$. Applying this to $A = Hom_{\mathbf{Z}}(R, \mathbf{Z})$ and $B = R$ gives that the annihilator of I is a copy of the R-module maps $Hom_{\mathbf{Z}}(R, \mathbf{Z}) \to R$, and the image in R is then the possible images of the trace element.

Note well that even though the principal parts module of the restriction of $\mathcal{O}(6p)$ to an affine coordinate chart already is of the form $R \otimes R$ tensored with the restricted module, Noether's reasoning about different quotients does not directly apply there, it needs to be generalized, but, in fact, one way to generalize it is to observe that the three-by-three determinant, when written in local coordinates, due to the magic we saw above, of how the Leibniz quotient rule interacts with the invariant differential form, becomes a two-by-two Jacobian determinant made of rational functions that happen to be defined near a point of interest when the line bundle is trivialized. The size three determinant really is the one which could have arisen, if we had wished to consider it, from the defining relations of the affine cone. Therefore, it is the messy local calculation immediately above which proves that Noether's different extends to principal parts.

Thus, let $\mathcal{L}$ be the subset of $\overline{J}$ consisting of all polynomials in the elements $X, Y, Z \in J$ whose degree is congruent to 1 modulo $6p$. It is locally free of rank one over J and each tensor power $\mathcal{L}^{\otimes i}$ can be identified with the polynomials in X, Y, Z of degree congruent to i modulo $6p$. Likewise let $\mathcal{N}$ be polynomials in $x, y, z \in \overline{\Lambda}$ of degree congruent to 1 modulo p. Let $d_\Lambda(x, y, z) = p^2(xyz)^{p-1} \in \mathcal{N}^{\otimes p-3}$ and $d_J(X, Y, Z) = p^2(XYZ)^{(p-1)} \cdot 6(X^pY^p - Y^pZ^p)(Y^pZ^p - Z^pX^p)(Z^pX^p - X^pY^p)(X^pY^p + Y^pZ^p + Z^pX^p)(Y^pX^p + Z^pY^p + X^pZ^p) \in \mathcal{L}^{\otimes(p-3)}$.

4. Theorem.

i) There is a root of unity $\alpha_J \in \overline{J}$ such that $d_J(X, Y, Z) = d_J(a, b, c)\alpha_J$ and where we define $d_J(a, b, c)$ to be the rational integer $d_J(a, b, c) = p^2(abc)^{p-1} \cdot 6(a^pb^p - a^pc^p)(b^pc^p - b^pa^p)(c^pb^p - c^pa^p)(a^pb^p + b^pc^p + c^pa^p)(b^pa^p + c^pb^p + a^pc^p)$.

ii) Assuming $a^p + b^p + c^p = 0$, the different ideal of the algebra J is $\mathcal{L}^{\otimes(4p+3)}d_J(X, Y, Z)$. Explicitly it is polynomials in $X, Y, Z \in \overline{J}$ which are simultaneously multiples of $d_J(X, Y, Z)$ and degree a multiple of $6p$.

iii) There is a root of unity $\alpha_\Lambda \in \overline{J}$ such that $d_\Lambda(x, y, z) = d_\Lambda(a, b, c)\alpha_\Lambda$ and where we define $d_\Lambda(a, b, c)$ to be the rational integer $d_\Lambda(a, b, c) = p^2(abc)^{p-1}$

iv) The different ideal of the algebra Λ is $\mathcal{M}^{\otimes 3}d_\Lambda(x, y, z)$. Explicitly it is polynomials in $x, y, z \in \overline{\Lambda}$ which are simultaneously multiples of $d_\Lambda(x, y, z)$ and degree a multiple of p.

v) Also, the index of each relevant algebra R in its trace dual R' is the square of its index in its normalization $\overline{R}$, so the rational integer d_R in each case is given

$$d_R = [R' : R]^{\frac{1}{rank_{\mathbf{Z}}(R)}} = [\overline{R} : R]^{\frac{2}{rank_{\mathbf{Z}}(R)}}.$$

Proof. We have already seen that the different element is an element of the module $\mathcal{L}^{\otimes(p-3)}$ Before specializing it was possible to identify the different element after locally trivializing a line bundle with the Noether different. Therefore the differentials module is $\mathcal{L}^{p-3}$ modulo the span of the different element, tensored with $\mathcal{L}^{3-p}$.

By wedging the logarithmic form $d\ log\ \ j$ with the differential of the defining equation of the fermat curve we were restricting it correctly, and the "different element" in $\mathcal{O}(13p-3)$ was describing the residue. Now in the end we are just calculating the Kahler differentials of each coordinate chart of the fiber in a standard way. Although we needed to insert and then remove the polynomial P and keep track of twisting (as we did not do very well in the end anyway).

The same considerations apply to the module $\mathcal{M}$ and the algebra Λ.

Using part v) to calculate $d_J(a,b,c)$ would requires a significant note of caution. The legitimacy of the calculation relies on the assumption that $a^p + b^p + c^p = 0$. Hence we can never actually apply the index formula above $d_J(a,b,c) = [\overline{J} : J]^{\frac{1}{rank(R)}}$ to evaluate $d_J(a,b,c)$ explicitly unless we could find such numbers a, b, c. Here is an example using the formula with $p = 1$ (which is not a prime). Take $a = 5, b = 7, c = -12$, adding to zero. The index is the 6/2 (=half the rank) power of $2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 17 \cdot 19 \cdot 109^2$, which is identical to $(abc)^{p-1} \cdot (a^p c^p - b^p c^p)(b^p a^p - c^p a^p)(c^p b^p - a^p b^p)(a^p b^p + b^p c^p + a^p c^p)^2$ (for some reason the leading coefficient of 6 is missing, but it is invertible since we work in $\mathbf{Z}$ now, not $\mathbb{Z}$). Once we repeat for $a = 3, b = -9, c = 5$ adding to -1 the index is the 6/2 power of $2^4 \cdot 3 \cdot 7$, not even divisible by 5. The reappearance of of factors when the sum becomes zero forbids a direct sum decomposition of the residue algebra we will look at later when the symmetrical different applies, as part of the expression factorizes $...(abc)^{p-1} \cdot (a^p c^p - b^p c^p)... = ...(abc)^{p-1} \cdot c^p(a^p - b^p)...$ with a factor of c on both sides of the dot. When it is direct-sum indecomposable we will pass to considering tensor decompositions.

Returning to generalities, in scheme language, when the different ideal of such an algebra R as we are discussing generates the same ideal in the normalization as an element of $\mathbf{Z}$, the implies that the same element of $\mathbf{Z}$ defines on each irreducible component of $Spec(R)$ the locus where that component meets the union of all the other components. We have allowed $2, 3, p$ to have inverses in $\mathbf{Z}$ to ensure that no ramification occurs in normalizing any component, that is why the different element can correctly describe intersections. But we must be careful. The relation on components of meeting in the semilocalization at a rational prime is not an equivalence relation.

Let us state just one direction of this bi-implication carefully and precisely, including making a choice of a prime ideal in $\mathbb{Z}[\omega]$.

5. Theorem. Let $q \in \mathbf{Z}$ be a prime divisor of $d_\Lambda(a,b,c)$. Then for every $i \in \{1,...,p+2\}$ there is a two element subset subset $S = \{i,j\} \subset \{1,2,...,p+2\}$ including i and a prime ideal Q of Λ_S containing q times the identity element, such that, denoting by $\Lambda_{S,Q}$ the corresponding local ring, and $\Lambda_{\{i\},Q}$ and $\Lambda_{\{j\},Q}$ the corresponding projections to components of the corresponding semilocalization of the normalization (or components of the total fraction ring of the normalization as one may wish), $\frac{[\overline{\Lambda}_{S,Q}:\Lambda_{S,Q}]}{[\overline{\Lambda}_{\{i\},Q}:\Lambda_{\{i\},Q}]\cdot[\overline{\Lambda}_{\{j\},Q}:\Lambda_{\{j\},Q}]}$ is divisible by q. Likewise let q instead be a prime divisor of $d_J(a,b,c)$. Then for every $j \in S_3 \times \{1,...,p+2\}$ there is a two-element subset $S = \{j,k\} \subset S_3 \times \{1,2,...,p+2\}$ including j and a prime ideal Q of J containing the identity time q, such that the index quotient $\frac{[\overline{\Lambda}_{S,Q}:J_{S,Q}]}{[\overline{\Lambda}_{\{j\},Q}:J_{\{j\},Q}]\cdot[\overline{\Lambda}_{\{k\},Q}:J_{\{k\},Q}]}$ is divisible by q

Recall where we are, the numbers $1,2,...,p+2$ index orbit representatives for the action of $\mathrm{Aff}(F_p)$ on F_p^3 with the number 1 indexing $(0,0,0)$.

Applying this principle, and the invariance of the rational integer associated to the different element in $\mathbf{Z}$ under direct sum and summand, one has this corollary.

6. Corollary. Let $q \in \mathbf{Z}$ be a prime element which is a divisor of abc. Suppose the different element of Λ and J are as we described. Then there is a four-element subset $S \subset S_3 \times \{1,2,..,.p+2)\}$ and a prime ideal Q of J_S with $S = \{(1,1),(1,j),(\sigma,k),(\sigma,l)\}$ with the permutation σ satisfying $\sigma \neq 1$, and with i,j,k,l satisfying $j \neq 1, k \neq l$, such that for every two-element subset $T = \{\alpha,\beta\} \subset S$ the index quotient $\frac{[\overline{J}_{T,Q}:J_{T,Q}]}{[\overline{J}_{\{\alpha\},Q}:J_{\{\alpha\},Q}]\cdot[\overline{J}_{\{\beta\},Q}:J_{\{\beta\},Q}]}$ is divisible by q.

Proof. First let's give a scheme-theoretic proof. $Spec(J)$ is a union of six schemes each with $(p+2)$ irreducible components, one copy of $Spec(\mathbb{Z})$ and $p+1$ homomorphic images of copies of $Spec(\mathbb{Z}[\omega]$. $Spec(\Lambda^6)$ is the abstract disjoint union of those six schemes. Choose any prime ideal of $A_{1,1}$ containing q and let Q denote its inverse image in $\Lambda = \Lambda_1$. We may assume by permuting a,b,c that $q|a$. The rational integer $d_\Lambda(a,b,c)$ describes the locus on each component of $Spec(\Lambda)$ where that component meets the union of the remaining components. Since q times the identity element of Λ belongs to Q there must be at least one other component among the images of $Spec(A_{1,2}),...,Spec(A_{1,p+2})$ whose image meets $Spec(\Lambda_1)$ at the point corresponding to Q. So there is a j such that the image of A_j contains the point Q. Consider the image in $Spec(\Lambda)$ of the disjoint union of $Spec(A_{1,1}$ and $Spec(A_{1,j})$ The coordinate ring of the union is the image of the projection of all of Λ_1 on two factors, which is the same as the projection of J on the same two factors, it is $((\Lambda_1)_{\{(1,1),(1,j)\}} = J_{\{(1,1),(1,j)\}}$ The local ring of this ring corresponding to our prime ideal Q is just the image of of the local ring $\Lambda_Q = \Lambda_{1,Q}$ in either the semilocalization or total fraction ring of the normalization projected to the same two components. We may call this $\Lambda_{\{1,1,1,j\},Q}$. The index of the localized ring in its normalization, which is incidentally just $A_{(1,1),Q} \times A_{(1,j),Q}$ is divisible by q just because it is not an isomorphism, the local ring is not normal since it is not irreducible. (We could use the symbol J or Λ_1 or Λ interchangeably since we the projection of J onto two factors of the normalization of $\Lambda = \Lambda_1$ factors through the projection of J in Λ_1 itself.) Next, if all the irreducible components of J which are incident to $Spec(A_{1,1})$ at Q belong to the image of $Spec(\Lambda_1)$ then they are in the image of a part of the disjoint union which would map isomorphically in a neighbourhood of the intersection point, and the rational integers $d_J(a,b,c)$ and $d_\Lambda(a,b,c)$ associated to the different elements, being an invariant of the isomorphism types of the coordinate rings, would be agree as elements of $\mathbb{Z}$ localized at q. But this is not the case, a higher power of q is a divisor of $d_J(a,b,c)$. Therefore some projection $J_{\{(1,1),(\sigma,k)\}}$ has index in its normalization divisible by q, and this produces our permutation σ. Now we work within Λ_σ and repeat the earlier steps which we did when we were talking about Λ_1, to produce a (σ, l) such that $J_{\{(\sigma,k),(\sigma_l)\}}$ has index in its normalization divisible by q. We have produced our four element set S and verified a relation between pairs whose transitive closure is all of S. Since one of the components is rational $(\mathbf{Z})$ the inverse image of the maximal ideal defined by q is a maximal ideal of J with residue field the prime field F_q, and the relation in question is merely the equality of the intersection of the maximal ideal with J. This is a transitive relation, so all other pairwise projections coming from other two-element subsets of S must have index in their normalization divisible by q. Note that for components whose normalization is isomorphic to $\mathbf{Z}[\omega]$, even while the normalization can have more than one maximal ideal containing q, this is not so for J itself.

9. Remark. If J occurs as the coordinate ring of an affine subscheme of a curve whose localization at $6p$ is smooth (such as a Fermat curve), the ring J and also hence its homomorphic image which we are considering here must have locally principal differentials module. This is an extremely restrictive condition; it imples that the indecomposable local ring of order q^{2p} with residue field F_q produced by the theorem must be tensor indecomposable, so isomorphic to $F_q[T]/(T^{2p})$. We will give examples at the end where a choice of a, b, c not satisfying the Fermat equation has the expected tensor decomposition – thus detectably inconsistent with the Fermat equation – but where the tensor factors merge into one once the q-adic valuation of $b + c$ is allowed to be much larger than that of a.

Direct-sum decomposition

The previous results use the different element to establish a hypothesis, and that is exactly the hypothesis of the next theorem.

10. Theorem. Let p be a prime number, let ω be a primitive p'th roof of unity. Let a, b, c be pairwise coprime, let $q|a$ be prime divisor of a with $q \neq 2, 3, p$.

Choose the set H of orbit representatives of $\mathrm{Aff}(F_p)$ acting on F_p^3 such that the first coordinate is zero, the second coordinate is 0 or 1 and if the second coordinate is 0 the third coordinate is 0 or 1. Let s be a permutation of a,b,c. Let v_0, v_1, v_2, v_3 be elements of our orbit representative set $H \subset F_p^3$ such that $v_0 = (0,0,0)$, $v_1 \neq v_0$, and $v_3 \neq v_2$. Consider the subring of $Z[w]^4$ spanned by all homogeneous polynomials of degree a multiple of $6p$ in the three elements

$$\begin{gathered} x = (aw^{v_0[0]}, aw^{v_1[0]}, s(a)w^{v_2[0]}, s(a)w^{v_3[0]}) \\ y = (bw^{v_0[1]}, bw^{v_1[1]}, s(b)w^{v_2[1]}, s(b)w^{v_3[1]}) \\ z = (cw^{v_0[2]}, cw^{v_1[2]}, s(c)w^{v_2[2]}, s(c)w^{v_3[2]}) \end{gathered}$$

It has rank k where k is the number of i such that $v_i = (0,0,0)$ plus $p-1$ times the number of i such that $v_i \neq (0,0,0)$. Choose a prime divisor q of a in $\mathbf{Z}$ and localize our algebra at a prime ideal Q containing q times the identity element. Suppose that the corresponding projection on the corresponding semilocalization of the first two components in the normalization is direct-sum indecomposable (corresponding to the corresponding components meeting at Q in the fiber over one λ element), and suppose also that the projection on corresponding semilocalization of the normalization of the last two comments is direct-sum indecomposable (corresponding to two components meeting at Q in the fiber over another λ value). Suppose now that the local ring is direct-sum indecomposable (by transitivity which holds since we are talking about a local ring, (this could be established by showing one commponent of the first two meets one commponent of the second two at Q)

Then necessarily s is the transposition

$$\begin{gathered} s(a) = a \\ s(b) = c \\ s(c) = b \end{gathered}$$

. Also, after interchanging v_2 and v_3 if necessary, there is a $j \in \{1, 2, .., p-1\}$ such that

$$\begin{gathered} v_0 = (0,0,0) \\ v_1 = (0,1,1) \\ v_2 = (0,0,1) \\ v_3 = (0,1,j) \\ b^2 \equiv c^2\omega \ mod \ Q \end{gathered}$$

Proof. In the case when $s(a) \neq a$, we may assume by interchanging labels that $s(a) = b$. Then $x^{6p} = (a^{6p}, a^{6p}, b^{6p}, b^{6p}) \in J$ This has two components which are units and two which are divisible by q times the identity so belong to Q. The reduction modulo Q of this together with the identity span an F_q algebra which is at least two dimensional, but the residue field of Q is just F_q so the algebra could not be direct sum indecomposable.

We turn to the more difficult case when $s(a) = a$. Our choice $v_0 = (0, 0, 0)$ ensured that the residue field we are considering is the prime field F_q. This means that when we consider our algebra, a localization at one prime ideal Q of the set of polynomials in x, y, z homogeneous of degree a multiple of $6p$ where x, y, z are the particular elements of the normalization shown above, the residue field is the prime field, and the reduction of the first coordinate modulo q gives a consistent way to evaluate the residue class of any such polynomial modulo Q. Those which evaluate to 0 are the ones which belong to Q. By contrast, the actual multiples of q in our subring are represented by those polynomials $P(x, y, z)$ of degree a multiple of $6p$ which have only the weaker condition that all coefficients are divisible by q.

Any polynomial divisible by x (as a polynomial, recall x is not an element of our subring) does belong to Q since the first coordinate of x is a which is divisible by q. Next consider polynomials not involving x, the $P(y, z)$ which are homogeneous of degree a multiple of $6p$ as expressions in the variables y and z. We know y and z as elements of $\overline{J}$ are of the form

$$y = (b, b\omega^q, c\omega^r, c\omega^s)$$

$$z = (c, c\omega^t, b\omega^u, b\omega^v).$$

Consider the particular monomial of degree $6p$ which is $y^{3p-1}z^{3p+1} = b^{3p-1}c^{3p-1}(c^2, c^2\omega^{t-q}, b^2\omega^{r-u}, b^2\omega^{s-v})$. Now, b and c are invertible in our local ring which then includes

$$(1, \omega^{t-q}, b^2c^{-2}\omega^{r-u}, b^2c^{-2}\omega^{s-v})$$

Unless $t \equiv q \ mod \ p$ the projection on the first two factors has a direct sum decomposition. We can see that by exhibiting the first two entries of x, y, z

$$\begin{matrix}(a, a) \\ (b, b\omega^q) \\ (c, c\omega^t)\end{matrix}$$

We may take q, t to be the last two entries in any one of our orbit representatives besides of $(0, 0, 0)$ which occurs already in the first column. If we choose any but $(0, 1, 1)$ we have $q \not\equiv t \ mod \ p$ and the monomials of degree 1 and $6p$ include

$$(b^ic^j, b^ic^j\omega^{qi+tj}) = b^ic^j(1, \omega^{qi+tj})$$

for $i + j = 6p$ and $(1, 1)$. Since b, c are coprime to q the span of these if we invert b, c in our base ring $\mathbf{Z}$ is the same as the span of

$$(1, \omega^{qi+tj})$$

Thus we have $(1, \omega^j)$ for all j, the sum of these for $j = 0, 1, ..., p - 1$ is $(p, 0) = p(1, 0)$ and recall p is invertible so we obtain $(1, 0)$. Then we obtain all $(0, \omega^j)$.

Thus the only possibility for the second column is the orbit representative $(0, 1, 1)$.

Our ring is now spanned by monomials multiples of $6p$ in

$$\begin{array}{c} x = (a, a, a, a) \\ y = (b, b\omega, c\omega^u, c\omega^v) \\ z = (c, c\omega, b\omega^r, b\omega^s) \end{array}.$$

From the monomial $y^{3p+1}z^{3p-1}$ after dividing by $(bc)^{3p+1}$ as we may, assuming b, c invertible, we are obtain as an element of our subring

$$(1, 1, c^2b^{-2}\omega^{r-u}, c^2b^{-2}\omega^{s-v}).$$

Subtracting $(1, 1, 1, 1)$ gives

$$(0, 0, c^2b^{-2}\omega^{r-u} - 1, c^2b^{-2}\omega^{s-v} - 1).$$

Now localize our algebra at a maximal ideal Q containing q times the identity element $(1, 1, 1, 1)$ to obtain a local ring. Unless all four entries belong to the maximal ideal Q some entries will be invertible and others zero, splitting the algebra. This requires then that $r - u = s - v$ and $\omega^{r-u} \equiv c^{-2}b^2 \ mod\ Q$. where the expression c^{-2} refers to the inverse of c mod q.

After replacing the third component by its AffF_p representative we obtain up to interchanging v_2 and v_3 is the claimed pattern. QED

11. Example. If we take a, b, c, p, q to be $13, 7, 3, 5, 11$ we obtain an algebra of rank 13 and index $3^4 \cdot 5^2 \cdot 7^6 \cdot 11^{16} \cdot 41^2 \cdot 101^2$ in its normalization. The reduction modulo 11 is direct sum decomposable of dimension 13 over $\mathbb{F}_{11}$. If we instead build the subring of $\mathbb{Z}^4$ where we have substituted ω with 37107 in the three rows, the reduction of the subalgebra modulo q times its identity element is an indecomposable algebra of rank four but with radical whose third power is zero, which is therefore tensor-decomposable by our definitions. The way we chose the number 37107 is to take $c^2b^{-2} \equiv 4\ mod 11$ and raise it to a high power of 11, and reduce modulo a high power of 11 to obtain the corresponding Teichmuller representative.

In some sense, it seems the tensor decomposability of the algebra is merely encoding that in attempting to solve the Fermat equation, 11^5 is not really a divisor of $3^5 + 7^5$.

Tensor decomposition

I should clarify, when I speak of a tensor decomposition of an algebra A over a field F, I mean a surjecive homomorphism $B \otimes_F C \to A$ in which neither the composition with $A \otimes F \to A \otimes B$ nor with $F \otimes B \to A \otimes B$ is surjective.

Let's make a deformation construction. Consider the algebra which we were already looking at, the subring of $\mathbb{Z} \times \mathbb{Z}[\omega]^3$ spanned by monomials of degree multiples of $6p$ in

$$\begin{gathered} x = (a, a, a, a) \\ y = (b, b\omega, c, c\omega) \\ z = (c, c\omega, c\omega, c\omega^2) \end{gathered}$$

We might as well revert to calling this J_S for S the appropriate four-element subset of $S_3 \times \{1, 2, ..., p+2\}$. A generalization of this is the sub-algebra of the polynomial algebra $\mathbf{Z}[T]^4$ generated by polynomials of degree multiples of $6p$ in the elements

$$\begin{gathered} x = (a, a, a, a) \\ y = (b, bT, c, cT) \quad . \\ z = (c, cT, cT, cT^j) \end{gathered}$$

Another specialization of the general algebra occurs if we apply the homomorphism of $\mathbb{Z}[T]^4 \to \mathbb{Z}^4$ which on each component is the map $\mathbf{Z}[T] \to \mathbf{Z}$ sending T to an integer representative of c^2b^{-2} *mod* q, under our assumptions of direct sum indecomposability this will reduce to a primitive p'th root of unity in $\mathbf{F}_q$, and we may choose the integer representative to reduce to a p'th root of unity modulo a successively higher power of q by raising it to the p'th power repeatedly.

If we apply instead the homomorphism $\mathbb{Z}[T] \to \mathbf{Z}[\omega]$ on each component sending T to ω we'll recover our algebra.

Next, we reduce our subalgebra of $\mathbf{Z}^4$ modulo the ideal *in the subring* generated by q times the identity element. The result will always be an $\mathbf{F}_q$-algebra of dimension four.

I claim that this algebra of dimension four is a homomorphic image of the localization of J_S at Q.

A conventional way of arguing, instead of using $\mathbf{Z}[T]$, would be to embed $\mathbf{Z}[\omega]$ into the completion of $\mathbf{Z}$ at q. Under our assumptions of direct sum indecomposability we do have that $q \equiv 1$ *mod* p so this is possible.

In any case, we may find a sufficiently high power of (q, q, q, q) in $\mathbf{Z}^4$ such that the ideal generated in $\mathbf{Z}^4$ by that power (q^N, q^N, q^N, q^N) is contained in the ideal in the subring generated by the first power (q, q, q, q), and therefore we may obtain the same $\mathbf{F}_q$ algebra at the end if we first tensor $\mathbf{Z}^4$ over $\mathbf{Z}$ with $\mathbf{Z}/(q^N\mathbf{Z})$. For example, by the Artin-Rees theorem. When we do that, we see that ω has been correctly specialized to a primitive p'th root of unity in each factor anyway.

12. Theorem. Let a, b, c be coprime integers and p an odd prime. If any divisor q of a besides $2, 3, p$ is not a divisor of $b + c$ and the subalgebra of $\mathbb{Z}^4$ described above, reduced modulo its own element q, is tensor decomposable (as it indeed is in many examples) then $a^p + b^p + c^p \neq 0$.

Proof. This may be an elementary property of the structure of the algebra, but it is easiest to prove by combining things we know. The algebra is not even direct sum indecomposable unless ω is congruent to $b^{-2}c^2$ modulo Q in $\mathbf{Z}[\omega]$, this implies that q is a divisor of the difference quotient $b^{p-1} - cb^{p-2}... + c^{p-1}$. The comparison of the rational integer $d_\Lambda(a,b,c)$ coming from the different element of the disjoint union of the fibers over the λ lying over j and the rational integer $d_J(a,b,c)$ coming from the full fiber showed that there must be such an indecomposable configuration of four components such as this, even while localized at a particular prime ideal Q containing q, and we showed in the previous theorem that this is the essentially unique way it could happen. But any such local algebra must have locally principal differentials module (recall we inverted $1/6p$), and this forces the maximal ideal in our local algebra to become principal when the algebra is reduced modulo q. QED

Remark. Tensor indecomposability of the reduction modulo q of such examplesis equivalent to the condition that for all α, β in our F_q algebra which do not reduce to zero, α is a divisor of β in the F_q algebra if and only if $v_m(\alpha) < v_m(\beta)$.

We already know from the preliminary section that if the Fermat equation were true, once $v_q(b^{p-1} - cb^{p-2}... + c^{p-1})$ is nonzero, as long as $q \neq p$, the valuation must take the value $p \cdot v_q(a)$. It is interesting to consider the remark above taking α to be a monomial of degree $6p$ in x, y, z which is divisible only by the first power of x, and to take β to be $(y - z)$ times a monomial of degree $6p$. It seems likely that the comparison critereon above about anti-symmetry of valuation comparisons would allow a person to re-deduce the fact that the order at q of the difference quotient cannot take any intermediate value between 0 and $pv_q(a)$ just from the previous remark, depending therefore only on smoothness of the Fermat curve (with p inverted) and the symmetry of the different element.

Examples

14. Example. We already know that this type of example will be inconsistent with the Fermat equation anyway, but it is interesting to see what happens with actual numbers a, b, c which – by necessity of our choices – do not satisfy the Fermat equation. To find an example where the F_q algebra is tensor indecomposable, we avoid the condition in Theorem 13, thus let's take $b + c$ divisible by a high power of q, so we take $a = 3, b = 19, c = 59030, p = 5, q = 3$ obtaining a rank 10 subring of index 52851989777827347726236832454215866380455969825 in its normalization whose reduction modulo q is neither direct-sum decomposable nor tensor indecomposable. Perhaps this example can exist because $b + c = a^{2p}$, and so $(y + z)y^{6p-1}$ exceeds the nilpotency degree of the algebra and cannot be a generator. To see this example calculated click here.

The clear situation is this: in analysis the fiber over a j value is a pullback, and smooth local analytic rings are topologically monogenic, while fibers over distinct lambda values do not meet. In algebra, the different element says the fibers meet at closed points, and differential calculus still holds that the residue rings over $Spec(Z)$ must be literally monogenic. In cases when the order of a and $b+c$ at a prime q are comparable, a sort of analytic pullback structure peeks in, a pair of generators is needed. But algebraic local rings at pullback points have a tensor decomposition, here we expected a tensor decomposition and found there is, two generators are needed. Yet, the order of nilpotency of a finite algebra is also finite, and we can shift one or the other generator out of existence by making the order at q of a and $b+c$ incomparable. Although the order of nilpotency is $2p$, for some reason we cannot prove decomposability when the valuation of one element is even p times that of the other.

15. Comment. Our analysis in Corollary 3 involving the factorization of b^p+c^p breaks down in the case $p=2$. Theorem 13 refers to q-adic order in $\mathbf{Z}$ where 2 is invertible. I do not know if it is possible to prove that $x^2+y^2+z^2$ cannot be zero for x, y, z not all zero, without attaching signs to real values. Hilbert attached signs algebraically for example, to the odd number -135, by considering the indecomposable sumamnds of $\mathbf{Z}/((-135)\mathbf{Z}) \cong \mathbf{Z}/(5\mathbf{Z}) \oplus \mathbf{Z}/(27\mathbf{Z})$. He reduced the orders of the summands modulo 4 to arrive at the sequence $(1,-1)$ and compared this to the reduction $-135 \ mod\ 4 = 1$. The triple product $1\cdot(-1)\cdot 1 \equiv -1 \ mod\ 4$ is the sign. As odd squares are added the reduction modulo 4 cycles through the number of terms in the sum.

We are approaching the same limitation, even without any precise calculation, this must be true because reducing modulo q means that when the valuation at q of a and $b+c$ differs by more than the dimension $2p$ one or the other becomes negligible. Using the completion instead of the reduction will not help since in this setting a module is principal if and only if it is principal modulo its radical.

The absence of nontrivial sums of squares adding to zero, and explanation of the Fermat equation, would be explained by by the concept of tensor indecomposability in all cases when the valuation at q of $b+c$ and a are not too far apart multiplicatively.

16. Remark. In the example, if 59030 is replaced by $3^5 - 19$ the algebra remains tensor indecomposable, and tensor decomposes when it is replaced by $3^4 - 19$. The case of $3^5 - 19$ is when the bound is achievable, but recall q is not supposed to equal $2, 3$ or p. We should not be using $a = 3$ since it is not coprime to the permutation group order, but the analogous transition occurs when $q = a = 5, p = 3, c = q^n - b$, for various values of b. They are are indecomposable and tensor indecomposable for $n = p$. Click here for the case $b = 3$ and you can observe that if you reduce c to $5^2 - b = 22$ a tensor decomposition occurs.

17. Remark. Robert May once used Lotka-Volterra's equations to contradict a report asserting that subdividing a natonal park by a road would increase species diversity. I failed to understand that May was not actually saying, “Let’s rely on Lotka-Volterra from now on.”

While it could have acted as a salve to run a model like Lotka-Volterra showing virtual animals springing into existence when a road is removed (I actually tried to do this), absent being able to apply Popper’s philosophy of science where people need to irreversibly decide future actions, we need to understand, as likely Robert May would have understood – in fact I know that he was dismissive of my attempt when I had hoped to tutor a student about it – that every model is actually only a disaster model. Climate models can meaningfully show something going wrong; but they can not establish any way back to safety, besides contradicting isolated misconceptions (engines in these tractors will make the soil suitable for food, this dam will generate power, etc). Evolutionary psychology does give a reliable intuitive vision of the shifting baseline paradigm, the so-called ‘appeal to nature fallacy’ is not a fallacy even while it cannot be scientifically supported.

For a specific example, Chemists label lines in a spectrum by a pair of ‘term symbols.’ Although they speak colloquially about an ‘electron transition’ they know full well that it is almost never correct to speak of an ‘electron’ unless The notion of probability can be rigorous when observing experiments, but it is not rigorous to say, here is a way a photon can appear, leaving this type S term symbol, an electron.

Wave equations were historically justified by thinking of a fluid as a collection of particles, or trying to describe probability waves or quantum fields. One intuitively knows, (this may be universal among practitioners in chemistry) that a harsh logical proposition about the type of a term symbol sits as a sort-of damaging piece of hardware in a stream of consciousness in some sense almost intended to more faithfully represent what is naturally there, but which is not scientifically supported. Here, for the Fermat equation, the same familiar paradigm shows us a tensor decomposition merging, as for isolating a rational point, or for a chemist to isolate an electron, or in elementary teaching, for an inequality about a discriminant or some sort of base extension to separate roots of a polynomial. There could be no ab initio notion that it should be insightful to look at real points and guess conditions for them to be rational, as the case of $x^2 + y^2 + z^2$ illustrates. (We can interpret non-negativity of area various ways, instead of subdividing a mosaic, Pythagoras might have noticed that the self-similar subdivision which fails for the pentagram actually does work for similarities of a right triangle, or anyway our consistent mainstream formulations of the real line and exterior algebra support that there was no such reason to restrict area be only a positive quantity).

For us to say, once the tensor decomposition has merged, a rational point can appear, is still only yet another statement passing from being intuitive, tentative, and ambiguous, to being mechanical, eventually seen failing to encompass duality, perspective. Removing such a notion by a type of political correctness isn’t good to do either. It is hard then to see any option besides an accumulating warehouse of conceptual junk that does not work anymore, or give up and wait for the boss at Microsoft to update something, or try to find it on the first page of Google.

The situation reminds me of Wittgenstein's well-discussed notion of the dangerous cave, about the danger of wasting time reconsidering things that needn't be considered. A notion of considering that beliefs could be illusory was then a playful abstraction, the danger was wasting time examining meaning and intentions which needn't be considered anymore. But there is in that sense in modern discourse what would be termed another cave where people go all the time without worrying. Animals appear healthy and well if they are well-kept, while, by contrast, in wild animals a relatively un-eroded context for meaningful thought allows something relatively transient and powerful. I liked listening to an online comment of N Chomsky, we are familiar with ways that animals don't appreciate human thought; it might be likely that if we could have encountered an intact residue of pre-historic thought, that is, some thinking of wild or un-domesticated people, we would be in the position of an animal trying to understand human speech.

References

1. E.Noether, Idealdifferentiation und Differente, notes from 1929 lecture in Prague, J.reine ang.Math, 188, 1-21 (1950)
2. E. Kunz, Kahler Differentials, Advanced Lectures in Mathematics (1986)
3. Discriminants and Differents (38 pages), the Stacks project.