

Galois Theory Research

1st January 2011

© 2011 by Jim Adams

Introduction.

This was the content of an email to Doly García. It is controversial, and is put here to give background to the way I was thinking at the time.

Since you say you don't like Galois theory (Galois wouldn't have got published if he had lived), let me make two statements.

- (1) Galois theory is right.
- (2) Galois theory may be wrong.

I will attempt to justify in different senses both of the above statements.

Galois theory is right.

To justify this we need to know in a nutshell what Galois theory is: *it is about irreducibility.*

What do we mean by this? I will give an example. Call the rational numbers \mathbb{Q} , and a polynomial in the variable x which is rational $\mathbb{Q}[x]$. Then the polynomial

$$x^2 + 2$$

is irreducible over $\mathbb{Q}[x]$. This is because it factorises in the complex numbers, the roots are

$$(x + \sqrt{-2})(x - \sqrt{-2})$$

– so it is irreducible over the rationals and reducible over the complex numbers.

What is Galois theory about? It is about irreducibility over $\mathbb{Q}[\omega]$. Here ω are complex roots of unity, i.e. numbers of the form $e^{i2\pi/n}$. It states that polynomials of degree ≥ 5 cannot be factorised over this field. Why?

Let us look at the quintic

$$(x + a)(x + b)(x + c)(x + d)(x + e).$$

It is evident that if you permute any of a , b , c , d or e then the above polynomial remains the same.

We say the polynomial is invariant under the symmetric group – in other words the group of permutations, in this case, of 5 objects.

Why is this irreducible over $\mathbb{Q}[\omega]$?

Well, what permutations are available to ω ? The available transformations are *rigid*. All you can do is mirror reflect them (in other words, complex conjugation) or rotate them (multiply by a root of unity). So the number of transformations you can do to $\mathbb{Q}[\omega]$ is *less* than the transformations you can do to the roots – at least for the quintic.

That is how Abel and Ruffini proved the quintic is insoluble in the case

$$x^5 - 4x + 2.$$

The group theory is as follows. The symmetric group on 5 objects, S_5 , has only *one* proper subgroup, A_5 , and this is not commutative. Since fields are commutative, although there is a normal series

$$S_5 \supset A_5 \supset 1,$$

It has only one factor group, $A_5/[1]$, and this is non-abelian (non-commutative). The definition of the word *solvable* for groups is that there is a normal series of groups (which corresponds to solving polynomials of successively lower degree) *and* factor groups are abelian. Since fields are abelian, this appears to be eminently sensible, and the quintic is therefore insoluble by group theory.

Galois theory may be wrong.

We are working in fields, but we don't have to. A matrix, X , is generally non-commutative. So if you have a polynomial in matrices

$$(X + A)(X + B),$$

when you swap A and B , because

$$AB \neq BA$$

you *don't* get invariance. So the arguments tend to break down. This makes things more difficult. I have a number of comments to make about the group theory here.

In the first place, to find an algorithm for a solution means effecting a transformation. In category theory, where we are dealing with morphisms – another word for transformation – we can have objects (in our case, our initial preference for these is matrices), and we have morphisms, but another way of looking at this is to treat the objects as a special type of morphism. So a not-so sophisticated comment we could make about this is that transformations of matrices can be operations like $A*B = AB - BA$ which are not associative, unlike matrices. We add in parenthesis that this is not category theory, which deals with associative systems, but the idea carries over.

Secondly, in the definition of solvability, what is the status now of the statement that factor groups are abelian? If we have a matrix polynomial with real coefficients, then these coefficients commute, and n th and m th powers of a matrix commute with each other. However, in the solution of a cubic, even one which has real coefficients, complex solutions obtrude. Thus we might expect, even restricting solutions to matrices, non-commutative operations to be inherent in the solution if there is one, and a matrix, given its representation as the imaginary number i , does not commute with a general 2×2 matrix. So the set of solutions might depend on whether we represent them as terms in order left to right or in order right to left. So I am not convinced, at this stage, that the existence of abelian factor groups is a necessary condition in the non-abelian case.

Lastly, what is the status of the normal series condition $S_5 \supset A_5 \supset 1$? There are no intermediate normal groups between S_5 and A_5 , or A_5 and 1 . This immediately says, if the interpretation system is correct, that there is no intermediate algorithm, or that there is no solution in stages involving the quartic, cubic and quadratic. There is a statement by Artin in his book on Galois theory, that if a solution in the abelian case of the quintic could be found, then a normal series would exist. We are now claiming that if a solution in the non-abelian case can be found, this implies the above normal series, and the solution has to be found in two steps, not four. This is formidably discouraging, even if a solution exists.

I would also like to add the comment, that Galois theory is traditionally presented as a theory of groups, but its natural setting is a theory of rings. As ring theory, normal groups are kernels of homomorphisms, and factor groups are represented as ideals. This seems to carry over quite well to the non-commutative case.

The remainder of this piece is as it was originally.

If you assume that Galois theory for commutative fields works, and you equate – I will introduce these later – the matrix equivalent of real and complex parts – then you get out again that the quintic and higher degree polynomials are insoluble. On the way you get new solutions – of the quadratic, cubic and quartic – which don't correspond to the traditional solutions – this is on my website www.jimhadams.com – the Galois theory of non-commutative fields.

So we have proved that polynomial equations in five or more variables – even matrix ones – are insoluble, yes? No! Not yet!

I first want to mention a statement made on page 20 of [1]. There are two zeros of the polynomial

$$(\lambda - 1)(\lambda + 2) = 0,$$

but if A is an arbitrary 2×2 matrix, then

$$(A - I)(A + 2I) = A^2 + A - 2I = 0$$

has more than two zeros. This follows since the product of two matrices $(A - I)$ and $(A + 2I)$ may be the zero matrix even in the case of nonzero factors. For the above matrix polynomial, as well as the zeros I and $-2I$, it is not difficult to see that the matrix

$$A = \begin{vmatrix} -2 & a \\ 0 & 1 \end{vmatrix}$$

is also a zero for any number a .

Consider the *matrix* polynomial

$$(X + A)(X + B)(X + C)(X + D)(X + E)$$

In which every swapping of A, B, C, D and E leaves the polynomial invariant. Isn't that a scalar field? *Not necessarily!*

All we need to do is maintain invariance with respect to A, B, C, D and E , not anything in between! OK, where are we with group theory and roots of unity – don't the latter have to be *rigid*?

Well. I combine these ideas together to form what I call hyperintricate numbers – these are representations of $2^n \times 2^n$ matrices. First note that a number

$$a_1 + bi$$

where a_1 is real and bi is imaginary – so $i = \sqrt{-1}$ – can be represented by matrices

$$a_1 + bi,$$

$$\text{where } 1 = \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} \text{ and } i = \begin{vmatrix} 0 & 1 \\ -1 & 0 \end{vmatrix}$$

The algebra is entirely the same as for the complex field. Now introduce an additional

$$\text{set of matrices, the } \textit{actual} \text{ matrix } \begin{vmatrix} 1 & 0 \\ 0 & -1 \end{vmatrix} \text{ and the } \textit{phantom} \text{ matrix } \begin{vmatrix} 0 & 1 \\ 1 & 0 \end{vmatrix}$$

We now have four matrices describing a general 2 x 2 matrix (an *intricate* number denoted by I):

$$a1 + bi + c\alpha + d\phi.$$

As it rests, this will not solve our problem. Introduce the 2-hyperintricate basis of I^2

$$\left\| \begin{array}{c|c} + & 0 \\ \hline 0 & + \end{array} \right\| \left\| \begin{array}{c|c} 0 & + \\ \hline - & 0 \end{array} \right\| \left\| \begin{array}{c|c} + & 0 \\ \hline 0 & - \end{array} \right\| \left\| \begin{array}{c|c} 0 & + \\ \hline + & 0 \end{array} \right\|$$

where '+' is any intricate basis element and '-' is the negative of it.

This is an alternative description to Lie groups.

This *still* won't solve our problem. Introduce a 3-hyperintricate basis in the same way: the '+' matrices are the 2-hyperintricate ones, the '-' being their negative. I claim the 3-hyperintricate basis is useful. Why?

We are dealing now with 8 x 8 matrices, generally non-commutative. Some of our elements – the intricate ones – act as imaginary numbers – so we have roots of unity, but – *we have more than one set of these*. In fact 2-hyperintricate numbers – 4 x 4 matrices – contain the quaternions – with *three* sets of imaginary units.

Right, I now want a multiplicative matrix description of permutations. I show an example

$$(a, b, c) \left\| \begin{array}{c|c|c} 0 & 1 & 0 \\ \hline 1 & 0 & 0 \\ \hline 0 & 0 & 1 \end{array} \right\| = (b, a, c).$$

We have an *elementary matrix* (3 x 3) with one 1 in each row and column and zeros elsewhere, which represents the permutation.

A general permutation of 2^n objects may be represented by a n-hyperintricate number. This is because *any* $2^n \times 2^n$ matrix has a unique n-hyperintricate representation. *Thus a 3-hyperintricate number (8 x 8 matrix) may faithfully represent the permutations of 5 objects.*

To go back to the issue of commutativity again, which we need for our solution of the matrix quintic, we note that a real plus imaginary, a real plus actual and a real plus phantom number are on their own commutative. However, in any non-trivial combination, they are non-commutative. So the question I will raise and answer, but not rigorously, is that if I choose, say, the *real plus actual* combination, then a general intricate, extended to hyperintricate, matrix that commutes with everything is of the form

$$\left\| \begin{array}{c|c|c|c|c} c_{11} & 0 & 0 & 0 & \dots \\ \hline 0 & c_{22} & 0 & 0 & \dots \\ \hline 0 & 0 & c_{33} & 0 & \dots \\ \hline \dots & & & & \\ \hline 0 & 0 & 0 & \dots & c_{nn} \end{array} \right\|$$

where the c_{rr} are real or natural number entries. Call this matrix C . Then C commutes with any permutation of the symmetric group. We have the additional observation that any permutation commutes with its inverse. Combine these two conditions together and we have a general commutativity relation.

In order to *solve* this quintic, I then need a normal series

$$S_5 \supset A_5 \supset 1,$$

which is provided by my 3-hyperintricate numbers.

I then need to be able to solve the *non-commutative* (even in A, B, C, D and E) polynomial representing A_5 , which does not have abelian factor groups (it is non-commutative). So in the traditional terminology, it is insoluble. My claim, which if I am successful, future work must substantiate, is that the designation in this case is insecure: the polynomial in A_5 is *solvable* via hyperintricate numbers.

To go back to reducibility again, I claim the quintic is reducible over $\mathbb{H}[\omega']$, where ω' are 3-hyperintricate roots of unity.

How does this fit in with traditional group theory? Well, the quaternions are equivalent to a certain 4 x 4 matrix algebra. The generalisation of these is the spinors in higher dimensions. Also, when we go up further, we come across the octonions, which are non-associative. However, these are related to Lie groups which are associative – namely the exceptional Lie groups E_6 , E_7 and E_8 . So, basically, my claim is that the quintic (and the septic) can be solved using one of these groups. It would be nicer (and easier) if we were able to use the spinors.

If you want to get involved in this, I would caution that we are probably not dealing with a substitution theory. My experience is that you can substitute one variable for another until you are blue in the face, and will not get a quintic solution. In my work on the Galois theory of non-commutative fields, I actually use substitutions, in equating hyperintricate parts, but this means we are left with a real equation in real variables, which is therefore insoluble by these methods, and also the hyperintricate parts conditions exhaust all the available variables, so there are not enough degrees of freedom to come up with a completely innovative solution.

Nevertheless it would be interesting and not difficult to see whether the cubic, for instance, is solvable via substitutions of hyperintricate numbers, in a similar way that the quadratic is with intricate numbers. However, the quarternions, which are a subalgebra of the 2-hyperintricates, do not yield results beyond that obtained in the Galois theory of non-commutative fields, which seems to rule out solutions to the quintic reduced just to spinor solutions. The calculation is as follows.

Let $x = a1 + bi + cj + dk$ be a quaternion. Then if

$$x^3 + Px + Q = 0,$$

equating real and quaternionic parts

$$(a^3 - 3ab^2 - 3ac^2 - 3ad^2) + Pa + Q = 0$$

$$(-b^3 + 3a^2b + Pb)i = 0$$

$$(-c^3 + 3a^2c + Pc)j = 0$$

and

$$(-d^3 + 3a^2d + Pd)k = 0.$$

Thus if b, c and $d \neq 0$, then $b = \pm c = \pm d$, and the real part reduces to a standard cubic.

Usually what you need, for example for the cubic, if you are killing central terms, is to introduce a quadratic equation, for which you have a solution. Thus, in finding a solution by hyperintricate radicals, the normal series condition may be essential.

If you want to avoid the normal series conditions, say by finding a solution directly by perturbation methods, this may be possible, but the solution will be transcendental, not a solution by complex radicals.

The penultimate thing I want to mention for the moment is *generators* for symmetric group elements. In our matrix notation I mention two generators which in combination give the full symmetric group on five objects. These are the *swap* matrix

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

and the *cyclic generator*

$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Every permutation may be built out of two hyperintricately representable matrices of types similar to these.

Here is an example of swapping two non-contiguous elements (2 and 4) of the permutations of (12345) using a swap on the first two elements, a full cyclic permutation and its inverse.

Identity (12345) cycle (23451) swap (32451) cycle (24513) swap (42513) reverse cycle (34251) swap (43251) reverse cycle (14325).

It is possible to generalise this example to a permutation of n objects swapping any two interior objects. A general permutation is composed of such arbitrary swaps.

However, our equations do not deal with vectors, but with roots (nevertheless, it is possible to consider equations as vector equations, for example the quadratic

$$[(x_1, x_2) + (c, d)][(x_1, x_2) + (d, c)] = 0.$$

For a swap of roots, how many transformations will swap roots just a and b ? Call M a transformation from a to b . Then there is precisely one M , and M^{-1} will transform b to a .

For a cyclic permutation, there is a series of transformations $a \rightarrow b$, $b \rightarrow c$ etc., given by M , N and so on, so that the combined operation is given by their product, call this P . Then general cyclic permutations are given by P , P^2 , etc.

Thus we have within our intricate lexicon all the transformations necessary to provide a violation of the conditions of the Abel-Ruffini theorem. These transformations are in general non-rigid.

Reference.

[1] P. Lancaster & M. Tismenetsky, *The theory of matrices*, Academic Press, (1985).