

# Re: New paper, algebraic integers, Galois Theory

Source: <http://sci.tech-archive.net/Archive/sci.math/2004-10/3035.html>

---

**From:** W. Dale Hall ([mailto:wd-hall\\_at\\_pacbell.net](mailto:wd-hall_at_pacbell.net))

**Date:** 10/10/04

Date: Sun, 10 Oct 2004 22:39:19 GMT

James Harris wrote:

> *Commented on Galois Theory at end. \_\_\_JSH*

>

>

>

-----

>

> *I. First section*

>

> *The following are in a commutative ring.*

>

> *Start with*

>

>  $P(m) = f^2 ((m^3 f^4 - 3m^2 f^2 + 3m) x^3 - 3(-1 + m f^2) x u^2 + u^3 f)$

>

> *with the factorization*

>

>  $P(m) = (a_1 x + uf)(a_2 x + uf)(a_3 x + uf)$

>

> *and note that at*

>

>  $m=0, P(0) = u^2 f^2 (3x + uf),$

>

> *which gives you terms that do not vary as m varies.*

>

> *So what about  $(a_1 x + uf)$ ,  $(a_2 x + uf)$ , and  $(a_3 x + uf)$ ?*

>

>  $(a_1 x + uf)(a_2 x + uf)(a_3 x + uf) = u^2 f^2 (3x + uf)$

>

> *which shows that at least two of the a's have to equal 0 at m=0, while*

> *one equals 3.*

>

> *Since, at m=0, two of the a's must equal 0, it's convenient to just*

> *arbitrarily select  $a_1$  and  $a_2$  as those two.*

>

> *Then you have  $uf$  for the first,  $uf$  for the second and  $3x + uf$  for the*

> *third as terms that do not vary when m varies.*

>

- > Now then, if  $m=1$ , what are the \*constant\* terms?
- >
- > They are  $uf$ , for the first,  $uf$  for the second, and  $3x + uf$  for the
- > third.
- >
- > That's logical because they do not vary with  $m$ , so if  $m=1003909273$ ,
- > what are the constant terms?
- >
- > They are  $uf$ , for the first,  $uf$  for the second, and  $3x + uf$  for the
- > third.
- >
- > Now divide  $f^2$  from both sides, which gives
- >
- >  $P(m)/f^2 = (m^3 f^4 - 3m^2 f^2 + 3m) x^3 - 3(-1 + mf^2) xu^2 + u^3 f$
- >
- >  $P(m)/f^2 = (a_1 x + uf)(a_2 x + uf)(a_3 x + uf)/f^2$
- >
- > and you note that  $P(0)/f^2 = u^2(3x + uf)$ , which means that now your
- > constant terms are  $u$  for the first,  $u$  for the second and  $3x + uf$  for
- > the third.
- >
- > Now then, if  $m=1$ , what are the constant terms now?
- >
- > They are  $u$  for the first,  $u$  for the second, and  $3x + uf$  for the third.
- >
- > If  $m = 2938479378$ , what are the constant terms now?
- >
- > They are  $u$  for the first,  $u$  for the second, and  $3x + uf$  for the third.
- >
- > How can the constant terms of the first two go from  $uf$  to  $u$ ?
- >
- > They must be divided by  $f$ .
- >
- > Now, the constant term of  $a_1 x + uf$ , is  $uf$ , but when  $f^2$  is divided
- > from  $P(m)$ , it is  $u$ ; therefore,  $a_1 x + uf$  is divided by  $f$ , and you
- > have
- >
- >  $a_1 x/f + u$
- >
- > and the constant term of  $a_2 x + uf$  is  $uf$ , but when  $f^2$  is divided
- > from  $P(m)$ , it is  $u$ ; therefore,  $a_2 x + uf$  is divided by  $f$ , and you
- > have
- >
- >  $a_2 x/f + u$
- >
- > while the constant term of  $a_3 x + uf$  is  $3x + uf$ , and after  $f^2$  is
- > divided off, it is  $3x + uf$ , so you have
- >
- >  $a_3 x + uf$
- >
- > so, dividing  $P(m)$  by  $f^2$  gives

>  
 >  $P(m)/f^2 = (a_1 x/f + u)(a_2 x/f + u)(a_3 x + uf)$ .  
 >  
 >  
 >  
 > *II. Second section*  
 >  
 > *Now take*  
 >  
 >  $P(m)/f^2 = (a_1 x/f + u)(a_2 x/f + u)(a_3 x + uf)$   
 >  
 > *and multiply inside the parentheses by  $f^2/(a_1 a_2 a_3)$ , and outside*  
 > *by  $f^2(a_1 a_2 a_3)$  and you have*  
 >  
 >  $P(m)/f^2 = ((a_1 a_2 a_3)/f^2)(x + uf/a_1)(x + uf/a_2)(x + uf/a_3)$   
 >  
 > *and since  $a_1 a_2 a_3 = f^2(m^3 f^4 - 3m^2 f^2 + 3m)$ , that is*  
 >  
 >  $P(m)/f^2 =$   
 >  
 >  $(m^3 f^4 - 3m^2 f^2 + 3m)(x + uf/a_1)(x + uf/a_2)(x + uf/a_3)$ .  
 >  
 >  
 > *Now consider the case that  $m, f$ , and  $u$  are algebraic integers, then  $I$*   
 > *have the ratios of algebraic integers:*  
 >  
 >  $uf/a_1, uf/a_2$ , and  $uf/a_3$ ,  
 >  
 > *and now let*  
 >  
 >  $v_1/w_1 = uf/a_1, v_2/w_2 = uf/a_2$ , and  $v_3/w_3 = uf/a_3$   
 >  
 > *where the  $v$ 's and  $w$ 's are algebraic integers in each case coprime to*  
 > *each other.*  
 >  
 > *Making the substitutions I have*  
 >  
 >  $P(m)/f^2 =$   
 >  
 >  $(m^3 f^4 - 3m^2 f^2 + 3m)(x + v_1/w_1)(x + v_2/w_2)(x + v_3/w_3)$ .  
 >  
 > *And I have from before that*  
 >  
 >  $P(m)/f^2 = (m^3 f^4 - 3m^2 f^2 + 3m) x^3 - 3(-1 + mf^2) xu^2 + u^3 f$   
 >  
 > *so*  
 >  
 >  $(m^3 f^4 - 3m^2 f^2 + 3m)(v_1 v_2 v_3)/(w_1 w_2 w_3) = f$   
 >  
 > *as that is the last coefficient from the last term  $u^3 f$ , which proves*  
 > *that*

>  
>  $(m^3 f^4 - 3m^2 f^2 + 3m)$  has  $w_1, w_2$  and  $w_3$  as factors, so let  
>  
>  $(m^3 f^4 - 3m^2 f^2 + 3m) = w_1 w_2 w_3$   
>  
> then I have  
>  
>  $P(m)/f^2 = (w_1 x + v_1)(w_2 x + v_2)(w_3 x + v_3)$   
>  
> but I still have that  
>  
>  $P(m)/f^2 = (a_1 x/f + u)(a_2 x/f + u)(a_3 x + uf)$ .  
>  
>  
>  
> III. Third section  
>  
> So, even if  $a_1/f$  is not an algebraic integer, you can find  $w_1$  an  
> algebraic integer.  
>  
> But if  $a_1/f$  is an algebraic integer and  $w_1$  is not, they cannot be  
> equal.  
>  
> But I have  
>  
>  $P(m)/f^2 = (w_1 x + v_1)(w_2 x + v_2)(w_3 x + v_3)$   
>  
> and  
>  
>  $P(m)/f^2 = (a_1 x/f + u)(a_2 x/f + u)(a_3 x + uf)$   
>  
> so how do you reconcile a case where  $a_1 x/f$  is not an algebraic  
> integer?  
>  
> There must exist  $z_1, z_2,$  and  $z_3$  such that  
>  
>  $w_1 = (a_1 x z_1)/f, w_2 = (a_2 x z_2)/f$  and  $w_3 = a_3 x z_3$   
>  
> and  $z_1 z_2 z_3 = 1,$   
>  
> so algebraically the  $z$ 's are units, but  $z_1, z_2$  and  $z_3$  are not units  
> in the ring of algebraic integers, if  $a_1/f$  is not.  
>  
> I've often faced arguments over the result from Section 1, and at  
> times I've dealt with people claiming that Galois Theory proves  
> something about the factors of roots of monic polynomials with integer  
> coefficients.  
>  
> The basic claim is that *each* of the roots of a monic polynomial with  
> integer coefficients that is irreducible over rationals must share  
> non-unit factors with ALL of the prime factors of the last

> *coefficient.*  
>

Note that this claim does not require Galois Theory, and is easily proven using the very basic results of field theory, together with the elementary properties of the integers. Briefly stated, one takes such a polynomial  $P$  (i.e., monic integral polynomial, irreducible over rationals) and constructs the field  $Q(a)$ , where  $a$  is a root of  $P$ . This is done without reference to which root " $a$ " really is, and as a result, one finds that the two field extensions  $Q(a)$  and  $Q(b)$ , where  $a$  and  $b$  are distinct roots of  $P$ , are isomorphic in such a way that the elements of  $Q$  are held fixed.

In particular, the ring of integers in  $Q$  is held fixed, and further:

\*anything you can express\* using arithmetic operations and integers and the root " $a$ " can be rewritten \*simply by replacing all occurrences of the symbol " $a$ " with the symbol " $b$ "\* to yield an equivalent statement about the root " $b$ ".

This directly implies that if  $k$  is an integer, then if " $a$ " and  $k$  are coprime, so are " $b$ " and  $k$ . Why? Because if " $a$ " and  $k$  are coprime, I can find polynomials  $A$ ,  $B$ , and  $C$ , with integer coefficients, such that

$$A(x)*x + B(x)*k = C(x)*P(x) + 1.$$

If this is true, then I can substitute " $b$ " in for the variable  $x$  in that equation, and find integers  $u, v$  in  $Q(b)$  for which

$$u b + v k = 1.$$

No Galois Theory, no fancy dancing with field extensions, no Galois group. Just a pair of field extensions that we can prove directly are isomorphic, fixing the field of rationals (and its ring of integers).

> *For instance, with  $P(x) = x^2 + x + 6$ , the claim would be that the two*  
> *roots:*  
>  
>  *$(-1 + \sqrt{32})/2$  and  $(-1 - \sqrt{32})/2$*   
>

Um, the roots of  $P(x)$  are given by the quadratic formula:

For the equation

$$ax^2 + bx + c = 0$$

the roots are given by the formula

$$x = (-b \pm \sqrt{b^2 - 4ac})/2a$$

Here, we have  $a = 1$ ,  $b = 1$ ,  $c = 6$ .

The discriminant is  $b^2 - 4ac = 1 - 4 \cdot 1 \cdot 6 = 1 - 24 = -23$

So the roots are

$$x = (-1 \pm \sqrt{-23})/2$$

Not, as you have incorrectly written,

$$> (-1 + \sqrt{32})/2 \text{ and } (-1 - \sqrt{32})/2$$

> *would, supposedly, each have to share non-unit factors with 2 and 3.*

>

So, let's see about this. Does each share a factor with 2 and 3?

Let  $r$  be either of these roots. Note that the numbers

$$g = -(r + 2)$$

$$h = r - 1$$

$$k = 2r + 3$$

are algebraic integers, and that

$$\begin{aligned} g h &= -(r+2)(r-1) = 2 - r - r^2 \\ &= 2 - (r^2 + r) = 2 - (-6) = 8, \end{aligned}$$

and

$$\begin{aligned} g k &= -(r + 2)(2r + 3) \\ &= -(2r^2 + 7r + 6) \\ &= -2r^2 - 7r - 6 \\ &= -2(-r - 6) - 7r - 6 \\ &= 2r + 12 - 7r - 6 \end{aligned}$$

So,

$$g k = -5r + 6.$$

But, since  $r^2 = -r - 6$ , we have

$$\begin{aligned} r^3 &= -r^2 - 6r \\ &= -(-r - 6) - 6r \\ &= r + 6 - 6r = -5r + 6. \end{aligned}$$

Thus,  $gk = r^3$ .

In other words, the numbers  $g, h, k$  are all algebraic integers, and satisfy

$$\begin{aligned} gh &= 2^3, \\ gk &= r^3. \end{aligned}$$

If we take cube roots

$$\begin{aligned}u^3 &= g, \\v^3 &= h, \\w^3 &= r,\end{aligned}$$

we'll have algebraic integers  $u, v, w$  with

$$\begin{aligned}uv &= 2 \\uw &= r.\end{aligned}$$

A similar exercise yields common algebraic integer divisors for  $r$  and  $3$ . In this case, instead of the above choices of  $g, h, k$ , one uses the following:

$$\begin{aligned}g &= -2r - 3 \\h &= 2r - 1 \\k &= r + 2.\end{aligned}$$

and one obtains

$$\begin{aligned}gh &= 3^3 \\gk &= r^3.\end{aligned}$$

I'll leave the details up to the reader, since I'm tired of typing all this stuff in. You will need to take cube roots again, as the ideals  $\langle r, 2 \rangle$  and  $\langle r, 3 \rangle$  are both of order 3 in the ideal class group of the extension  $\mathbb{Q}(r)$ .

> My works shows that it's possible that actually neither does and you  
> have to check using advanced polynomial factorization techniques.  
>

Sorry, wrong answer.

> Faced with the algebra, certain people simply claimed that Galois  
> Theory *\*forces\** that result, when in fact, it does not.  
>

Oh, really? Why does elementary field theory force it to be the case, then?

Where is your "fact", anyhow? All you're doing is making baseless assertions, unsupported by *\*any\** evidence. Show an example, why don't you? I mean an *\*actual example\**, with numbers for the coefficients, and a *\*specific\** claim.

> That's kind of obvious as consider  
>  
>  $P(x) = x^2 + 5x + 6 = (x+2)(x+3)$   
>

> *and if Galois Theory forced the previous on irrationals, why wouldn't*  
> *it force it on rationals as well?*  
>

You still haven't gotten it through that thick skull that reducibility makes a real difference, have you?

The fact that the polynomial splits already means that the factors can be independent in  $\mathbb{Q}[x]$ . If the polynomial  $P$  is irreducible in  $\mathbb{Q}[x]$ , then  $\langle P \rangle$ , the ideal it generates in  $\mathbb{Q}[x]$ , is prime;  $\mathbb{Q}[x]$  is of dimension one, so nonzero prime ideals are maximal, thus  $\mathbb{Q}[x]/\langle P \rangle$  forms a field. In this field, which contains a canonical copy of  $\mathbb{Q}$  itself, the class represented by  $x + \langle P \rangle$  is a root of the polynomial  $P(x)$ .

You might note that this "formal" extension of  $\mathbb{Q}$  doesn't really depend on which root you are considering. It shows the arithmetic properties of  $\mathbb{Q}(a)$  for *any* root of the irreducible polynomial  $P$ .

The same thing just does not hold for a reducible polynomial  $P$ . For one thing, the construction above just does not produce a field. When you perform that construction using a reducible polynomial, you actually introduce zero-divisors and destroy any likelihood of reaching a field until those zero-divisors are eliminated.

> *It doesn't force anything on either. They were just wrong.*  
>

Please show my error in the arithmetic regarding the quadratic equation above, fool.

>  
> *James Harris*

The more you imagine you can fool anyone with your meaningless blathering about stuff you clearly know nothing about, the less likely it is that you'll ever get to a point of knowledge.

What's the real problem with sitting down and *learning* something? Are you mentally deficient? Scared? Too proud of your own ignorance and too ashamed of your own shortcomings?

Dale