

# Re: Another Galois theory problem

---

*Source:* <http://sci.tech-archive.net/Archive/sci.math/2006-07/msg02195.html>

---

- *From:* "magidin@xxxxxxxxxxxxxxxxxxxx" <magidin@xxxxxxxxxxxxxxxxxxxx>
  - *Date:* 11 Jul 2006 22:31:48 -0700
- 

Doug B wrote:

Hi, I am trying to show that a field of characteristic  $p > 0$  is perfect iff it has the property that every element has a  $p$ th root (the definition of perfect field I have is, "F is perfect if every algebraic extension is separable").

I don't really know how to proceed either direction. I've had the most luck proving if it is perfect, it has the  $p$ th root property. I do this by supposing it does not. Then there's an  $a$  such that  $x^p - a$  has no roots. I take a splitting field and, enlarging it if necessary, assume it is an algebraic extension.

That last statement makes no sense whatsoever. A splitting field of a (set of) polynomials over  $F$  is  $\rightarrow$ necessarily $\leftarrow$  an algebraic extension! It is generated by adjoining roots of polynomials, and therefore it is generated over  $F$  by algebraic elements; hence the extension must be algebraic. So why are you saying that you are "enlarging it if necessary" to make it algebraic? Methinks you are missing some very important and basic facts about field extensions!

There,  $x^p - a$  splits, so pick  $r$  with  $r^p = a$ . Then what I \*WANT\* to write is  $(x-r)^p = x^p - r^p = x^p - a$ ,

This follows trivially from the fact that the characteristic is  $p$ . The coefficient of  $x^i$  in the expansion of  $(x-r)^p$  is  $\binom{p}{i} r^{p-i}$ , which is a multiple of  $p$  for all  $i$ ,  $0 < i < p$ .

so  
that  $r$  is a multiple root of  $x^p - a$ , contradiction.

## Re: Another Galois theory problem

Indeed. See below.

But this is not rigorous, since in fields of characteristic  $>0$ , just because two polynomials agree everywhere does not imply they are the same polynomials.

Just multiply out  $(x-r)^p$ . Don't know why you are trying to evaluate anything.

(By the way: it  $\rightarrow$ is $\leftarrow$  true for polynomials of degree less than  $\text{char}(F)$ , though that is neither here nor there in this situation)

So even though the polynomials  $x^p-a$  and  $(x-r)^p$  agree everywhere, I don't know how to show they are the same polynomials, if indeed they even are.

Yes,. they are. Just write out  $(x-r)^p$  and remember the characteristic is  $p$ .

Also, I am implicitly assuming here that  $x^p-a$  is irreducible, otherwise even if I could show it has multiple roots in a splitting field, that would prove nothing.

Think minimal polynomial: the minimal polynomial of  $r$  over  $F$  must divide  $x^p-a$ . Since  $x^p-a$  is equal to  $(x-r)^p$ , then the minimal polynomial of  $r$  over  $F$  must be of the form  $(x-r)^k$  for some  $k$ ,  $0 < k \leq p$ . If  $k > 1$ , then this gives you the inseparability, and if  $k=1$ , that tells you that  $a$  already had a  $p$ -th root in  $F$ , which contradicts your choice of  $a$ .

But I have no idea how to show that  $x^p-a$  is even irreducible in the original field.

You don't have to (although it will be, since it will turn out that for an irreducible polynomial to be inseparable, it must be of the form  $g(x^p)$  for some polynomial  $g$ ).

And all this is just one direction of the statement, the other direction I have

Re: Another Galois theory problem

even less of a clue how to proceed...

If every algebraic extension is separable, let  $a$  in  $F$  and consider the polynomial  $x^p - a$ . Let  $r$  be a root, and consider  $F(r)$ . Now argue as above about what the minimal polynomial of  $r$  must look like, and use the fact that the extension is separable to deduce that  $r$  is already in  $F$ .

Arturo Magidin. sans .sig

.