

Re: Galois Field

Source: <http://sci.tech-archive.net/Archive/sci.math/2005-10/msg00514.html>

- *From:* barr@xxxxxxxxx
 - *Date:* 6 Oct 2005 09:57:24 -0700
-

Jyrki Lahtonen wrote:

> Arturo Magidin wrote:

>> In article <yU71f.327\$2i4.115@xxxxxxxxxxxxxxxxxx>,

>> Ricky R. <noemail@xxxxxxxxxxxx> wrote:

>>

>>>I have to show that $GF(125)$ is a splitting field for $p(x) = x^3+x+1$ over

>>> $GF(5)$. I need a hint.

>>

>>

>> You know that it has a root over $GF(125)$, since it is irreducible over

>> $GF(5)$. All you need to do is show that the resulting quadratic also

>> has its roots there; and for that, you just need to show that a

>> certain discriminant is a square in $GF(125)$.

>>

>

> Actually I don't think all of that is necessary, if you know

> a little bit of Galois theory. The Galois group of the

> splitting field (over the prime field) is known to be a

> transitive permutation group of the three roots of the

> irreducible cubic. All the extensions of finite fields have

> cyclic Galois groups, so...

>

> Cheers,

>

> Jyrki Lahtonen, Turku, Finland

To continue this post, let me point out that it is a standard result that every finite extension of a finite field is a Galois extension (normal and separable). That means that when you adjoin one root, you get them all. Now if you take an irreducible polynomial of degree k over a field of q elements, when you adjoin one root you get a field of order q^k in which the polynomial splits. In this case, your polynomial either has three roots, one root or no roots in $GF(5)$. In the first case, the splitting field is $GF(5)$; in the second $GF(25)$ and in the third $GF(125)$.

.

- **References:**

- ◆ **Re: Galois Field**

- ◇ *From:* Arturo Magidin

- Prev by Date: **Correlation coefficient: proving it's between -1 and 1**

- Next by Date: **Re: Missing equality operator**

- Previous by thread: **Re: Galois Field**

- Next by thread: **Re: sequentially complete spaces**

- Index(es):

- ◆ **Date**

- ◆ **Thread**