Re: algebra with finite field and isomorphic.

Source: http://sci.tech−archive.net/Archive/sci.math/2006−09/msg00334.html

---

- *From*: mareg@xxxxxxxxxxxxxxxxxxxxxxxxx ()

- *Date*: Sat, 2 Sep 2006 11:30:55 +0000 (UTC)

In article <edb4avlra1@xxxxxxxxxxxxxxxx>,
"mina_world" <mina_world@xxxxxxxxxxx> writes:

> hello sir~
>
> show that two finite fields of the same order p^n
> are isomorphic.
>
> [hint : let p(x) in Z_p[x] be irreducible of degree n.
> show every field of p^n elements is isomorphic
> to Z_p[x]/<p(x)>.]
>
> −−
> yes, i try it.
> i had three questions.
>
> proof 1)
>
> lemma 1) The multiplicative group <F^*,.> of
> nonzero elements of a finite field F is cyclic.
>
> Let F and F' be two finite fields of the order p^n.
>
> These fields must have characteristic p, for a prime p,
> so, they contain Z_p as a subfield.
>
> by lemma 1, unit group of F is cyclic.
> so, F^* = <a>. namely "a" is a generator.
> so, F = Z_p(a) is a finite extension of Z_p.
> so, F = Z_p(a) is a algebraic extension and simple extension.
>
> since "a" is algebraic over Z_p,
> let f(x) be the minimal(irreducible) polynomial of "a" over Z_p.
>
> so, F = Z_p(a) ~ Z_p[x]/<f(x)>.
>
> the elements of F and F' are exactly the roots of
> the polynomial h(x) = x^p^n −x.
> since a in F, h(a) = 0.

so, f(x) is one of the irreducible factors of h(x).
so, there exists "b" in F' such that f(b) = 0.

since "b" is algebraic over Z_p
so, Z_p(b) ~ Z_p[x]/<f(x)>.

but i mush show that F' = Z_p(b).
i can't this. how do you show it ?

b is a root of the irreducible polynomial f of degree n over Z_p,
so the extension Z_p(b) has degree n over Z_p, so |Z_p(b)| = p^n = |F'|.

−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−−
proof 2)

the elements of F and F' are exactly the roots of
the polynomial h(x) = x^p^n −x.

so, F = F'
thus, isomorphic.

is this a foolish thinking ?

i think that it means that
F=F' is unique splitting field of [x^p^n −x] over Z_p.
no ?

It is not necessarily true that F = F', but this argument is basically correct.
F and F' consist of the p^n roots of x^p^n − x, so they must both be splitting
fields of x^p^n − x over Z_p. Now there is a theorem which says that any two
splitting fields of an irreducible polynomial over a field are isomorphic, so
it follows from that theorem that F and F' are isomorphic.

−−
proof 3)

anyway, i don't use the hint.
[hint : let p(x) in Z_p[x] be irreducible of degree n.
show every field of p^n elements is isomorphic
to Z_p[x]/<p(x)>.]

i want to prove with hint.
so, i need your advice.

I think the hint is very unhelpful! In order to use the hint, you first have
to prove that there exists an irreducible polynomial of degree n over Z_p,

which is by no means trivial.

Derek Holt.

i also need the advice of Arturo Magidin.

.