

algebra with finite field and isomorphic.

Source: <http://sci.tech-archive.net/Archive/sci.math/2006-09/msg00303.html>

- *From:* "mina_world" <mina_world@xxxxxxxxxxx>
 - *Date:* Sat, 2 Sep 2006 14:23:33 +0900
-

hello sir~

show that two finite fields of the same order p^n are isomorphic.

[hint : let $p(x)$ in $\mathbb{Z}_p[x]$ be irreducible of degree n . show every field of p^n elements is isomorphic to $\mathbb{Z}_p[x]/\langle p(x) \rangle$.]

yes, i try it.
i had three questions.

proof 1)

lemma 1) The multiplicative group $\langle F^*, \cdot \rangle$ 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 \mathbb{Z}_p as a subfield.

by lemma 1, unit group of F is cyclic.
so, $F^* = \langle a \rangle$. namely " a " is a generator.
so, $F = \mathbb{Z}_p(a)$ is a finite extension of \mathbb{Z}_p .
so, $F = \mathbb{Z}_p(a)$ is an algebraic extension and simple extension.

since " a " is algebraic over \mathbb{Z}_p ,
let $f(x)$ be the minimal(irreducible) polynomial of " a " over \mathbb{Z}_p .

so, $F = \mathbb{Z}_p(a) \sim \mathbb{Z}_p[x]/\langle f(x) \rangle$.

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 $f(b) = 0$.

algebra with finite field and isomorphic.

since "b" is algebraic over Z_p
so, $Z_p(b) \sim Z_p[x]/\langle f(x) \rangle$.

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

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 ?

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 $Z_p[x]/\langle p(x) \rangle$.]

i want to prove with hint.
so, i need your advice.
i also need the advice of Arturo Magidin.