

Re: algebra with finite field and isomorphic.

Re: algebra with finite field and isomorphic.

Source: <http://sci.tech-archive.net/Archive/sci.math/2006-09/msg00520.html>

- *From:* "mina_world" <mina_world@xxxxxxxxxxx>
 - *Date:* Sun, 3 Sep 2006 19:34:42 +0900
-

"mina_world" <mina_world@xxxxxxxxxxx> wrote in message
[news:ede0on\\$omj\\$1@xxxxxxxxxxxxxxxxxxxxxxxx](mailto:news:ede0onomj1@xxxxxxxxxxxxxxxxxxxxxxxx)

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

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 Z_p as a
subfield.

Re: algebra with finite field and isomorphic.

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 a 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 $f(b) = 0$.

since "b" is algebraic over
 \mathbb{Z}_p
so, $\mathbb{Z}_p(b) \sim \mathbb{Z}_p[x]/\langle f(x) \rangle$.

but i must show that $F' =$
 $\mathbb{Z}_p(b)$.
i can't this. how do you
show it ?

b is a root of the irreducible polynomial f of
degree n over \mathbb{Z}_p ,

why ?

Which part of the assertion are you querying?
You have already said that f is irreducible.
You have already said that $f(b) = 0$, so b is a root of f.
And f has degree n because $F = \mathbb{F}_p(a)$ with $|F| = p^n$ and "a" a root of

Re: algebra with finite field and isomorphic.

f.

yes, so, $|Z_p(b)| = p^n = |F|$.
and $Z_p(b)$ in F
how do you show that F in $Z_p(b)$?

um...It was silly of me.
it's trivial...so, $F = Z_p(b)$.

i try again with hint.

let F be finite field of the order p^n .
 F contain Z_p as a subfield.

let $p(x)$ in $Z_p[x]$ be irreducible of degree n .
so, there exists "a" in algebraic closure of Z_p such that
 $p(a) = 0$.

since "a" is algebraic over Z_p ,
 $Z_p(a) \sim Z_p[x]/\langle p(x) \rangle$.

since the basis of $Z_p[x]/\langle p(x) \rangle$ is $\{1, a, a^2, \dots, a^{n-1}\}$,
 $|Z_p[x]/\langle p(x) \rangle| = p^n$.

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

maybe, i think that it's impossible solution.
but It is doubtful that this hint is a mistake of Fraleigh book.

anyway, thank you very much for your advice.

.