

Re: Algebra with root and $Z_2[x]$.

Source: <http://sci.tech-archive.net/Archive/sci.math/2007-11/msg04566.html>

- *From:* José Carlos Santos <jcsantos@xxxxxxxx>
 - *Date:* Fri, 23 Nov 2007 14:40:10 +0000
-

On 23-11-2007 9:07, mina_world wrote:

Prove that every polynomial of degree 1, 2, or 4 in $Z_2[x]$ has a root in $Z_2[x] / \langle x^4 + x + 1 \rangle$.

 $x^4 + x + 1$ is irreducible over Z_2 .

By Kronecker, $x^4 + x + 1$ has a root in $Z_2[x] / \langle x^4 + x + 1 \rangle$.

Anyway, this is not useful in my problem.

Let $f(x) = x + a$ in $Z_2[x]$.

a is 0 or 1.

so, $f(x)$ has a root in Z_2 .

Let $f(x) = x^2 + ax + b$ in $Z_2[x]$.

Sorry. I can't progress any more.

so, I need your advice.

You have four possibilities: $f(x) = x^2$, $f(x) = x^2 + x$, $f(x) = x^2 + 1$, and $f(x) = x^2 + x + 1$. The first three have a root in Z_2 already. Now, take $a = [x]$ in $Z_2[x] / \langle x^4 + x + 1 \rangle$. Then

$$a^2 + a + 1 = [x^2 + x + 1]$$

and therefore

$$(a^2 + a + 1)^2 = [x^4 + x^2 + 1] = [x^2 + x] = (a^2 + a + 1) + 1.$$

So, $a^2 + a + 1$ is a root of $x^2 + x + 1$ in $Z_2[x] / \langle x^4 + x + 1 \rangle$.

Now, try the same approach with fourth degree polynomials.

Oh, good idea.

With fourth degree...

I have 16 possibilities.

I must examine 4 cases among 16 possibilities.

Re: Algebra with root and $Z_2[x]$.

Namely, $f(x) = x^4 + x^3 + 1$, $x^4 + x^2 + 1$, $x^4 + x + 1$,
 $x^4 + x^3 + x^2 + x + 1$.

Indeed.

If $f(x) = x^4 + x + 1$, $f(x)$ has a root in $Z_2[x] / \langle x^4 + x + 1 \rangle$ by Kronecker.
so, I must examine 3 cases.

Anyway,

If $f(x) = x^4 + x^3 + 1$,

Let $a = 1 + \langle x^4 + x + 1 \rangle$. $f(a)$ not in $\langle x^4 + x + 1 \rangle$. then a is not root of $f(x)$.

Let $a = x + \langle x^4 + x + 1 \rangle$. $f(a)$ not in $\langle x^4 + x + 1 \rangle$. then a is not root of $f(x)$.

Let $a = (x + 1) + \langle x^4 + x + 1 \rangle$. $f(a)$ not in $\langle x^4 + x + 1 \rangle$. then a is not root of $f(x)$.

Let $a = x^2 + \langle x^4 + x + 1 \rangle$. $f(a)$ not in $\langle x^4 + x + 1 \rangle$. then a is not root of $f(x)$.

Let $a = x + \langle x^4 + x + 1 \rangle$. Then $a^4 + a + 1 = 0$, and, since a is not
0,

$$a^4(1 + 1/a^3 + 1/a^4) = 0 \Leftrightarrow 1 + 1/a^3 + 1/a^4$$

$$\Leftrightarrow (1/a)^4 + (1/a)^3 + 1 = 0.$$

So, $1/a$ is a root of $x^4 + x^3 + 1 = 0$.

Best regards,

Jose Carlos Santos

.