

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

---

*Source:* <http://sci.tech-archive.net/Archive/sci.math/2007-11/msg04521.html>

---

- *From:* José Carlos Santos <[jcsantos@xxxxxxxx](mailto:jcsantos@xxxxxxxx)>
  - *Date:* Fri, 23 Nov 2007 07:54:21 +0000
- 

On 23-11-2007 7:06, 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  $f(x) = x^2 + a.x + b$  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.

Best regards,

Jose Carlos Santos

.