A Book of Abstract Algebra | (2nd Edition)

Chapter 27, Problem 4EC   Bookmark   Show all steps: ON

Problem

Let $p(x)$ be an irreducible polynomial of degree n over F. Let c denote a root of $p(x)$ in some extension of F (as in the basic theorem on field extensions).

Using part 3, explain why there are exactly four elements in $\mathbb{Z}_2[x]/\langle x^2+x+1\rangle$. List these four elements, and give their addition and multiplication tables. {HINT: Identify $\mathbb{Z}_2[x]/\langle x^2+x+1\rangle$ with $\mathbb{Z}_2(c)$, where c is a root of x^2+x+1. Write the elements of $\mathbb{Z}_2(c)$ as in part 3. When computing the multiplication table, use the fact that $c^2+c+1=0$.}

Step-by-step solution

Step 1 of 3

Objective is to determine the elements of $Z_2[x]/\langle x^2+x+1\rangle$ with their addition and multiplication tables.

The elements of $Z_2[x]/\langle x^2+x+1\rangle$ has the following form:

$$\frac{Z_2[x]}{\langle x^2+x+1\rangle}=\{ax+b+\langle x^2+x+1\rangle : a,b\in Z_2\}.$$

The polynomial is linear because all higher degree polynomials will get absorb by $\langle x^2+x+1\rangle$.
Since $a,b\in Z_2$, so both have only 2 choices. Thus, there are only 4 elements.

Comments (1)

Step 2 of 3

And the elements will be $0x+0, 0x+1, x+0, x+1$, or

$$\frac{Z_2[x]}{\langle x^2+x+1\rangle}=\{0,1,x,x+1\}.$$

From part 3, the elements of $Z_2[c]$ are $0,1,c,c+1$, where $c^2+c+1=0$.

For the addition table use the condition that $2\equiv 0$ in Z_2.

$+$	0	1	c	$c+1$
0	0	1	c	$c+1$
1	1	$2\equiv 0$	$c+1$	$c+2\equiv 0$
c	c	$c+1$	$2c\equiv 0$	$2c+1\equiv 1$
$c+1$	$c+1$	$c+2\equiv c$	1	$2c+c\equiv 0$

Comment

Step 3 of 3

For multiplication table, use $-1\equiv 1$ in Z_2 and $c^2+c+1=0$:

$\cdot$	0	1	c	$c+1$
0	0	0	0	0
1	0	1	c	$c+1$
c	0	c	$c^2\equiv c+1$	$c^2+c\equiv 1$
$c+1$	0	$c+1$	$c^2+c\equiv 1$	$c^2+2c+1\equiv c$

Comment