# A Book of Abstract Algebra | (2nd Edition)

Chapter 27, Problem 5EC | 1 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).

Describe $Z_2[x]/\langle x^3 + x + 1\rangle$, as in part 4.

## Step-by-step solution

**Step 1** of 3

Objective is to determine the elements of $Z_2[x]/\langle x^3+x+1\rangle$ with their addition and multiplication tables.

The elements of $Z_2[x]/\langle x^3+x+1\rangle$ has the following form:

$$\frac{Z_2[x]}{\langle x^3+x+1\rangle} = \left\{ax^2+bx+c+\langle x^3+x+1\rangle : a,b,c \in Z_2\right\}.$$

The polynomial is quadratic because all higher degree polynomials will get absorb by $\langle x^3+x+1\rangle$. Since $a,b,c \in Z_2$, so all three have only 2 choices. Thus, there are only $2^3 = 8$ elements.

Comments (2)

**Step 2** of 3

And the elements will be:

$$\frac{Z_2[x]}{\langle x^3+x+1\rangle} = \left\{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\right\}.$$

From part 3, the elements of $Z_2[c]$ are $0, 1, c, c+1, c^2, c^2+1, c^2+c, c^2+c+1$, where $c^3+c+1=0$. For the addition table use the condition that $2 \equiv 0$ in $Z_2$. Let $X = x^2+x+1$

| + | 0 | 1 | $x$ | $x+1$ | $x^2$ | $x^2+1$ | $x^2+x$ | $X$ |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 1 | $x$ | $x+1$ | $x^2$ | $x^2+1$ | $x^2+x$ | $X$ |
| 1 | 1 | $2\equiv 0$ | $x+1$ | $x$ | $x^2+1$ | $x^2$ | $X$ | $x^2+x$ |
| $x$ | $x$ | $x+1$ | 0 | 1 | $x^2+x$ | $X$ | $x^2$ | $x^2+1$ |
| $x+1$ | $x+1$ | $x$ | 1 | 0 | $X$ | $x^2+x$ | $x^2+1$ | $x^2$ |
| $x^2$ | $x^2$ | $x^2+1$ | $x^2+x$ | $X$ | 0 | 1 | $x$ | $x+1$ |
| $x^2+1$ | $x^2+1$ | $x^2$ | $X$ | $x^2+x$ | 1 | 0 | $x+1$ | $x$ |
| $x^2+x$ | $x^2+x$ | $X$ | $x^2$ | $x^2+1$ | $x$ | $x+1$ | 0 | 1 |
| $X$ | $X$ | $x^2+x$ | $x^2+1$ | $x^2$ | $x+1$ | $x$ | 1 | 0 |

Comment

**Step 3** of 3

For multiplication table, use $-1 \equiv 1$ in $Z_2$ and $x^3+x+1=0$. Then proceed as:

$$x^3 = -(x+1) \equiv x+1$$
$$x(x^2+1) = x^3+x \equiv 1$$
$$x(x^2+x) = x^3+x^2 \equiv x^2+x+1$$
$$x(x^2+x+1) = x^3+x^2+x \equiv x^2+1$$

| + | 0 | 1 | $x$ | $x+1$ | $x^2$ | $x^2+1$ | $x^2+x$ | $X$ |
|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | $x$ | $x+1$ | $x^2$ | $x^2+1$ | $x^2+x$ | $X$ |
| $x$ | 0 | $x$ | $x^2$ | $x^2+x$ | $x+1$ | 1 | $X$ | $x^2+1$ |
| $x+1$ | 0 | $x+1$ | $x^2+x$ | $x^2+1$ | $X$ | $x^2$ | 1 | $x$ |
| $x^2$ | 0 | $x^2$ | $x+1$ | $X$ | $x^2+x$ | $x$ | $x^2+1$ | 1 |
| $x^2+1$ | 0 | $x^2+1$ | 1 | $x^2$ | $x$ | $X$ | $x+1$ | $x^2+x$ |
| $x^2+x$ | 0 | $x^2+x$ | $X$ | 1 | $x^2+1$ | $x+1$ | $x$ | $x^2$ |
| $X$ | 0 | $X$ | $x^2+1$ | $x$ | 1 | $x^2+x$ | $x^2$ | $x+1$ |

where $X = x^2+x+1$.

Comment