A Book of Abstract Algebra | (2nd Edition)

Chapter 29, Problem 2EC

Bookmark

Show all steps: ON

Problem

By the proof of the basic theorem of field extensions, if $p(x)$ is an irreducible polynomial of degree n in $F[x]$, then $F[x]$, then $F[x]/\langle p(x)\rangle \cong F(c)$ where c is a root of $p(x)$. By Theorem 1 in this chapter, $F(c)$ is of degree η over F. Using the paragraph preceding Theorem 1:

Construct a field of four elements. (It is to be an extension of $\mathbb{Z}_2$.) Describe its elements, and supply its addition and multiplication tables.

Step-by-step solution

Step 1 of 2

The objective is to construct a field of four elements. Describe its elements, and supply its addition and multiplication tables.

Comment

Step 2 of 2

Let $f(x)=x^2+x+1\in {}_2[x]$.

Then $f(0)=1$ and $f(1)=1+1+1 \ =1$.

So , $f(x)$ has no zeros in ${}_2$ and thus is irreducible over ${}_2[x]$.

Then there exist an extension field E of ${}_2$containing a zero α of $f(x)$.

Since every element β of a simple extension $E=F(\alpha)$ can be uniquely expressed in the form $\beta=b_0+b_1\alpha+...+b_{n-1}\alpha^{n-1}$ where $b_i\in F$ and α is algebraic over F , ${}_2(\alpha)$ has elements $0,\ 1,\ \alpha,\ 1+\alpha.$.

This gives a field of four elements.

<u>Addition Tables: Multiplication Tables:</u>

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

$\cdot$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

Comment