

A Book of Abstract Algebra | (2nd Edition)

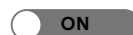


Chapter 29, Problem 3EC



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 $F[x]/\langle p(x) \rangle \cong F(c)$ where c is a root of $p(x)$. By Theorem 1 in this chapter, $F(c)$ is of degree n over F . Using the paragraph preceding Theorem 1:

Construct a field of eight elements. (It is to be an extension of \mathbb{Z}_2).

Step-by-step solution

Step 1 of 2

The objective is to construct a field of eight elements.

[Comment](#)

Step 2 of 2

Let $f(x) = x^3 + x + 1 \in \mathbb{Z}_2[x]$.

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

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

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

Since every element β of a simple extension $E = \mathbb{F}_2(\alpha)$ can be uniquely expressed in the form

$$\beta = b_0 + b_1\alpha + \dots + b_{n-1}\alpha^{n-1} \text{ where } b_i \in \mathbb{F}_2 \text{ and } \alpha \text{ is algebraic over } \mathbb{F}_2, \mathbb{F}_2(\alpha) \text{ has}$$

elements $0, 1, \alpha, \alpha^2, 1+\alpha, 1+\alpha+\alpha^2, 1+\alpha^2, \alpha+\alpha^2$.

This gives a field of eight elements.

[Comment](#)