A Book of Abstract Algebra | (2nd Edition)

Chapter 29, Problem 4EC

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:

Prove that if F has q elements, and a is algebraic over F of degree n, then $F(a)$ has q^n elements.

Step-by-step solution

Step 1 of 2

Consider a field F having q elements, and a is algebraic over F of degree n. The objective is to prove that $F(a)$ has q^n elements.

Comment

Step 2 of 2

As $F(a)$ is an F – vector space, an F – basis for $F(a)$ is the set $S=\{1,a,\dots,a^{n-1}\}$.

Thus, $F(a)=\{b_0+b_1a+b_2a^2+...+b_{n-1}a^{n-1}:b_i\in F, 0\le i\le n-1\}$.

Note that there are q choices for b_0, q choices for b_1, and in general q choices for each b_i with $0\le i\le n-1$.

In total there are $qq...q=q^n$ choices for $\{b_0,...,b_{n-1}\}$.

As every element of $F(a)$ can be uniquely expressed in this form, $F(a)$ has q^n elements.

Comment