A Book of Abstract Algebra | (2nd Edition)

Chapter 29, Problem 5EC

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 for every prime number p, there is an irreducible quadratic in $\mathbb{Z}_p[x]$. Conclude that for every prime p, there is a field with p^2 elements.

Step-by-step solution

Step 1 of 3

Objective is to prove that for every prime number p, there is an irreducible quadratic in $Z_p[x]$. Also conclude that there is a field with p^2 elements.

Suppose to the contrary that there are no irreducible quadratic polynomials in $Z_p[x]$. Then every irreducible factor of $x^{p^2}-x$ must have degree less than 2. It shows that $x^{p^2}-x$ must divide the product

$$\left(x^{p^0}-x\right)\left(x^{p^1}-x\right).$$

But the degree of this product is

$$p^0+p^1=1+p<p^2,$$

a contradiction. Thus, there is at least one irreducible polynomial of degree 2.

Comment

Step 2 of 3

Let $f(x) \in Z_p[x]$ is irreducible quadratic polynomial. Then by the theorem, $Z_p[x]/\langle f(x)\rangle$ is a field, because Z_p is a field (for prime *p*). The elements of $Z_p[x]/\langle f(x)\rangle$ will be of the form:

$$a_0 + a_1x + \langle f(x)\rangle$$

for some $a_i \in Z_p$. Since there are *p* choices for both the coefficients, therefore there are exactly p^2 such elements.

Comment

Step 3 of 3

Thus, $Z_p[x]/\langle f(x)\rangle$ is a field with p^2 elements.

Comment