A Book of Abstract Algebra | (2nd Edition)

Chapter 27, Problem 3EC | 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).

Conclude from parts 1 and 2 that every element in *F*(*c*) can be written *uniquely* as *r*(*c*), with deg *r*(*x*) < *n*.

Step-by-step solution

Step 1 of 5

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.

1. Prove: Every element in $F(c)$ can be written as $r(c)$, for some $r(x)$ of degree $<n$ in $F[x]$.

2. If $t(c)=s(c)$ in $F(c)$, where $s(x)$ and $t(x)$ have degree $<n$, prove that $t(x)=s(x)$.

Conclude from part 1 and 2 that every element in $F(c)$ can be written *uniquely* as $r(c)$, with $\deg r(x)<n$.

Comment

Step 2 of 5

First part shows that every element in $F(c)$ can be written as $r(c)$, for some $r(x)$ of degree $<n$ in $F[x]$.

Here we use "Division Algorithm".

Let $t(c)\in F(c)$ be any element. Consider $t(x)$ be any polynomial over $F(c)$.

Also, it is given that $p(x)$ is irreducible over F and c denote a root of $p(x)$ in some extension of F.

So, by division algorithm, there exists two polynomials $q(x)$ and $r(x)$ such that

$t(x)=q(x)p(x)+r(x)$, where $\deg r(x)<n$. ---------- **(i)**

Now, put $x=c$ in above expression and use the fact that c is root of $p(x)$.

Hence, $t(c)=q(c)p(c)+r(c)=r(c)$ $[\because p(c)=0]$

That is, $t(c)=r(c)$.

Hence, every element in $F(c)$ can be written as $r(c)$, for some $r(x)$ of degree $<n$ in $F[x]$.

Now it remain to conclude that this representation by $r(c)$ is unique, that is what comes from part 2.

Let $t(c)=s(c)$.

Suppose $t(x)\neq s(x)$.

By Division Algorithm, we have

$$\begin{aligned} t(x)&=q(x)p(x)+r(x)\\ s(x)&=q'(x)p(x)+r'(x)\end{aligned} \quad \text{where } \deg r(x), \deg r'(x)<n.$$

Now put $x=c$ and use the fact that $p(c)=0$.

We have, $t(c)=r(c)$ and $s(c)=r'(c)$. But $t(c)=s(c)$, therefore, $r(c)=r'(c)$.

Also by assumption,

$q(x)p(x)+r(x)\neq q'(x)p(x)+r'(x)$

$\Rightarrow q(c)p(c)+r(c)\neq q'(c)p(c)+r'(c)$

$\Rightarrow r(c)\neq r'(c)$ which is contradiction.

Comment

Step 3 of 5

Comment

Step 4 of 5

Comment

Step 5 of 5

Comment