A Book of Abstract Algebra | (2nd Edition)

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).

Prove: Every element in $F(c)$ can be written as $r(c)$, for some $r(x)$ of degree $< n$ in $F[x]$. [HINT: Given any element $t(c) \in . F(c)$, use the division algorithm to divide $t(x)$ by $p(x)$.]

Step-by-step solution

Step 1 of 3

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.

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

Comment

Step 2 of 3

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 $\deg r(x) < n$.

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, the result.

Comment

Step 3 of 3

Comment