A Book of Abstract Algebra | (2nd Edition)

Problem

Suppose $a(x) \in F[x]$, and K is an extension of F. An element $c \in K$ is called a multiple root of $a(x)$ if $(x - c)^m | a(x)$ for some $m > 1$. It is often important to know if all the roots of a polynomial are different, or not.

We now consider a method for determining whether an arbitrary polynomial $a(x) \in F[x]$ has multiple roots in any extension of F.

Let K be any field containing all the roots of $a(x)$. Suppose $a(x)$ has a multiple root c.

Show that each of the following polynomials has *no* multiple roots in any extension of its field of coefficients:

$x^3 - 7x^2 + 8 \in \mathbb{Q}[x]$ $\quad x^2 + x + 1 \in \mathbb{Z}_5[x]$ $\quad x^{100} - 1 \in \mathbb{Z}_7[x]$

The preceding example is most interesting: it shows that there are 100 *different* hundredth roots of 1 over $\mathbb{Z}_7$. (The roots ±1 are in $\mathbb{Z}_7$, while the remaining 98 roots are in extensions of $\mathbb{Z}_7$.) Corresponding results hold for most other fields.

Step-by-step solution

Step 1 of 4

Objective is to prove that following polynomials have no multiple roots in any extension of its field of coefficients.

The polynomial is $a(x) = x^3 - 7x^2 + 8 \in Q[x]$.

Consider the fact that: a polynomial $a(x)$ in $F[x]$ has a multiple root if and only if $a(x)$ and $a'(x)$ have a common factor of positive degree in $F[x]$.

Comment

Step 2 of 4

Calculate the derivative of the polynomial and get

$a'(x) = 3x^2 - 14x$.

The rational roots of derivative are $x = 0, x = 14/3$ (because $x(3x - 14) = 0$). Note that, no value of x satisfy the equation $x^3 - 7x^2 + 8 = 0$. It shows that $a(x)$ and $a'(x)$ have no common factor.

Hence, by the stated fact, $a(x)$ has no multiple roots in any extension of its field of coefficients.

Comment

Step 3 of 4

The polynomial is $a(x) = x^2 + x + 1 \in Z_5[x]$.

The derivative of this polynomial is

$a'(x) = 2x + 1$.

Check the roots of $a(x)$ in $Z_5[x]$ by simply substituting the elements of Z_5 and get,

$a(0) = 1$
$a(1) = 3$
$a(2) = 7 \equiv 2$
$a(3) = 13 \equiv 3$
$a(4) = 21 \equiv 1$.

That is, there is not root of $a(x)$ in $Z_5[x]$. Thus, $a(x)$ and $a'(x)$ cannot have any factor in common.

Comment

Step 4 of 4

The polynomial is $a(x) = x^{100} - 1 \in Z_7[x]$.

Then, $a'(x) = 100x^{99}$. Note that $x = 0$ is the only root of $a'(x)$ in $Z_7[x]$. But 0 does not satisfy $a(x)$. Therefore, both $a(x)$ and $a'(x)$ cannot have any factor in common.

Hence, $a(x)$ has no multiple roots in any extension of its field of coefficients

Comment