Math 521A

4.4 – Polynomial Functions, Roots, and Reducibility

Objective: To determine when a given polynomial is irreducible.

Throughout this section, R will denote a commutative ring. Let

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \in R[x].$$

Then $f(x)$ *induces* a function $f : R \to R$ given by

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0.$$

f is called the polynomial function induced by $f(x)$.

Let $a \in R$. If $f(a) = 0_R$, then a is called a root (or a zero) of $f(x)$.

Example

The polynomial $x^2 + x + 1 \in \mathbb{Z}_2[x]$ induces the function $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ given by $f(x) = x^2 + x + 1$. Note that $f(0) = 1$ and $f(1) = 1$.

Example

The polynomial $x^2 + 7x + \frac{1}{2} \in \mathbb{Q}[x]$ induces the function $f : \mathbb{Q} \to \mathbb{Q}$ given by $f(x) = x^2 + 7x + \frac{1}{2}$. Note that

$$f(0) = \frac{1}{2}, \quad f(1) = \frac{17}{2}, \quad f\left(\frac{-7+\sqrt{47}}{2}\right) = 0.$$

Example

The polynomial $x^2 - 2 \in \mathbb{Q}[x]$ has no roots in $\mathbb{Q}$. However, if $x^2 - 2$ is regarded as a polynomial in $\mathbb{R}[x]$, then it has $\sqrt{2}$ and $-\sqrt{2}$ as roots.

Theorem (The Remainder Theorem)

Let F be a field, $f(x) \in F[x]$, and $a \in F$. The remainder when $f(x)$ is divided by $x - a$ equals $f(a)$.

Example

i) Find the remainder when $x^4 - 3x + 1$ is divided by $x - 2$ in $\mathbb{Q}[x]$.

ii) Find the remainder when $x^{100} + 3x + 1$ is divided by $x + 1$ in $\mathbb{Q}[x]$.

Theorem (The Factor Theorem)

Let F be a field, $f(x) \in F[x]$, and $a \in F$. Then

$$a \text{ is a root of } f(x) \text{ if and only if } x - a \mid f(x).$$

Example

The Factor Theorem can be used to show that $x^{20} + x^{19} + x^{15} + x^{13} + x + 1$ is reducible in $\mathbb{Z}_2[x]$.

Corollary

Let F be a field and $f(x)$ a nonzero polynomial of degree n in $F[x]$. Then $f(x)$ has at most n roots in F.

The proof is presented on the board.

Remark (about the last result): The *Fundamental Theorem of Algebra* states that every nonzero polynomial of degree n in $\mathbb{C}[x]$ has exactly n roots, counted with multiplicity. For example, $x^2 - 2x + 1 = (x-1)^2$ has two roots in $\mathbb{C}$ ($r = 1$ is a double root).

As we saw in Section 4.3, all polynomials of degree 1 in $F[x]$ are irreducible.

Corollary

Let $f(x) \in F[x]$ with $\deg f(x) \geq 2$. If $f(x)$ is irreducible in $F[x]$ then $f(x)$ has no roots in F.

Corollary

Let $f(x) \in F[x]$ be such that $\deg f(x) = 2$ or 3. Then $f(x)$ is irreducible in $F[x]$ if and only if $f(x)$ has no roots in F.

Attention! When $\deg f(x) > 3$, the converse of the result stated in the last corollary does not hold. For example, $p(x) = x^4 + x^2 + 1$ has no roots in $\mathbb{Z}_2[x]$, but it is reducible because

$$p(x) = (x^2 + x + 1)^2 \text{ in } \mathbb{Z}_2[x].$$

In $\mathbb{R}[x]$, $p(x) = x^4 + x^2 + 2 = (x^2 + x + 1) \cdot (x^2 - x + 1)$, and $p(x)$ has no roots in $\mathbb{R}$.

Corollary

Let F be an infinite field and $f(x), g(x) \in F[x]$. Then $f(x)$ and $g(x)$ induce the same function if and only if $f(x) = g(x)$ in $F[x]$.

Remark: The last result fails if the field is finite. For example, although $f(x) = x^5 + x$ and $g(x) = 2x$ are different polynomials in $\mathbb{Z}_5[x]$, they induce the same function in $\mathbb{Z}_5[x]$. To see this, check that $f(i) = g(i)$ for $i = 0, 1, 2, 3, 4$.