LECTURE 20

Polynomial Functions, Roots, and Reducibility

We will now look for conditions under which a given polynomial $f \in R[x]$, R being a commutative ring, factorizes.

DEFINITION 20.1. *Let R be a commutative ring. To any $f \in R[x]$, we can associate a map $\tilde{f} : R \to R$ as follows: if $f = a_n x^n + a_{n-1}x^{n-1} + \cdots a_1 x + a_o \in R[x]$ and $r \in R$, then we can define $\tilde{f}(r) \in R$ by*

$$\tilde{f}(r) = a_n r^n + a_{n-1} r^{n-1} + \cdots + a_1 r + a_o \quad .$$

*The function $\tilde{f}(x)$ is called the **polynomial function associated to** the polynomial f.*

Remark: One rarely uses separate notation to distinguish between $f \in R[x]$ and $\tilde{f} \in \{functions\ from\ R\ to\ R\}$.

Example: Consider the polynomials

$$\begin{aligned} f &= [1]_3 x^4 + [1]_3 x + [1]_3 \\ g &= [1]_3 x^3 + [1]_3 x^2 + [1]_3 \end{aligned}$$

These two polynomials are distinct when regarded as elements of $\mathbb{Z}_3[x]$. However,

$$\begin{aligned} \tilde{f}([0]_3) &= [1]_3 = \tilde{g}([0]_3) \\ \tilde{f}([1]_3) &= [0]_3 = \tilde{g}([1]_3) \\ \tilde{f}([2]_3) &= [1]_3 = \tilde{g}([2]_3) \end{aligned}$$

so, as functions from $\mathbb{Z}_3$ to $\mathbb{Z}_3$, $\tilde{f}(x)$ and $\tilde{g}(x)$ are identical.

More generally, if R is a ring with only n elements there will be only n^n distinct functions from R to R; even though there will be an infinite number of distinct polynomials on R.

DEFINITION 20.2. *Let R be a commutative ring and let $f \in R[x]$. An element $a \in R$ is said to be a **root** of the polynomial f if $\tilde{f}(a) = 0_R$.*

Example.

The polynomial $x^2 + 1$ has no roots when regarded as an element of $\mathbb{R}[x]$ because there is no real number r such that $r^2 = -1$. However, when we regard $x^2 + 1$ as an element of $\mathbb{C}[x]$ it has two roots $\pm i$.

THEOREM 20.3 (The Remainder Theorem). *Let F be a field, $f \in F[x]$, and $a \in F$. The remainder of f when divided by the polynomial $x - a$ is $\tilde{f}(a)$ (regarded as a zero degree element of $F[x]$).*

Proof.

By the Division Algorithm, there exists unique polynomials q and r in $F[x]$ such that

$$f = q(x - a) + r$$

with

$$r = 0_F \qquad \text{or} \qquad deg(r) < deg(x - a) = 1 \quad .$$

so either $r = 0$ or r is a non-zero constant. Thus, in either case, $r \in F$. If we now "evaluate" both sides of (20) at $a \in F$, we get

$$\tilde{f}(a) = \tilde{q}(a)(a - a) + r = r \quad .$$

∎

THEOREM 20.4 (The Factor Theorem). *Let F be a field, $f \in F[x]$, and $a \in F$. Then a is a root of the polynomial f if and only if $(x - a)$ is a factor of f in $F[x]$.*

Proof.

In view of Theorem 4.11, we have

$$f = (x - a)q + f(a) \quad .$$

Thus, if $f(a) = 0$, then $x - a$ is a factor of f. Using the uniqueness property of the division algorithm, we can also conclude that if $x - a$ divides f then $f(a) = 0$. ∎

COROLLARY 20.5. *Let F be a field and f a nonzero polynomial of degree n in $F[x]$. Then f has at most n roots in $F[x]$.*

Proof.

The proof is by induction on degree. If $n = 0$, then f is a nonzero constant polynomial and therefore has no roots. Thus. the statement is true for $n = 0$.

Now suppose that the statement of the theorem is true for all polynomials of degree less than n and that $deg(f) = n$. If f has no roots in F, then the statement is true. If f has a root $a \in F$, then we know by Theorem 4.12 that f factors as

$$f = (x - a)g$$

for some polynomial $g \in F[x]$. Suppose $c \in F$ is any root of f other than a. Then $(c - a) \neq 0$, and so $\tilde{f}(c) = 0$ implies that $\tilde{g}(c) = 0$ because F is an integral domain. Thus, the only roots of f in F are a and the roots c of g. But $deg(g)$ is $n - 1$. By the induction hypothesis, g, therefore, has at most $n - 1$ roots. Therefore, f has at most n roots. ∎

COROLLARY 20.6. *Let F be a field and $f \in F[x]$, with $deg(f) \geq 2$. (i) If f is irreducible in $F[x]$, then f has no roots in F. (ii) If f has degree 2 or 3 and has no roots in F, then f is irreducible in $F[x]$.*

Proof. (i) If f is irreducible, then it has no factor of the form $x + a$, $a \in F$. But then Theorem 4.12 implies that f has no roots $a \in F$.

(ii) Suppose f has degree 2 or 3 and has no roots in F. Then f has no first degree factor in $F[x]$, since every first degree polynomial $cx + d$ in $F[x]$ has a root in F, namely $-c^{-1}d$. Therefore, if

$$f = rs$$

then neither r nor s can have degree 1. Since f has degree 2 or 3, either r or s must have degree 0. Thus, r or s is a constant. And so f is irreducible by Theorem 4.8. ∎

COROLLARY 20.7. *Let F be an infinite field and $f, g \in F[x]$. Then f and g induce the same function from F to F if and only if $f = g$ in $F[x]$.*

Proof.

$\Leftarrow$

This is obvious.

$\Rightarrow$

Suppose that f and g induce the same function from F to F. Then $\tilde{f}(a) = \tilde{g}(a)$ for all $a \in F$. So

$$\tilde{f}(a) - \tilde{g}(a) = 0_F \quad , \quad \forall\, a \in F \quad .$$

This means that every $a \in F$ is a root of the polynomial $f - g$. Since F is infinite there must be an infinite number of roots of $f - g$. But this would contradict Corollary 4.13 - unless $f - g$ is the zero polynomial $0_F \in F[x]$. Therefore $f - g = 0_F$, which is to to say; $f = g$. ∎

Example:

1. Prove that $f = x^3 + x + 1$ is irreducible when regarded as an element of $\mathbb{Z}_5[x]$.

We have

$$\begin{aligned}
\tilde{f}\left([0]_5\right) &= [0]_5 + [0]_5 + [1]_5 = [1]_5 \\
\tilde{f}\left([1]_5\right) &= [1]_5 + [1]_5 + [1]_5 = [3]_5 \\
\tilde{f}\left([2]_5\right) &= [8]_5 + [2]_5 + [1]_5 = [1]_5 \\
\tilde{f}\left([3]_5\right) &= [27]_5 + [3]_5 + [1]_5 = [1]_5 \\
\tilde{f}\left([4]_5\right) &= [32]_5 + [4]_5 + [1]_5 = [2]_5
\end{aligned}$$

so $\tilde{f}(a) \neq [0]_5$ for all $a \in F$. By Corollary 4.14(i), f must be irreducible.