LECTURE 11.

ALIREZA SALEHI GOLSEFIDY

Last time we saw The Remainder Theorem:

Theorem 1. *Let F be a field and $f(x) \in F[x]$. Then for any $a \in F$ there is a unique $g(x) \in F[x]$ such that*

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

Corollary 2. *Let F be a field and $f(x) \in F[x]$. Then a is a zero of f if and only if $x-a$ divides $f(x)$ (is a factor of $f(x)$).*

Corollary 3. *Let F be a field and $f(x) \in F[x]$. If $f(a) = 0$, then there is a unique positive integer k and $g(x) \in F[x]$ such that*

$$f(x) = (x-a)^k g(x) \quad \text{and} \quad g(a) \neq 0.$$

Proof. By Corollary 2, $x - a$ is a factor of $f(x)$. Let

$$k = \max\{i |\ (x-a)^i \text{ is a factor of} f(x)\}.$$

Note that by Corollary 2 k is positive. Since $(x-a)^k$ is a factor of f, there is $g(x) \in F[x]$ such that

$$f(x) = (x-a)^k g(x).$$

Now we claim that $g(a) \neq 0$. Otherwise, $g(a) = 0$ and so by Corollary 2, $g(x) = (x-a)h(x)$ for some $h(x) \in F[x]$. Thus $f(x) = (x-a)^k g(x) = (x-a)^k (x-a)h(x) = (x-a)^{k+1}h(x)$, which means $(x-a)^{k+1}$ is also a factor of $f(x)$. But this contradicts the fact that k is the largest integer i such that $(x-a)^i$ is a factor of $f(x)$.

Uniqueness: If $f(x) = (x-a)^{k_1}g_1(x) = (x-a)^{k_2}g_2(x)$ and $g_2(a) \neq 0$ and $g_1(a) \neq 0$, then it is easy to show that

$$k_1 = k_2 = \max\{i |\ (x-a)^i \text{ is a factor of} f(x)\}.$$

Now by the cancellation rule, we have $g_1(x) = g_2(x)$. □

Corollary 4. *Let F be a field and $f(x) \in F[x]$. Then f has at most* $\deg(f)$ *zeros in F (counting with multiplicity).*

Proof. We proceed by strong induction. The base of the induction is easy.

Let $f \in F[x]$ and assume that the number of zeros of any polynomial g whose degree is strictly less than $\deg(f)$ is at most the degree of g.

If f has no zeros in F, then there is nothing to prove. Now assume that a is a zero of f. By Corollary 4 there is $gx(\in F[x]$ such that $f(x) = (x-a)^k g(x)$ and $g(a) \neq 0$. Now if $b \neq a$ is a zero of f, then $0 = f(b) = (b-a)^k g(b)$. So $g(b) = 0$ (note that $b - a \neq 0$ and F has no zero-divisor). Hence

$$\text{Number of zeros of } f = \text{multiplicity of } a + \text{number of zeros of } f \text{ which are not equal to } a$$

$$= k + \text{number of zeros of } g \leq k + \deg(g) = \deg(f).$$

□

Date: 2/6/2012.

Remark 5. If R has zero-divisors, then $f(x) \in R[x]$ might have more than $\deg(f)$ zeros. For instance $x^2 - 1 \in \mathbb{Z}/8\mathbb{Z}[x]$ has 4 zeros.

Mathematics Dept, University of California, San Diego, CA 92093-0112

E-mail address: golsefidy@ucsd.edu