Florian Enescu, Polynomials, Fall 2010: Lecture notes Week 2.

1. Polynomials. Definitions and basic facts.

In what follows we will use the letter K to denote any of the following $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. Let X be an indeterminate over $\mathbf{K}$. An expression f, or $f(X)$, of the form $f = f(X) = \sum_{k=0}^{n} a_k X^k$ where $n \in \mathbf{N}$, $a_k \in K$, for any $k = 1, \ldots, n$ and $a_n \neq 0$, is called a **polynomial** of one variable over K. Zero is also considered a polynomial. Their collection form a set called a polynomial ring, $K[X]$.

The addition and multiplication of polynomials is defined in the obvious manner:

If $f, g \in K[X]$, $f = \sum_{k=0}^{n} a_k X^k$, $g = \sum_{k=0}^{m} b_k X^k$, then

$$f + g = \sum_{k=0}^{h} c_k X^k, f \cdot g = \sum_{k=0}^{l} d_k X^k,$$

where

$$h = \max\{m, n\}, l = n \cdot m, c_k = a_k + b_k, d_k = \sum_{i+j=k} a_i b_j,$$

with the convention that a_k, b_k are zero whenever are not defined.

The degree of a polynomial $f = f(X) = \sum_{k=0}^{n} a_k X^k$ is degree$(f) = n$ and its leading term is $a_n X^n$ with leading coefficient a_n. The constant term (or free term) is a_0. The degree of the zero polynomial is $-\infty$.

It is clear that $\deg(fg) = \deg(f) + \deg(g)$ as long as $f \cdot g \neq 0$. This observation allows us to check that $f \cdot g = 0$ then $f = 0$ or $g = 0$.

The Division and Remainder Theorem is well-known:

Theorem 1.1 (Division and Remainder Theorem)**.** *Given any two polynomials $f, g \in K[X]$, there exist two unique polynomials $q, r \in K[X]$ such that*

$$f = qg + r,$$

and $r = 0$ or $\deg(r) < \deg(g)$.

Definition 1.2. If $f = f(X) \in K[X]$, then $\alpha \in \mathbb{C}$ is called a *root* for f if $f(\alpha) = 0$.

Given two polynomials $f, g \in K[X]$, then we say that g divides f if and only if there exists $h(X) \in K[X]$ such that $f(x) = g(X)h(X)$.

Proposition 1.3. *For a polynomial $f \in K[X]$, and $a \in K$, then exists a unique $q(x) \in K[X]$ such that $f(x) = (X - a)g(X) + f(a)$. In fact $X - a$ divides $f(X)$ if and only if $f(a) = 0$.*

Proof. Apply Theorem 1.1 to f and $X - a$ and hence there exist unique q, r such that

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

and $r = 0$ or $\deg(r) < \deg(X - a) = 1$. So, r is certainly a constant (possibly zero).

But if we plug in a in the above relation we get that $f(a) = r$. This finishes the proof since $f(a) = 0$ means that a is root for f and $r = 0$ means that $X - a$ divides f. □

Definition 1.4. We say that a root $a \in K$ for f has multiplicity k if $(X - a)^k$ divides f but $(X - a)^{k+1}$ does not. This is equivalent to saying that $f = (X - a)^k g$, $g \in K[X]$ and $g(a) \neq 0$.

Theorem 1.5. *Let $f = f(X)$ be a polynomial in $K[X]$ and $a_1, \dots, a_l$ distinct roots for f in K.*

Then $f(X) = (X - a_1)^{k_1} \cdots (X - a_l)^{k_l} g(X)$, where $g(X) \in K[X]$, and $k_1, \dots, k_l$ are the multiplicities of $a_1, \dots, a_l$ respectively.

Proof. We will prove this induction on l.

If $l = 1$, then the statement follows from the definition.

Assume that the statement was proven for $l - 1$. We will prove it for l.

Since a_l is a root for f, then by definition $f(X) = (X - a_l)^{k_l} h(X)$ with $h(a_l) \neq 0$.

But $f(a_i) = 0$ for all $i = 1, \dots, l - 1$ so $h(a_i) = 0$ as well. In fact, a_i are roots for $h(X)$ with multiplicities k_i. Indeed, whatever the multiplicity of a_i as a root for h is, it must be k_i.

If $h(X) = (X - a_i)^{k_i'} h'(X), h'(a_i) \neq 0$, then $(X - a_i)^{k_i} f'(X) = (X - a_l)^{k_l} (X - a_i)^{k_i'} h'(X)$, and since $f'(a_) \neq 0, h(a_i) \neq 0$, it follows that $k_i = k_i'$.

Now we can apply the induction hypothesis to h and $a_1, \dots, a_{l-1}$ and immediately get the desired statement.

□

This Theorem implies that the number of roots counted with their multiplicities cannot exceed the degree of the polynomial:

$$k_1 + \cdots + k_l \leq n$$

Proposition 1.6 (Viète's relations)**.** *Let $f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_0$ be a polynomial over K. Then if f has n roots (possibly not distinct, but counted with their multplicities) say $x_1, \dots, x_n$, then*

$$f = a_n (X - x_1) \cdots (X - x_n),$$

$$-a_{n-1} = a_n (x_1 + \cdots + x_n)$$

$$a_{n-2} = a_n (x_1 x_2 + x_1 x_3 + \cdots + x_{n-1} x_n) = a_n \sum_{1 \leq i < j \leq n} x_i x_j$$

....

$$(-1)^n a_0 = a_n x_1 x_2 \cdots x_n.$$

Proof. By the above Theorem $f = (X - x_1) \cdots (X - x_n) g$ and $\deg(g) = 0$ so g is constant. By comparing leading coefficients we get $g = a_n$.

By expanding we get exactly the above relations

□

Example 1.7. If $X^2 - sX + p = 0$ has two roots x_1, x_2, then $x_1 + x_2 = s$ and $x_1 x_2 = p$.

We will prove the Fundamental Theorem of Algebra as a consequence to Rouche's Theorem. Another proof, algebraic in nature, will be provided later.

Theorem 1.8. *Let f, g be two complex polynomials and γ a closed curve without self-intersections in the complex plane. If*

$$| f(z) - g(z) | < | f(z) | + | g(z) |$$

for all $z \in \gamma$ then inside γ there is an equal number of roots of f and g, multiplicities counted.

Theorem 1.9 (Fundamental theorem of algebra)**.** *Let $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ be a complex polynomial. Then inside the circle $| z | = 1 + \max_i(a_i)$, there are exactly n roots of f, multiplicities counted.*

Proof. Let $a = \max_i(a_i)$. Let $g(x) = x^n$, which has 0 root of multiplicity n.

According to Rouche's Theorem, we only need to show that if $| z | = 1+a$, then $| f(z) - g(z) | < | f(z) | + | g(z) |$.

In fact, we can show that

$| f(z) - g(z) | < | g(z) |$.

Clearly, if $| z | = 1 + a$, then

$| a_{n-1}z^{n-1} + \ldots + a_0 | \leq a(| z |^{n-1} + \cdots + 1) = a\frac{|z|^n - 1}{|z| - 1} = | z |^n - 1 < | z |^n$.

□