March 10, 2019 Math 9

Algebra.

Polynomials and factorization.

Little Bézout's (polynomial remainder) theorem. Factoring polynomials.

Theorem. The **remainder** of a **polynomial** $P(x)$

$$P_n(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_2 x^2 + a_1 x^1 + a_0 \qquad (1)$$

divided by a **linear divisor** $(x - a)$ is equal to $P(a)$.

The polynomial remainder theorem follows from the definition of polynomial long division; denoting the divisor, quotient and remainder by, respectively, $G(x)$, $Q(x)$, and $R(x)$, polynomial long division gives a solution of the equation

$$P(x) = Q(x)G(x) + R(x)$$

where the degree of $R(x)$ is less than that of $G(x)$. If we take $G(x) = x - a$ as the divisor, giving the degree of $R(x)$ as 0, i.e. $R(x) = r$,

$$P(x) = Q(x)(x - a) + r. \qquad (2)$$

Here r is a number. Setting $x = a$, we obtain $P(a) = r$.

Roots of polynomials.

Definition 1. A number $a \in \mathbb{R}$ is called a **root** of polynomial $P(x)$ if $P(a) = 0$.

As a corollary to the polynomial remainder theorem, we obtain the following result, the factor theorem, which provides the basis for factoring polynomials.

Theorem (Factor Theorem). If a is a root of a polynomial $f(x)$, then $f(x)$ is divisible by $(x - a)$.

If $x_1, x_2, \ldots, x_m$ are distinct roots of a polynomial $f(x)$, then $f(x)$ is divisible by $(x - x_1)(x - x_2) \ldots (x - x_m)$.

Theorem. A non-zero polynomial $f(x)$ of degree n cannot have more than n roots. If it does have exactly n roots $x_1, x_2, \dots, x_n$, then

$$f(x) = c(x - x_1)(x - x_2) \dots (x - x_n)$$

As a corollary, we have the following result:

Theorem. If $f(x)$ and $g(x)$ are polynomials of degree n, which have the same values at more than n points, i.e., there exist $x_1, x_2, \dots, x_n, x_{n+1}$ such that $\forall i, 1 \le i \le n+1, f(x_i) = g(x_i)$, then $f(x) = g(x)$.

Theorem (rational root theorem). Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_1 x^0 + a_0$ be a polynomial with integer coefficients. Then, if $f(x)$ has a rational root, $x_0 = \pm p/q$, where p and q are relatively prime positive integers, then p is a divisor of a_0 and q a divisor of a_n, $a_0 \equiv 0 mod(p)$, $a_n \equiv 0 mod(q)$.

Proof. Consider first positive $x_0 = p/q$; x_0 being the root of $f(x)$, we can write,

$$a_n p^n + a_{n-1}p^{n-1}q + a_{n-2}p^{n-2}q^2 + \dots + a_1 pq^{n-1} + a_0 q^n = 0$$

From here, using the fact that p and q are relatively prime we immediately obtain, $a_0 \equiv 0 mod(p)$, $a_n \equiv 0 mod(q)$.

Exercise. Extend the proof for negative x_0.

Corollary. Let $f(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \dots + a_1 x + a_0$ be a polynomial with integer coefficients. Then any rational root $x_i, 1 \le i \le n$ of $f(x)$ must be integer, and must be a divisor of the constant term a_0.

Note that it is quite possible that there are no rational roots at all, i.e., that all roots are irrational.

Definition 2. A number $a \in \mathbb{R}$ is called a **multiple root** of polynomial $P(x)$ of multiplicity m if $P(x)$ is divisible (without remainder) by $(x-a)^m$ and not divisible by $(x-a)^{m+1}$.

If x_1 is the root of a polynomial $P_n(x)$ of degree n, then $r = 0$, and

$$P_n(x) = (x - x_1)Q_{n-1}(x), \qquad (3)$$

where $Q_{n-1}(x)$ is a polynomial of degree n – 1. $Q_{n-1}(x)$ is simply the quotient, which can be obtained using the **polynomial long division** (see last class handout). Since x_1 is known to be the root of $P_n(x)$, it follows that the remainder r must be zero.

If we know m roots, $\{x_1, x_2, \dots x_m\}$, of a polynomial $P_n(x)$ (why is it obvious that m ≤ n ?), then, applying the above reasoning recursively,

$$P_n(x) = (x - x_1)(x - x_2) \dots (x - x_m)Q_{n-m}(x), \quad (4)$$

So if we know that $P_n(x)$ given by (1) has n roots, $\{x_1, x_2, \dots x_n\}$, then,

$$P_n(x) = a_n(x - x_1)(x - x_2) \dots (x - x_n). \quad (5)$$

If two polynomials,

$$P_n(x) = a_n x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_2 x^2 + a_1 x^1 + a_0$$

and

$$Q_n(x) = b_n x^n + b_{n-1}x^{n-1} + b_{n-2}x^{n-2} + \cdots + b_2 x^2 + b_1 x^1 + b_0$$

are equal, $P_n(x) = Q_n(x)$, then all corresponding coefficients are equal,

$$a_n = b_n, a_{n-1} = b_{n-1}, a_{n-2} = b_{n-2}, \dots, a_{n-m} = b_{n-m}, \dots, a_1 = b_1, a_0 = b_0. \quad (6)$$

This is the easiest way to obtain the Vieta's theorem and its generalizations for higher-order polynomials.

Vieta theorem.

Theorem. Let $f(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots + a_1 x^0 + a_0$ be a polynomial with leading coefficient 1 and roots $x_1, x_2, \dots, x_n$,

$f(x) = (x - x_1)(x - x_2) \dots (x - x_n)$.

Then the coefficients of $f(x)$ can be written in terms of roots,

$$a_0 = (-1)^n x_1 x_2 \dots x_n$$

$$a_1 = (-1)^{n-1}(x_1 x_2 \dots x_{n-1} + x_1 x_2 \dots x_{n-2} x_n + \cdots + x_2 x_3 \dots x_n)$$

…

$$a_{n-1} = -(x_1 + x_2 + \cdots + x_n)$$

For $n = 2$, quadratic equation, $x^2 + px + q = (x - x_1)(x - x_2)$, we have,

$q = x_1 x_2$ and $p = -(x_1 + x_2)$

For the cubic equation, $n = 3$, where x_1, x_2 and x_3 are the roots,

$x^3 + a_2 x^2 + a_1 x + a_0 = (x - x_1)(x - x_2)(x - x_3)$,

$a_0 = -x_1 x_2 x_3, a_1 = x_1 x_2 + x_2 x_3 + x_1 x_3, a_2 = -(x_1 + x_2 + x_3)$

Moreover, any expression in the roots $x_1, x_2, \ldots, x_n$ which is symmetric (i.e., doesn't change when we permute any two roots) can be written in terms of the coefficients $a_0, a_1, \ldots, a_n$. Example: for n = 2, $x_1^2 + x_2^2 = \cdots$

Cubic equation.

Equations involving cubic polynomial are called cubic equations.

$ax^3 + bx^2 + cx + d = 0, a \neq 0$ or

$x^3 + \frac{b}{a}x^2 + \frac{c}{a}x + \frac{d}{a} = 0, x^3 + Px^2 + Qx + R = 0$

Using the substitution, $x = y - \frac{b}{3a} = y - \frac{P}{3}$, this can be simplified to a reduced form,

$y^3 + py + q = 0$.

Gerolamo Cardano derived a closed formula for the solution of this equation known as Cardano formula, which he published in 1545,

$y = u - \frac{p}{3u}$, where $u = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$,

which is quite complicated. Derivation of Cardano is somewhat esoteric. More consistent derivation was given later by Lagrange. Perhaps, the best one is achieved by using trigonometry. All of these are quite cumbersome (you

might look these up on Wikipedia, http://en.wikipedia.org/wiki/Cubic_function).

The only other polynomial equation that is solvable in radicals is the quartic equation, which has been solved by Cardano's student, **Ludovico Ferrari** in 1540. The solution is known as Ferrari formula, and is even more cumbersome than that of Cardano. In fact, it utilizes the latter. It was published by Cardano in his book Ars Magna together with the cubic formula in 1545 (http://en.wikipedia.org/wiki/Quartic_equation).

Biquadratic equation.

Equations of the following type are called biquadratic equations:

$ax^4 + bx^2 + c = 0,\ a \neq 0\ \ (1)$

If we replace x^2 with $y\,(x^2 = y)$, we will get the following quadratic equation:

$ay^2 + by + c = 0, a \neq 0\ \ (2)$

This equation can have two, one or no roots. If it doesn't have any roots equation (1) will not have any roots also.

Generally the roots of equation (2) are:

$$y = \frac{-b + \sqrt{b^2 - 4ac}}{2a} \ \vee\ y = \frac{-b - \sqrt{b^2 - 4ac}}{2a}$$

and equation (1) will have four roots (or two in the case when D=0 for equation (1)).

$$x^2 = \sqrt{\frac{-b + \sqrt{b^2 - 4ac}}{2a}} \ \vee\ x^2 = \sqrt{\frac{-b - \sqrt{b^2 - 4ac}}{2a}}$$

$$x = +\sqrt{\frac{-b+\sqrt{b^2-4ac}}{2a}} \vee x = -\sqrt{\frac{-b+\sqrt{b^2-4ac}}{2a}} \vee x = +\sqrt{\frac{-b-\sqrt{b^2-4ac}}{2a}} \vee x = -\sqrt{\frac{-b-\sqrt{b^2-4ac}}{2a}}$$

Note, that equation $x^4 = 0$ has one root x=0, equation $x^4 - x^2 = 0$ has three roots $x_1 = 0, x_2 = 1, x_3 = -1$.