MATH 9: VIETA FORMULAS

2021/03/21

1. Becoming Comfortable with Roots

Recall that, given a polynomial $p(x)$, the roots of $p(x)$ are numbers x_i such that $p(x_i) = 0$. We know from the factorization theorem that $p(r) = 0 \leftrightarrow (x - r)|p(x)$, and similarly for a collection of distinct numbers x_1, ..., x_k, that they are all roots if and only if $(x - x_1)(x - x_2)...(x - x_k)|p(x)$. The "number of roots" theorem says that a polynomial of degree n is uniquely determined by its n roots, if it has n roots. Well, it turns out that a polynomial of degree n always has n roots - though these roots may be repeated, and some of them might not be real numbers. But still the following theorem is useful.

Theorem 1 (Fundamental Theorem of Algebra)**.** *Any polynomial of degree ≥ 1 has a root. This root may be complex.*

Proof. Don't worry too much about the proof of this theorem, I just want you to know what it's called, and that it's quite a famous theorem. There are many proofs of it, but most involve analysis or abstract algebra. □

Now, you can break a degree n polynomial down to its roots by applying the Fundamental Theorem of Algebra and then the Factorization Theorem to pull out the $(x - x_i)$ factors one by one. Here is an example.

$$p(x) = x^3 + x^2 - x - 1$$

How do you factorize this polynomial? All its roots are real, so let's go through it step by step. The first root I want to point out is $x_1 = 1$. You can check for yourself that 1 is a root by plugging it into $p(x)$. Now divide $p(x)$ by $(x - 1)$ to factor out the root $x_1 = 1$. This leaves you with

$$p(x) = (x - 1)(x^2 + 2x + 1)$$

You may or may not recognize the remaining factor, but I'll tell you that -1 is a root of it. So, $x^2 + 2x + 1$ should be divisible by $(x + 1)$. This gives us

$$p(x) = (x - 1)(x + 1)(x + 1)$$

And we see that the final root is -1. We have therefore broken down this degree 3 polynomial into a product of three degree 1 factors.

A similar process can be done for any polynomial, so long as you feel safe working with complex numbers. For the moment, however, I want you to notice the repeat of one of the roots. This is possible in general, and it is called multiplicity. Given any number r and a polynomial $p(x)$, the greatest integer k such that $(x - r)^k|p(x)$ is called the multiplicity of the root r. In this example, the roots of $x^3 + x^2 - x - 1$ are 1 with multiplicity 1, and -1 with multiplicity 2.

Here is one more theorem for fun.

Theorem 2 (Rational Root Theorem)**.** *If $p(x)$ is a polynomial with **integer coefficients** and $r \in \mathbb{Q}$ is a root of $p(x)$, then r is an integer, and r is a factor of the constant term of $p(x)$.*

Proof. Let $r = \frac{a}{b}$ for relatively prime integers a, b. Let the degree of $p(x)$ be n, and write $p(x)$ as $x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_0$. Then

$$b^n p(\frac{a}{b}) = a^n + a_{n-1}a^{n-1}b + a_{n-2}a^{n-2}b^2 + ... + a_0 b^n$$

Given that $p(r) = 0$, we then get

$$a^n + a_{n-1}a^{n-1}b + a_{n-2}a^{n-2}b^2 + ... + a_0 b^n = 0$$

Take this equation mod b to get

$$a^n \equiv 0 \mod b$$

Therefore $b|a$. Since the gcd of a, b is 1, and $b|a$ implies b is a common factor of a, b, we must have $b = 1$. This proves that r is an integer. Now take the equation mod a to get

$$a_0 b^n \equiv 0 \mod a$$

This proves that $a_0 \equiv 0 \mod a$, which means that $a|a_0$. □

2. Vieta: Quadratic

Now I can talk to you about the relationship between roots and coefficients. This theory concerns what are called the Vieta formulas.

Theorem 3 (Vieta, Quadratic)**.** *Given a quadratic polynomial $x^2 + bx + c$, with real coefficients $b, c \in \mathbb{R}$, the roots x_1,x_2 satisfy the following equations:*

$$(-1) \cdot (x_1 + x_2) = b$$

$$x_1 x_2 = c$$

Proof. Given that x_1,x_2 are roots of the polynomial, we can factor it as $(x - x_1)(x - x_2)$. We therefore get

$$x^2 + bx + c = (x - x_1)(x - x_2) = x^2 - x_1 x - x_2 x + x_1 x_2 = x^2 - 1 \cdot (x_1 + x_2)x + x_1 x_2$$

□

Thus the coefficients of a quadratic polynomial depend directly on its roots. These formulas are extremely helpful in understanding quadratic polynomials, and can be used in a variety of contexts.

3. Vieta: In General

To understand the general Vieta formulas, it is helpful to know the word symmetric polynomial. A symmetric polynomial of degree k on n variables is a polynomial of n variables that satisfies the property that swapping the order of the variables doesn't change the polynomial. The elementary symmetric polynomial of degree k, written σ_k, is the sum of all products of k variables from the collection of n variables plugged into the polynomial. Here is an example of σ_3:

$$\sigma_3(x_1, x_2, x_3) = x_1 x_2 x_3$$

$$\sigma_3(x_1, x_2, x_3, x_4) = x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_3 x_4 + x_2 x_3 x_4$$

$$\sigma_3(x_1, x_2, x_3, x_4, x_5) = x_1 x_2 x_3 + x_1 x_2 x_4 + x_1 x_2 x_5 + ...$$

Basically, it contains all combinations of 3 variables. If there are n variables $x_1, ..., x_n$, then there are n choose 3 terms in $\sigma_3(x_1, ..., x_n)$.

Now here are the Vieta formulas.

Theorem 4 (Vieta Formulas)**.** *Given a degree n polynomial $p(x) = x^n + a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + ... + a_0$ (notice that the coefficient of x^n is 1), with roots $x_1, ..., x_n$, the coefficient of x^{n-k} is the symmetric polynomial $(-1)^k \sigma_k(x_1, ..., x_n)$.*

Here is an example of what it looks like on a cubic polynomial. Let $p(x)$ be the cubic polynomial $p(x) = x^3 + ax^2 + bx + c$, and let the roots of this polynomial be q, r, s. Then

$$a = (-1)(q + r + s)$$

$$b = (+1)(qr + qs + rs)$$

$$c = (-1)(qrs)$$

In particular, for a degree n polynomial whose leading coefficient is 1, the coefficient of x^{n-1} is -1 times the sum of the roots, and the constant term is $(-1)^n$ times the product of the roots.