Lecture 5
Algebraic Roots of Geometry

We have attempted to characterize the notion of "geometric computation" by pointing out some common features. But we have not really answered the fundamental question: what is "geometry"? In some sense, this is is an impossible task. Throughout the history of mathematics, different answers to this question has been given.

Geometry is more intuitive than algebra, and is the source of many mathematical ideas. On the other hand, the geometric approach cannot progress without a proper algebraic foundation. This impulse is seen in Descartes' program to algebraize geometry. In Felix Klein's Erlangen Program, the essence of geometry is reduced to invariant groups. David Hilbert, in his work on axiomatic mathematics, also used geometry as a launching point. In this lecture, we look at the viewpoint of Alfred Tarski, which can be viewed as a synthesis of Hilbert's logical view and Descartes' algebraic approach.

§1. Algebraic Background

We assume some familiarity with the following algebraic structures:

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}.$$

The prime example of a ring is $\mathbb{Z}$ (integers), and the rational numbers $\mathbb{Q}$ is our prime example of a field. We will try to state our results as concretely as possible. But student less familiar with abstract algebra may you may substitute these prime examples whenever we say "ring" or "field". Much of this material is summarized from my book [1].

Let K be a field. If X is a variable, let $K[X]$ denote the polynomial ring with coefficients in R. A typical polynomial $A = A(X)$ has the form

$$A(X) := \sum_{i=0}^{m} a_i X^i, \qquad a_m \neq 0$$

where each non-zero a_i is called a **coefficient** of A. Here, a_m is called the **leading coefficient** and m is called the **degree** of $A(X)$. These are denoted $\texttt{lead}(A) = a_m$ and $\deg(A) = m$ respectively. In case $A(X) = 0$, we define[1] $\texttt{lead}(0) = 0$ and $\deg(0) = -\infty$. If $\texttt{lead}A = 1$ then A is said to be **monic**. If $\alpha \in K$ and $A(\alpha) = 0$, we say α is a **root** of $A(X)$. There are several ways to measure the size of polynomials that takes into account its coefficients. For any number $p \geq 1$, define the **p-norm**,

$$\|A(X)\|_p := \sqrt[p]{\sum_{i=0}^{m} |a_i|^p}.$$

We can also define $\|A(X)\|_\infty = \max_{i=0}^{m} |a_i|$, The case $p = 2$ and $p = \infty$ (respectively) are also called the (Euclidean) length and height of A.

[1]Sometimes, $\deg(0)$ is defined as $+\infty$ instead of $-\infty$. Both definitions have advantages, but neither seems superior: for instance, exactly one of the following statements is true in either definition: (1) "the division algorithm for A, B produces Q, R such that $A = BQ + R$ with $\deg R < \deg B$". (2) "Every complex polynomial of degree m has exactly m roots". Of course, in practice, we just have to add the qualification that A is non-zero. If we define $\deg(0) = +\infty$, then the condition "$\deg A \leq d$" can be used to exclude the case $A = 0$, but then the condition "$\deg A > \deg B$" may produce some surprises. We have opted to avoid surprises.

A pair of polynomials $p, q \in K[X]$ defines a **rational function** in X which is usually denoted p/q. Moreover, if p'/q' is another rational function, then p/q and p'/q' are declared to be equal if and only if $pq' = p'q$. The set of rational functions is denoted $K(X)$.

In case $K = \mathbb{C}$, we have the Fundamental Theorem of Algebra which says that every $p(X) \in \mathbb{C}[X]$ has exactly $\deg(p)$ complex roots. A number $\alpha \in \mathbb{C}$ is said to be **algebraic** if it is the root of a polynomial $p \in \mathbb{Z}[X]$. If further, p is monic, then α ia called an **algebraic integer**. This generalizes our usual concept of integers.

UFD. Let R be a ring, $a, b \in R$. A domain is a ring in which $ab = 0$ implies $a = 0$ or $b = 0$. We say a **divides** b if there is a c such that $ac = b$. If $ab = 0$ and $b \neq 0$ then we call a a zero-divisor. Thus a domain is a ring whose only zero-divisor is 0. A **unit** a is an element that divides 1. Alternatively, the equation $ax = 1$ has a solution x. E.g., $\mathbb{Z}$ is a domain in which the only units are ± 1 In a field, all non-zero elements are units. A **unique factorization domain** (UFD) is a domain in which every element a can be written as a product $a = \prod_{i=1}^{k} p_i$ of irreducible elements p_i; this product is unique up to units in the sense that if $a = \prod_{i=j}^{\ell} q_j$ then $k = \ell$ and by suitable reordering, each $p_i = u_i q_i$ were u_i are units. The Fundamental Theorem of Arithmetic tells us that $\mathbb{Z}$ is a UFD. A basic result of Gauss says that if R is a UFD if and only if $R[X]$ is a UFD.

In a UFD, we can define the concept of a GCD of a set of elements. In the ring $K[X]$ over a field K, Euclid's algorithm can be extended to compute the GCD of two polynomials.

Resultants. A basic tool in algebraic number theory is the concept of resultants. Given $p, q \in K[X]$, we define their resultant $\mathtt{res}(p, q) \in K$ to be the determinant of the Sylvester matrix of p, q. This is a $m + n$ square matrix where $m = \deg p, n = \deg q$.

LEMMA: $\mathtt{GCD}(p, q)$ is a constant iff $\mathtt{res}(p, q) \neq 0$.

The concept of a resultant can be generalized to the the notion of subresultants. We state some basic properties of resultants: let A, B be polynomials with $\deg A = m, \deg B = n$, $\mathtt{lead}A = a, \mathtt{lead}B = b$. Also let the roots of A and B be $\alpha_1, \ldots, \alpha_m$ and $\beta_1, \ldots, \beta_n$ (resp.).

LEMMA:
(i) $\mathtt{res}((X - \alpha)p, q) = q(\alpha)\mathtt{res}(p, q)$.
(ii) $\mathtt{res}(A, B) = a^n \prod_{i=1}^{m} B(\alpha_i)$.
(iii) $\mathtt{res}(A, B) = (-1)^{mn} b^m \prod_{j=1}^{n} A(\beta_j)$.
(iv) $\mathtt{res}(A, B) = a^n b^m \prod_{i=1}^{m} \prod_{j=1}^{n} (\alpha_i - \beta_j)$.

It is easy to show (ii)-(iv) from (i). The proof of (i) is somewhat involved, but can be achieved by a direct computation. Also, we have

LEMMA
Let $A(\alpha) = 0, B(\beta) = 0$.
(i) If $\alpha \neq 0$ then $1/\alpha$ is a root of $X^m A(1/X)$.
(ii) $\beta \pm \alpha$ is a root of $\mathtt{res}_Y(A(Y), B(X \mp Y))$.
(ii) $\alpha\beta$ is a root of $\mathtt{res}_Y(A(Y), Y^n B(X/Y))$.

It follows from the above that the set of algebraic numbers forms a field. Moreover, the algebraic integers forms a ring.

Root Bounds. There is a very large classical literature on root bounds. Here, we content ourselves with a simple one.

Suppose $p(X) = \sum_{i=0}^{m} a_i X^i$, and $\alpha \neq 0$ is a root of $p(X)$. Then we have the following bound of Cauchy:

$$\frac{|a_0|}{|a_0| + H_0} < |\alpha| < 1 + \frac{H_m}{|a_m|}$$

where $H_0 = \max\{|a_1|, |a_2|, \ldots, |a_m|\}$ and $H_m = \max\{|a_0|, |a_1|, \ldots, |a_{m-1}|\}$.

Let us first prove the upper bound. If $|\alpha| \leq 1$, the result is true. Otherwise, we have

$$|a_m| \cdot |\alpha|^m \leq H_m \sum_{i=0}^{m-1} |\alpha|^i$$

which leads to the stated bound. For the lower bound, consider the polynomial $p(1/X)X^m$ instead.

We also have root separation bounds: this is slightly more involved to prove. The **discriminant** of a polynomial $A(X)$ is defined to be $\mathrm{disc}(A) := (-1)^{\binom{m}{2}}(1/a)\mathtt{res}(A, A')$ where $a = \mathtt{lead}A$ and A' is the derivative of A. For instance if $A(X) = aX^2 + bX + C$ then $\mathrm{disc}(A) = b^2 - 4ac$. If A has multiple roots, then $\mathrm{disc}(A)$ vanishes. The following bound is essentially from Mahler:

Theorem 1 *Let α, α' be distinct roots of $A(X) \in \mathbb{C}[X]$. Then*

$$|\alpha - \alpha'| > \sqrt{|\mathrm{disc}(A)|}\|A\|_2^{-m+1} m^{-(m+2)/2} (\sqrt{3}.$$

Sturm Theory Suppose $A, B \subseteq \mathbb{R}[X]$ and $\deg A > \deg B \geq 0$. We define a **generalized Sturm sequence** for (A, B) to be a sequence

$$\overline{A} = (A_0, A_1, \ldots, A_h)$$

where $A_0 = A, A_1 = B$ and for $i = 1, \ldots, h-1$,

$$\beta_i A_{i+1} = \alpha_i A_{i-1} + Q_i A_i$$

where $\alpha_i, \beta_i \in \mathbb{R}$, $Q_i \in \mathbb{R}[X]$ and $\alpha_i \beta_i < 0$, and finally

$$A_h | A_{h-1}.$$

The "standard construction" of such a generalized Sturm sequence is where

$$A_{i+1} = -(A_{i-1} \bmod A_i)$$

where we assume that the mod function operates over the entire real field. But as we noted in [1], when $A, B \in \mathbb{Z}[X]$, there are better methods which maintain the A_i's as integer polynomials.

In the following, it is convenient to assume some canonical construction so that once A, B are given, the rest of the sequence $\overline{A}$ is determined.

If $\overline{\alpha} = (\alpha_0, \alpha_1, \ldots, \alpha_h)$ is a sequence of real numbers, we define $\mathrm{SignVar}(\overline{\alpha})$ to be the number of sign variations (i.e., transitions from + to − or + to −) after we omit all 0 values from the sequence. E.g. $\mathrm{SignVar}(2, 0, 3.5, -1.2, 0, -10, 0, 0, 3) = 2$.

References

[1] C. K. Yap. *Fundamental Problems in Algorithmic Algebra*. Oxford University Press, 2000. Older version available at URL `ftp:/Preliminary/cs.nyu.edu/pub/local/yap/algebra-bk`.