Math 250A Lecture 17 Notes

Daniel Raban

October 24, 2017

1 Symmetric Functions and Polynomial Invariants

1.1 Symmetric functions and Newton's identities

Last time, we saw that any symmetric polynomial f is a polynomial in the elementary symmetric functions. We took the monomial $x_1^{n_1}x_2^{n_2}\cdots$ in f which is largest, and subtracted

$$(x_1 + \cdots + x_n)^{n_1-n_2}\cdots .$$

The key point was that since f is symmetric, $n_1 - n_2$, $n_2 - n_3$ and other terms are positive; if f has a term with $x_i^{n_i}x_j^{n_j}$ with $n_j < n_i$, then f also has $x_i^{n_j}x_j^{n_i}$.

1.1.1 Newton's identities

What is $x_1^4 + x_2^4 + x_3^4 + \cdots$? Look at

$$f(x) = (x - x_1)(x - x_2)\cdots(x - x_n) = x^n - e_1x^{n-1} + e_2x^{n-2} + \cdots .$$

Take the logarithmic derivative, $\frac{d}{dx}\log f(x) = \frac{f'(x)}{f(x)}$. The log derivative of fg is the log derivative of f plus the log derivative of g.

So the log derivative of $x - x_1$ is

$$\frac{1}{x - x_1} = \frac{1}{x} + \frac{x_1}{x^2} + \frac{x_1}{x^3} + \cdots .$$

And we get that the log derivative of f is

$$\frac{n}{x} + \frac{x_1 + x_2 + \cdots}{x^2} + \frac{x_1^2 + x_2^2 + \cdots}{x^3} = \frac{p_0}{x} + \frac{p_1}{x^2} + \cdots$$

So $f(\sum p_m/x^{m+1}) = f'$ gives us that

$$(x^n - e_1x^{n-1} + \cdots))(\frac{p_0}{x} + \frac{p_1}{x^2}) = nx^{n-1} - (n-1)e_1x^{n-2} + \cdots .$$

Equating the powers of x, we have

$$p_0 = n, \qquad p_1 - e_1p_0 = -(n-1)e_1, \qquad p_2 - e_1p_1 + e_2p_0 = (n-2)e_2$$

Example 1.1. Let α, β, γ be the roots of $z^3 + z + 1$. What is $\alpha^5 + \beta^5 + \gamma^5$? We have

$$p_0 = 3, \quad p_1 = 0, \quad p_2 + p_0 = 1, \quad p_2 = -1, \quad p_3 = -3, p_4 = 2.$$

and $p_5 + p_3 + p_2 = 0$. These are the coefficients of the polynomial.[1]

1.2 The discriminant

What about polynomials in $x_1, \ldots, x_n$ invariant under the alternating group, A_n?

Definition 1.1. A polynomials f in variables $x_1, \ldots, x_n$ is *antisymmetric* if it changes sign under elements $\sigma \notin A_n$.

Proposition 1.1. *Suppose f is invariant under A_n. Then $f = g + h$, where g is symmetric and h is antisymmetric.*

Proof. Set

$$g = \frac{f + \sigma f}{2}, \qquad h = \frac{f - \sigma f}{2}.$$

□

The polynomial h changes sign if we switch x_i and x_j, so h is divisible by the polynomial $(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)\cdots$. So let

$$\Delta = \prod_{i<j}(x_i - x_j).$$

The invariant functions of A_n are generated by the symmetric functions $e_1, \ldots, e_n$ and Δ. Note that Δ^2 is symmetric, so Δ^2 is some polynomial in $e_1, \ldots, e_n$. This is called *syzygy*.[2]

Definition 1.2. The *discriminant*[3] of $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ is $a_n^{2n-2}\Delta^2$.

The discriminant vanishes iff f has multiple roots.

Proposition 1.2. *A polynomial f has a multiple root iff f and f' have a common factor.*

Proof. If $f = (x - x_1)^2 \cdots$, then $f' = 2(x - x_1)\cdots + (x - x_1)^2 \cdots$, so $x - x_1$ is a common factor. The converse is an exercise. □

[1] In the 19th century, undergraduate students were expected to be able to calculate things like this involving symmetric functions.

[2] This comes from syn, which means together, and zygon, which means yoke. This is not the longest word in the English language with no vowels; that honor goes to the word rhythms.

[3] Invariants tend to end with -ant. For example, we have the determinany, the resultant, and the catalecticant. Professor Borcherds is glad the last of these has fallen out of usage.

When do $f(x), g(x)$ have a common factor?

$$f(x) = a_m x^n + \cdots + a_0$$

$$g(x) = b_n x^n + \cdots + b_0$$

If f, g have a common factor, then $f(x)p(x) - g(x)q(x) = 0$ for some p, q with $\deg(p) < n$ and $\deg(q) < m$ (set $p = g/(x-\alpha)$ and $q = -f/(x-\alpha)$).

This is a set of linear equations for coefficients of p, q. This has a nonzero solution if some determinant vanishes. So the coefficients of linear equations are:

$$\begin{bmatrix} a_m & a_{m-1} & \cdots & a_0 & 0 & 0 & 0 & 0 \\ 0 & a_m & \cdots & a_1 & a_0 & 0 & 0 & 0 \\ \vdots & & & & & & & \\ 0 & 0 & \cdots & a_n & \cdots & a_2 & a_1 & a_0 \\ b_n & b_{n-1} & \cdots & b_0 & 0 & 0 & 0 & 0 \\ 0 & b_n & \cdots & b_1 & b_0 & 0 & 0 & 0 \\ \vdots & & & & & & & \\ 0 & 0 & \cdots & b_n & \cdots & b_2 & b_1 & b_0 \end{bmatrix}$$

This matrix with $n + m$ rows is called the *Sylvester matrix.*

Definition 1.3. The *resultant* is the determinant of the Sylvester matrix.

Say f, g have a common root at ∞ if $a_m = b_m = 0$. The resultant equals 0 iff f and g have a common factor, possibly at ∞. This is the same as saying in geometry that the projective line is complete.

Example 1.2. The polynomial $f(x) = x^n - e_1 x^{n-1} + \cdots$ has a multiple root if the resultant of $f, f' = 0$. $\Delta = 0$ iff f has tahe multiple root, so Δ should be a constant times the resultant.

Example 1.3. When is the cubic curve $y^2 = x^3 + bx + c$ nonsingular? Curve $f(x, y)$ is nonsingular if $g(x, y) = 0 = f_x(x, y) = f_y(x, y)$ has no solutions, where f_x is the partial derivative with respect to x. These are the conditions that $2y = 0$ (so $y = 0$) and $3x^2 + b = 0$ (so $g(x) = x^3 bx + c = 0$); then we need to check if g, g' have a common root x.

The resultant of $x^3 + bx + c$ and $3x^2 + b$, is

$$\det \begin{bmatrix} 1 & 0 & b & c & 0 \\ 0 & 1 & 0 & b & c \\ 3 & 0 & b & 0 & 0 \\ 0 & 3 & 0 & b & 0 \\ 0 & 0 & 3 & 0 & b \end{bmatrix}$$

which is $4b^3 + 27c^2$ (up to a sign).

1.3 The ring of invariants, revisited

Suppose a finite group G acts on a complex vector space V spanned by $\{x_1, \dots, x_n\}$. Recal that the ring of invariant polynomials is the set of polynomials in $x_1, \dots, x_n$ invariant under the action of$G$. Is this ring finitely generated (over $\mathbb{C}$)?

Example 1.4. If $G = A_n$ and $V = \mathbb{C}^n$, then the ring is generated by $e_1, \dots, e_n, \Delta$.

In general this can be "mindbogglingly difficult."[4] Hilbert showed that the ring of invariants is finitely generated over $\mathbb{C}$.

Definition 1.4. The *Reynolds operator*[5] ρ is the average of the group elements,

$$\rho = \frac{1}{|G|} \sum_{g \in G} g.$$

The Reynolds operator takes polynomials in $\mathbb{C}[x,_1, \dots, x_n]$ to invariants.

Example 1.5. Let $G = S_n$. Then if $f = x_1$, $\rho(f) = \frac{x_1 + x_2 + \cdots + x_n}{n}$.

Proposition 1.3. *They Reynolds operator has the following properties:*

1. $\rho(f + g) = \rho(f) + \rho(g)$
2. $\rho(1) = 1$
3. $\rho(fg) = \rho(f)\rho(g)$ *if* $f = \rho(f)$

Proof. Exercise. □

Theorem 1.1 (Hilbert)**.** *If G is finite, the ring of invariants is always finitely generated over $\mathbb{C}$.*

Proof. Look at the ring $\mathbb{C}[x_1, \dots, x_n]$. This is graded by degree, where $\deg(x_i) = 1$. Let I be the ring of invariants. Then $I = \mathbb{C} \oplus I_1 \oplus I_2 \oplus \cdots$, where I_m is the set of invariants homogeneous of degree m. Look at the ideal generated by $I_1 \oplus I_2 \oplus I_3 \oplus \cdots$. By Hilbert's theorem, this ideal is finitely generated. Pick generators $i_1, \dots, i_k$ of this ideal. We show that they generate the ring I.

Suppose the generate $I_1, I_2, \dots I_k$. We want to show that they generate I_{k+1}. Pick $f \in I_{k+1}$. Then f is in an ideal J, so $f = a_1 i_1 + a_2 i_2 + \cdots + a_n i_n$ for some $a_n \in \mathbb{C}[x_1, \dots, x_n]$ with $\deg(a_i) > 0$.

Apply the Reynolds operator. Then

$$\rho(f) = \rho(a_1) i_1 + \rho(a_2) i_2 + \cdots + \rho(a_n) i_n$$

because f is invariant. So $\deg(a_n) < K$ as $\deg(i_n) > 0$, so $\rho(a_n)$ is a polynomial in $i_1, \dots, i_n$ by induction. So f is a polynomial in $i_1, \dots, i_m$. □

[4] Professor Borcherds showed us an invariant where the first generator took 13 pages to write out. Someone in the 19th century had a lot of spare time.

[5] Reynolds actually studied fluid dynamics. He showed that fluid flow averaged over time was a group.

The following example illustrates the reason we need to be careful about showing that $i_1, \ldots, i_k$ generate I.

Example 1.6. Let $R = \mathbb{C}[x, y]$, and take the subring containing the ideal generated by x and 1. This subring is not finitely generated as a ring.

Example 1.7. Let $G = \mathbb{Z}/n\mathbb{Z}$ act on $\mathbb{C}[x, y]$. Suppose that G is generated by σ, where $\sigma^n = 1$. Let $\sigma(x) = \zeta x$ and $\sigma(y) = \zeta y$, where $\zeta = e^{2\pi i/n}$. The ring of invariants is the polynomials with all terms of degree $0, n, 2n, \ldots$. A set of $n+1$ generators is $x^n, x^{n-1}y, x^{n-2}y^2, \ldots, y^n$. If we call these $a_n, a_{n-1}, \ldots, a_0$ respectively, there are many relations between the a_i. For example, $a_n a_{n-2} = a_{n-1}^2$.

Are the collection of syzygies finitely generated? Yes. The ring of invariants is given by a polynomial ring in generators $a_0, \ldots, a_n$ mod the ideal of syzygies. So the ideal of syzygies is finitely generated by Hilbert's theorem.