LECTURE 9, THURSDAY MARCH 11, 2004

FRANZ LEMMERMEYER

1. Elimination Theory

We know that a line and a curve of degree n intersect in exactly n points if we work in the projective plane over some algebraically closed field K. Using the fact that conics can be parametrized, it is not hard to show that a conic and a curve of degree n intersect in exactly $2n$ points. This seems to suggest that two curves of order m and n meet in exactly mn points if we define multiplicities carefully. This is easier said than done; given two curves $\mathcal{C}_f : f(x,y) = 0$ and $\mathcal{C}_g : g(x,y) = 0$ it is not even clear how we may compute the points of intersection, because we cannot simply solve g for y and then plug the result into f.

Yet there is a process that allows us to 'eliminate' a variable from the system $f(x,y) = g(x,y) = 0$, and it involves the theory of resultants.

1.1. **Resultants.** Let R be a UFD, and consider two polynomials

$$f(X) = a_0 + a_1X + \ldots + a_mX^m,$$
$$g(X) = b_0 + b_1X + \ldots + b_nX^n$$

of degrees $m, n \ge 1$. Assume that f and g have a common factor h, say $f = uh$ and $g = vh$ for polynomials

$$u(X) = c_0 + c_1X + \ldots + c_{m-1}X^{m-1},$$
$$v(X) = d_0 + d_1X + \ldots + d_{n-1}X^{n-1},$$

where c_{m-1} and d_{m-1} are allowed to vanish. Then u and v are nonzero polynomials with

$$vf - ug = 0. \tag{1}$$

where $0 < \deg u < m$ and $0 < \deg v < n$.

Conversely, assume that (1) holds for nonzero polynomials with $0 < \deg u < \deg f$ and $0 < \deg v < \deg n$. Then the prime divisors of f must divide ug, but since $\deg u < \deg f$, not all of them can divide u. Thus some prime divisor of f must divide g.

Equation (1) can be turned into a numerical criterion for f and g to have a common factor: multiplying out and comparing coefficients shows that (1) is equivalent to the following linear system of equations in the c_i, d_i (note that $c_i = d_j = 0$ for $i \ge m$ and $j \ge n$):

$$\begin{array}{llllllllll}
a_0d_0 & & & & - b_0c_0 & & & & & = 0 \\
a_1d_0 & + a_0d_1 & & & - b_1c_0 & - b_0c_1 & & & & = 0 \\
\ldots & \ldots & & & \ldots & \ldots & & & & \\
a_md_0 & + \ldots & + a_0d_m & & - b_mc_0 & - \ldots & & - b_1c_{m-1} & & = 0 \\
 & a_md_1 & + \ldots & + a_0d_{m+1} & & - b_{m+1}c_0 & - \ldots & - b_2c_{m-1} & & = 0
\end{array}$$

The last line is $a_m d_{n-1} - b_n c_{m-1} = 0$. This system will have a nontrivial solution if and only if the determinant of the coefficients is 0. Multiplying the b_i-columns by -1 and transposing (which changes the determinant only by a factor ± 1) we find that we have a nontrivial solution of and only if $R_{f,g} = 0$, where

$$R_{f,g} = \begin{vmatrix}
a_0 & a_1 & a_2 & \dots & a_m & & & & \\
 & a_0 & a_1 & a_2 & \dots & a_m & & & \\
 & & a_0 & a_1 & a_2 & \dots & a_m & & \\
 & & & \dots & & & & & \\
 & & & & \dots & & & & \\
 & & & & a_0 & a_1 & a_2 & \dots & a_m \\
b_0 & b_1 & b_2 & \dots & b_n & & & & \\
 & b_0 & b_1 & b_2 & \dots & b_n & & & \\
 & & b_0 & b_1 & b_2 & \dots & b_n & & \\
 & & & \dots & & & & & \\
 & & & & \dots & & & & \\
 & & & & b_0 & b_1 & b_2 & \dots & b_n
\end{vmatrix}$$

This is an $(m+n) \times (m+n)$-matrix: there are n rows with a's and m rows with b's. The determinant $R_{f,g}$ is called the resultant of f and g.

Theorem 1.1. *Let R be a UFD; then the polynomials*

$$f(X) = a_0 + a_1 X + \ldots + a_m X^m,$$
$$g(X) = b_0 + b_1 X + \ldots + b_n X^n.$$

in $R[X]$ have a non-constant common divisor if and only if the following equivalent conditions are satisfied:

1. *There exist nonzero polynomials $u, v \in R[X]$ with $\deg u < \deg f$, $\deg v < \deg g$, and $vf - ug = 0$.*
2. *$R_{f,g} = 0$.*

Let me quickly illustrate this with a simple example: take $f(x) = a_0 + a_1 x + a_2 x^2$ and $g(x) = b_0 + b_1 x$, and write $u(x) = c_0 + c_1 x$ and $v(x) = d_0$. Then

$$\begin{aligned} 0 &= vf - ug \\ &= a_0 d_0 + a_1 d_0 x + a_2 d_0 x^2 - b_0 c_0 - (b_1 c_0 + b_0 c_1) x - b_1 c_1 x^2 \end{aligned}$$

boils down to the following system of equations:

$$\begin{array}{llll}
a_0 d_0 & -b_0 c_0 & & = 0 \\
a_1 d_0 & -b_1 c_0 & -b_0 c_1 & = 0 \\
a_2 d_0 & & -b_1 c_1 & = 0
\end{array}$$

This is a system of 3 equations with 3 unknowns, whose coefficient matrix is

$$\begin{pmatrix} a_0 & -b_0 & 0 \\ a_1 & -b_1 & -b_0 \\ a_2 & 0 & -b_1 \end{pmatrix}$$

Transposing and multiplying the b-rows by -1 gives the determinant above.

Discriminants. The discriminant of a polynomial f with leading coefficient $a \neq 0$ is defined by the equation $(-1)^{n(n-1)/2} a \operatorname{disc} f = R_{f,f'}$.

As an example, the discriminant of $f(X) = aX^2 + bX + c$ is

$$\operatorname{disc} f = -\frac{1}{a}\begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix} = b^2 - 4ac.$$

Proposition 1.2. *The polynomial $f = a_n x^n + \ldots + a_0 \in R[X]$ with $na_n \neq 0$ has a multiple root if and only if* $\operatorname{disc} f = 0$.

Proof. Clearly f has a multiple root if and only if f and f' have a common root; this happens if and only if $R_{f,f'} = 0$. □

2. Applications

Intersection Points. Let us now apply resultants to curves. Consider first the circle $\mathcal{C}_f : x^2 + y^2 - 2 = 0$ and the parabola $\mathcal{C}_g : y - x^2 = 0$. In this case, computing the intersection of the two curves is easy: solve the second for y and plug it into the first equation. We find the quartic $x^4 + x^2 - 2 = (x^2 - 1)(x^2 + 2) = 0$, and get $x = \pm 1, \pm\sqrt{-2}$, corresponding to the four points of intersection $(\pm 1, 1)$ and $(\pm\sqrt{-2}, -2)$.

We can do the same with resultants: Consider both polynomials as polynomials in y over the UFD $R = K[x]$. Then

$$R_{f,g} = \begin{vmatrix} 1 & 0 & x^2 - 2 \\ 1 & -x^2 & 0 \\ 0 & 1 & -x^2 \end{vmatrix} = x^4 + x^2 - 2.$$

We know that f and g have a common component if and only if $R_{f,g} = 0$. If e.g. $x = 1$, then $R_{f,g} = 0$, and indeed we have $f(1, y) = y^2 - 1$ and $g(1, y) = y - 1$.

In general, suppose that (x_0, y_0) is a point on the intersection of $\mathcal{C}_f : f(x, y) = 0$ and $\mathcal{C}_g : g(x, y) = 0$. Then $F(y) = f(x_0, y)$ and $G(y) = g(x_0, y)$ are two polynomials with the common factor $y - y_0$. This allows us to find the points of intersection of two affine curves by computing their resultants.

Implicitation. Resultants can be used for implicitation: this is the technique of finding an implicit equation of a parametrized curve. Consider

$$x = \frac{p(t)}{q(t)}, \quad y = \frac{r(t)}{s(t)}.$$

Is there a polynomial $f(X, Y)$ such that the above is a parametrization of the corresponding affine curve? As a matter of fact, there is: consider the system

$$F(t) = Xq(t) - p(t),$$
$$G(t) = Ys(t) - r(t),$$

and let $R(X, Y) = R_{F,G}$ be the resultant of these polynomials in t. Now (x_0, y_0) is in the image of some t only if $x_0 q(t) - p(t) = y_0 s(t) - q(t) = 0$, that is, if $F(t) = G(t) = 0$ for this value of t. This in turn happens only if $R(x_0, y_0) = 0$: thus $R(x, y) = 0$ is the desired equation.

As an example, consider

$$x = \frac{t^2 - 1}{t^2 + 1}, \quad y = \frac{2t}{t^2 + 1}.$$

All we have to do to find a relation between X and Y is to eliminate t; `pari` easily computes the resultant of these polynomials:

```
f=X*(t^2+1)-(t^2-1):g=Y*(t^2+1)-2*t:polresultant(f,g,t)
```

gives the result $R_{f,g} = 4X^2 + 4Y^2 - 4$, hence X and Y satisfy $X^2 + Y^2 = 1$.