Chapter 9

Resultants

9.1 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.

Resultants

Let R be a UFD, and consider two polynomials

$$\begin{aligned} f(X) &= a_0X^m + a_1X^{m-1} + \ldots + a_m, \\ g(X) &= b_0X^n + b_1X^{n-1} + \ldots + b_n \end{aligned}$$

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

$$\begin{aligned} u(X) &= c_0X^{m-1} + \ldots + c_{m-2}X + c_{m-1}, \\ v(X) &= d_0X^{n-1} + \ldots + d_{n-1}X + d_{n-1}, \end{aligned}$$

where c_0 and d_0 are allowed to vanish. Then u and v are nonzero polynomials with

$$vf - ug = 0. \tag{9.1}$$

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

Conversely, assume that (9.1) 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 (9.1) can be turned into a numerical criterion for f and g to have a common factor: multiplying out and comparing coefficients shows that (9.1) is equivalent to the following linear system of equations in the c_i, d_i:

$$\begin{array}{llllllll}
a_0d_0 & & & & -\,b_0c_0 & & & =0\\
a_1d_0 & +\,a_0d_1 & & & -\,b_1c_0 & -\,b_0c_1 & & =0\\
\dots & \dots & & & \dots & \dots & & \\
a_{n-1}d_0 & +\,\dots & +\,a_0d_{n-1} & & -\,b_{n-1}c_0 & -\,\dots & & =0\\
a_nd_0 & +\,\dots & +\,a_1d_{n-1} & & -\,b_nc_0 & -\,\dots & & =0\\
a_{n+1}d_0 & +\,\dots & +\,a_2d_{n-1} & & & -\,b_nc_1- & \dots & =0\\
\dots & \dots & & & \dots & \dots & & \\
a_md_0 & +\,\dots & +\,a_{m-n+1}d_{n-1} & & & -\,\dots & -\,b_1c_{m-1} & =0\\
 & a_md_1+\dots & +\,a_{m-n+2}d_{n-1} & & & -\,\dots & -\,b_2c_{m-1} & =0\\
\dots & \dots & & & \dots & \dots & & \\
 & & a_md_{n-1} & & & & -\,b_nc_{m-1} & =0
\end{array}$$

This homogeneous system of linear equations 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. It is a simple exercise to show that $R_{f,g} = (-1)^{mn} R_{g,f}$.

Theorem 9.1.1. *Let R be a UFD and consider the polynomials*

$$f(X) = a_0X^m + \dots + a_{m-1}X + a_m,$$
$$g(X) = b_0X^n + \dots + b_{n-1}X + b_n$$

in $R[X]$. Then the following assertions are equivalent:

1. *f and g have a nontrivial common factor:* $\deg \gcd(f, g) > 0$*;*

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

3. $R_{f,g} = 0$.

Let me quickly illustrate this with a simple example: take $f(x) = a_0x^2 + a_1x + a_2$ and $g(x) = b_0x + b_1$, and write $u(x) = c_0x + c_1$ and $v(x) = d_0$. Then

$$\begin{aligned} 0 &= vf - ug \\ &= a_0d_0x^2 + a_1d_0x + a_2d_0 - b_0c_0x^2 - (b_1c_0 + b_0c_1)x - b_1c_1 \end{aligned}$$

boils down to the following system of equations:

$$\begin{array}{llll} a_0d_0 & -b_0c_0 & & = 0 \\ a_1d_0 & -b_1c_0 & -b_0c_1 & = 0 \\ a_2d_0 & & -b_1c_1 & = 0 \end{array}$$

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 monic polynomial f is defined by the equation

$$\operatorname{disc} f = (-1)^{n(n-1)/2} R_{f,f'}$$

.

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

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

Proposition 9.1.2. *The polynomial $f = x^n + a_1x^{n-1} \ldots + a_n \in R[X]$ with $n \neq 0$ 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 $R_{f,f'} = 0$. □

We remark without proof the following "explicit" formula for the resultant of two polynomials:

Theorem 9.1.3. *Let $f(X) = a_0X^m + \ldots + a_m$ and $g(X) = b_0X^n + \ldots + b_n$ be polynomials with roots α_i and β_j, respectively. Then*

$$R(f,g) = a_0^n b_0^m \prod_i \prod_j (\alpha_i - \beta_j) = a_0^m \prod_i g(\alpha_i).$$

This formula shows again that $R(f,g) = 0$ if and only if f and g have a common root.

9.2 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 $(\pm\sqrt{-2}, -2)$.

Here's how you can solve the same problem (and, of course, other and more difficult problems) using resultants. Assume that you are given two affine curves $\mathcal{C}_f : f(x,y) = 0$ and $\mathcal{C}_g : g(x,y) = 0$, and assume that (x_0, y_0) is a point of intersection. Then $f(x_0, y_0) = g(x_0, y_0) = 0$. Now consider the resultant $R_{F,G}$ of the polynomials $F(y) = f(x_0, y)$ and $G(y) = g(x_0, y)$. Since $F(y_0) = G(y_0)$, both polynomials have the factor $y - y_0$ in common. Thus we must have $R_{F,G} = 0$. Now consider f and g as polynomials in y, i.e. as elements in $R[Y]$ with $R = K[X]$, and let $R_{f,g}(x)$ denote their resultant. This will be a polynomial in x with the property that $R(x_0) = 0$. Thus we have shown:

Proposition 9.2.1. *Let $\mathcal{C}_f : f(x,y) = 0$ and $\mathcal{C}_g : g(x,y) = 0$ be affine curves. If $(x_0, y_0) \in \mathcal{C}_f \cap \mathcal{C}_g$, then x_0 is a root of the resultant $R_{f,g}(x)$, where we have interpreted f and g as polynomials in $R[y]$ with $R = K[x]$.*

In order to compute all points of intersection, compute the roots x_0 of $R_{f,g}(x)$ as above; then compute the roots y_0 of $R_{f,g}(y)$ (interchange the roles of x and y above) and then check which of the finitely many points (x_0, y_0) are on $\mathcal{C} \cap \mathcal{D}$.

In the example above, we get

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

The solutions are $x = \pm 1, \pm\sqrt{-2}$.

Plugging these values of x e.g. into $f(x,y) = 0$ and solving for y gives the points of intersection $(\pm 1, 1)$ and $(\pm\sqrt{-2}, -2)$. Alternatively, we can compute

the resultant $R_{f,g}(y)$ by eliminating x and get

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

Thus $y = 1$ and $y = -2$. Now look at all combinations (x, y) with $x \in \{\pm 1, \pm\sqrt{-2}\}$ and $y \in \{1, -2\}$ are on the curves; again we find the four points of intersection $(\pm 1, 1)$ and $(\pm\sqrt{-2}, -2)$.

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

$$\begin{aligned} F(t) &= Xq(t) - p(t), \\ G(t) &= Ys(t) - r(t), \end{aligned}$$

and let $R(X, Y) = R_{F,G}$ be the resultant of these polynomials in t. Now (x_0, y_0) is on the parametrized curve if and only if $x_0 q(t_0) - p(t_0) = y_0 s(t_0) - q(t_0) = 0$, that is, if $F(t_0) = G(t_0) = 0$. This in turn happens if and only if $t - t_0$ is a common factor of F and G, which is equivalent to $R(x_0, y_0) = 0$. Thus (x_0, y_0) is on the curve defined by $R(x, y) = 0$.

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 $X^2 + Y^2 = 1$.

Minimal Polynomials

Let α and β be algebraic numbers. Then there exist polynomials $f, g \in \mathbb{Q}[X]$ with $f(\alpha) = g(\beta) = 0$. From algebraic number theory you know that $\alpha + \beta$ is also algebraic. Resultants allow you to compute a polynomial $h \in \mathbb{Q}[X]$ such that $h(\alpha + \beta) = 0$.

Here's how: put $x = \alpha + \beta$ and consider the polynomials $F(Y) = f(x - Y)$ and $g(Y)$. The resultant of F and g is $R_{F,g}$; note that $F(\beta) = f(\alpha) = 0$ and $g(\beta) = 0$. Thus F and g have the common factor, hence $R_{F,g} = 0$.

This means that if we consider $\phi(Y) = f(X - Y)$ and $g(Y)$ as polynomials over $R[Y]$ with $R = \mathbb{Q}[X]$, then the resultant $R_{\phi,g}(X) \in \mathbb{Q}[X]$ has the property that $R_{\phi,g}(\alpha + \beta) = 0$.

As an example, let us compute the minimal polynomial of $\sqrt{2} + \sqrt[3]{2}$. We know that $f(X) = x^2 - 2$ and $g(x) = x^3 - 2$, and typing

```
polresultant((x-y)^2-2,y^3-2,y)
```

into `pari` shows that $R(x) = x^6 - 6x^4 - 4x^3 + 12x^2 - 24x - 4$.

As a more involved example, consider $\alpha = \sqrt{2} + \sqrt{3}$ and $\beta = \sqrt{5} + \sqrt{6}$; then we find that $\alpha + \beta$ is an element of $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{6}\,)$, hence should have a minimal polynomial of degree dividing 8. The resultant

```
r = polresultant((x-y)^4-10*(x-y)^2+1,y^4-22*y^2+1,y)
```

has degree 16, but factors into two polynomials of degree 8 each:

```
factor(r)
```

gives the two polynomials

$$a(x) = x^8 - 64x^6 - 96x^5 + 808x^4 + 1152x^3 - 2304x^2 - 1152x + 144,$$
$$b(x) = x^8 - 64x^6 + 96x^5 + 808x^4 - 1152x^3 - 2304x^2 + 1152x + 144.$$

Note that $b(x) = a(-x)$ here. In any case, $\alpha + \beta$ is the root of one of these polynomials. Now

$$\alpha + \beta = 7.8318\ldots,$$

and evaluating a and b at this value shows

$$a(\alpha + \beta) \approx -6.5 \cdot 10^{-22}, \quad b(\alpha + \beta) \approx 4568619.30\ldots;$$

thus the minimal polynomial of $\alpha + \beta$ is $a(x)$.

Similarly we can compute the minimal polynomial of α/β: consider the polynomials $F(Y) = f(XY)$ and $G(Y) = g(Y)$: then for $X = \alpha/\beta$, F and G have a common root $Y = \beta$, hence $X = \alpha/\beta$ must be a root of $R_{F,G} = 0$.

In our example above,

```
polresultant((xy)^2-2,y^3-2,y)
```

gives $R(X) = 4X^6 - 8$, hence $X^6 - 2$ is a minimal polynomial (it is Eisenstein for the prime 2, hence irreducible) for $\sqrt{2}/\sqrt[3]{2} = \sqrt[6]{2}$.

Note that the theory of resultants gives a constructive proof of the fact that algebraic numbers form a field, and that algebraic integers form a ring.