137 NOTES, PART 3: ALGEBRA SKETCH

Z. RAN

1. Rings and polynomial factorization

The general strategy for studying a plane curve C given by a polynomial equation $f(x, y) = 0$ is to view f as a polynomial in y, say, with coefficients which are polynomials in x:

$$f(x, y) = a_n(x)y^n + ... + a_1(x)y + a_0(x)$$

Thus we view f as a family $\{f(a, y) : a \in \mathbb{A}^1\}$ of 'ordinary' polynomials in y, one for each $a \in \mathbb{A}^1$. Geometrically, this corresponds to projecting

$$\pi : C \to \mathbb{A}^1$$

C to the x-axis and viewing C as made up of a family of cycles $\pi^{-1}(a) =$ Zeros$(f(a, y)$ for $a \in \mathbb{A}^1$. Making good on this idea requires studying polynomials in 1 variable with coefficients that are something more general than elements of one of our fields $\mathbb{F}$; indeed the coefficients need to be something at least as general as elements of $\mathbb{F}[x]$. It turns out that the right sort of structure of the set of coefficients is that of *ring*. Our next aim, then, is to present a condensed, but largely self-contained sketch of the necessary topics from ring theory. A more complete account is given in courses such as Math 171-2, and of course also in textbooks such as those used in those courses (e.g. Fraleigh-Beauregard). It would be a good idea to have a copy of such a text handy as we go through this portion of the course.

A *group* is by definition an abstract algebraic system consisting of a (nonempty) set G of elements, together with an operation denoted $*$, satisfying a suitable set of axioms, as follows

- $*$ is associative;
- $*$ admits a neutral element, denoted e;
- every element $a \in G$ admits an inverse with respect to $*$.

If the group operation $*$ is commutative, G is said to be a commutative or abelian group. Examples of groups include $\mathbb{F}^n$, $\mathbb{Z}$ (both

Date: March 19, 2006.

abelian), with operation + and neutral element 0; $\mathrm{GL}_n, \mathrm{PGL}_n, \mathrm{Aff}_n$ (non-abelian) with operation composition or matrix multiplication and neutral element the identity.

A *ring* is by definition an abstract algebraic system consisting of a (nonempty) set R of elements, together with two operations named 'plus' and 'times', denoted $+, \cdot$, satisfying axioms as follows

- Under $+$, R forms an abelian group with neutral element denoted 0;
- $\cdot$ is associative;
- the appropriate distributive laws hold, linking $+$ and $\cdot$.

Two other properties not part of the general definition of a ring, but which we shall always assume unless explicitly mentioned otherwise are

- commutativity: $\cdot$ is commutative;
- unitarity: $\cdot$ admits a neutral element, denoted 1.

Examples of rings:

- Perhaps the most important example for our purposes is $\mathbb{F}[x]$, the ring of polynomials with coefficients in $\mathbb{F}$, with the usual addition and multiplication operations. Similarly, we have a polynomial ring in any number n of variables, denoted $\mathbb{F}[x_1, ..., x_n]$
- Of course $\mathbb{F}$ itself is a ring, as is the ring of integers $\mathbb{Z}$.
- For any natural number $m > 1$ there is a ring denoted $\mathbb{Z}_m$ or $\mathbb{Z}/(m)$ of residue classes modulo m of integers.

A ring is said to be an *integral domain* if the product of nonzero elements is nonzero. A *field* is an integral domain such that every nonzero element admits a multiplicative inverse. Important examples of fields, besides the concrete fields $\mathbb{F} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ we've worked with before, include the fields $\mathbb{F}(x)$ of *rational functions with coefficients in* $\mathbb{F}$, i.e.

$$\mathbb{F}(x) = \{r(x) = f(x)/g(x) : f, g \in \mathbb{F}[x]\}.$$

The following result is no more than an abstraction of fraction arithmetic from middle school

Proposition 1.1. *Given an integral domain D, there exists a field K containing D, called the field of fractions of D, which consists of elements of the form $a/b, a, b \in D, b \neq 0$.*

For example, the field of fractions of $\mathbb{Z}$ is of course $\mathbb{Q}$; the field of fractions of $\mathbb{F}[x]$ is $\mathbb{F}(x)$, the field of rational functions.

Now given a ring R, we can construct another ring denoted $R[x]$ of polynomials in x with coefficients in R. Similarly for $R[x_1, ..., x_n]$. At least some of the important properties of ordinary polynomials carry over to this generality:

Theorem 1.2. *(Division algorithm) Let D be an integral domain, $f, g \in D[x]$ polynomials with $g \neq 0$.*

(i) There exist $q, r \in D[x], a \neq 0 \in D$ with $\deg(r) < \deg(g)$ such that $af = qg + r$.

(ii) if g is monic (more generally, if the leading coefficient of g has a multiplicative inverse in D), then we can take $a = 1$, so $f = qg + r$.

Proof. Write

$$f = a_n x^n + ... + a_0, g = b_m x^m + ... + b_0, a_n, b_m \neq 0.$$

We use induction on $n = \deg(f)$. If $n < m$, we can take $q = 0, r = f, a = 1$ and we're done. Else, let

$$f' = b_m f - a_n x^{n-m} g$$

and note that $\deg(f') < n$. By induction, we can write

$$a' f' = q' g + r', \deg(r') < m$$

Plugging in, we get

$$a' b_m f = (q' + a_n a x^{n-m})g + r'.$$

Moreover, if g is monic, i.e. $b_m = 1$, we can by induction take $a' = 1$ so we are done. The case b_m invertible is similar. □

Exercise 1.1. *Carry out the division algorithm for the following polynomials f, g over the respective domains D:*

(1) $f = 4x^3 - 2x^2 + 5x - 3, g = x^2 + x + 1, D = \mathbb{Z}$
(2) $f = x^5 + 5x^3 + 3x^2 + 2, g = x^2 + 4x + 5, D = \mathbb{Z}$
(3) *Same f,g, as previous 2 items, $D = \mathbb{Z}/7$.*

The division algorithm admits an important refinement as follows.

Theorem 1.3. *(gcd algorithm) Let K be a field and $f, g \in K[x]$. Then there exists $h \in K[x]$ such that*

(i) $h|f, g$;
(ii) there exist $A, B \in K[x]$ such that $h = Af + Bg$;
(iii) any polynomial k dividing f and g divides h.

Because of property (iii), h is called the *greatest common divisor* of f, g.

Proof. First, we note that (i) and (ii) imply (iii): because if $f = ku, g = kv$ then $h = (Au + Bv)k$. Now to construct h, start by dividing f by g:

$$f = q_1 g + r_1, \deg(r_1) < \deg(g). \tag{1}$$

For notational consistency, it will be convenient to set $r_0 = g, r_{-1} = f$. If $r_1 = 0$, then $g|f$ and we can just take $h = g$. Else, divide g by r_1:

$$g = q_2 r_1 + r_2, \deg(r_2) < \deg(r_1). \tag{2}$$

If $r_2 = 0$, it is easy to see that we can take $h = r_1$. Else, we next divide r_1 by r_2:

$$r_1 = q_3 r_2 + r_3, \deg(r_3) < \deg(r_2) \tag{3}$$

$$...$$

$$r_i = q_{i+2} r_{i+1} + r_{i+2}, \deg(r_{i+2}) < \deg(r_{i+1}) \tag{4}$$

$$...$$

Since the degrees keep dropping, the process must stop eventually. Let p be smallest so that $r_{p+1} = 0$, i.e.

$$...$$

$$r_{p-2} = q_p r_{p-1} + r_p \tag{5}$$

$$r_{p-1} = q_{p+1} r_p. \tag{6}$$

Set $h = r_p$ Thus $h|r_{p-1}$. From the last display, we see that $h|r_{p-2}$ as well. Continuing backwards, we see that $h|r_i$ for all i, hence $h|g$ and then finally $h|f$ as well, which shows (i). To show (ii), write

$$\begin{aligned} h = r_p &= r_{p-2} - q_p r_{p-1} \\ &= r_{p-2} - q_p(r_{p-3} - q_{p-1} r_{p-2}) \\ &= -q_p r_{p-3} + (1 + q_p q_{p-1}) r_{p-2} \\ &... \\ &= *r_i + *r_{i+1} \\ &... \\ &= Af + Bg \end{aligned}$$

□

Exercise 1.2. *Carry out the gcd algorithm for the following polynomials f, g over the respective fields $\mathbb{F}$:*

(1) $f = x^4 - x^2 - 2, g = x^3 + x^2 + x + 1, \mathbb{F} = \mathbb{Q}$
(2) $f = x^3 + 1, g = x + 2, \mathbb{F} = \mathbb{Q}$
(3) *Same f, g as in previous 2 items,* $\mathbb{F} = \mathbb{Z}/5$.

Corollary 1.4. *If K is a field, $f, g, h \in K[x]$, f is irreducible and $f|gh$, then either $f|g$ or $f|h$.*

Proof. Suppose $f \nmid g$. Since f is irreducible the gcd of f and g must be 1, therefore

$$1 = Af + Bg$$

as in the Theorem. Therefore

$$h = Afh + Bgh.$$

As $f|gh$ it foollows that $f|h$. $\square$

Definition 1. *Let D be an integral domain, $a, b, c \in D$.*

- *a is said to be a* unit *in D if a has a multiplicative inverse in D.*
- *a is said to* divide *b, $a|b$, if $b = ca$ for some $c \in D$. If c is a unit, a and b are said to be* associates *in D.*
- *a is said to be* reducible *if $a = bc$ with b, c both nonunits. If a is not reducible and not a unit, we say it is* irreducible.
- *D is said to be* factorial *if any nonzero nonunit $a \in D$ can be written as*

$$a = a_1 \cdots a_r$$

with $a_1, ..., a_r$ irreducible, and this expression is essentially unique: if also

$$a = b_1 \cdots b_s$$

with $b_1, ..., b_s$ irreducible, then after some permutation, each a_i is associate to b_i.

For example, the *Fundamental Theorem of Arithmetic* states that the ring of integers is factorial. It is a fairly easy consequence of Cor. 1.4 that for any field K, the polynomial ring $K[x]$ is factorial, but below we shall prove a much stronger result: for any factorial domain$D$, the polynomial ring $D[x]$ is factorial. Working towards that proof will occupy us for some time. Our general strategy will be to consider the fraction field K of D. Then elements of $D[x]$ are also in $K[x]$, and may be factored as such. We then try to study the denominators involved, to deduce from a factorization in $K[x]$ one in $D[x]$. In this study, the notion of *content* of a polynomial in $D[x]$ will play a large role.

Note that for any factorial domain D and nonzero elements $a, b, \in D$, a and b have a greatest common divisor $c \in D$, uniquely determined up to associates: c is just the product of all irreducible elements appearing in the irreducible factorization of both a and b, with each such element q appearing with an exponent that is the minimum of its exponents in a and b. For example in $D = \mathbb{Z}$, the gcd of $2 \cdot 3^3 5^2$ and $-3 \cdot 5^5$ is $\pm 35^2$.

Similarly, given any collection (even infinite) of nonzero elements $a_1, a_2, \ldots \in D$, there is a greatest common divisor $c \in D$ of these elements, and c is uniquely determined up to associates.

Lemma 1.5. *Let D be an integral domain, $a \in D$ and $f \in D[x]$. Then $a|f$ in $D[x]$ iff a divides every coefficient of f.*

From now on, we denote by D a factorial domain. By definition, the *content*, denoted $c(f)$, of a polynomial $f = a_n x^n + \ldots + a_1 x + a_0 \in D[x]$ is the gcd in D of $a_0, \ldots, a_n$. $c(f)$ is well defined up to an invertible factor, i.e. up to associates. f is said to be *primitive* if if its content is (associate to) 1. For any $f \in D[x]$, we can factor out the content and write f in the form

$$f = c(f) f_1$$

where $f_1 \in D[x]$ in primitive, called the primitive part of f. For example, $4 + 6x = 2(2 + 3x)$ so $4 + 6x$ has content ± 2 and primitive part $\pm(2 + 3x)$.

Note that if f is primitive and $f = gh, g, h \in D[x]$ then

$$f = c(g) g_1 c(h) h_1,$$

therefore $c(g)c(h)|f$. Since f is primitive, $c(g)$ and $c(h)$ must be units, so that g, h are primitive. Thus *a factor of a primitive polynomial is primitive.*

Lemma 1.6. *Let $a, b, c \in D$ with a irreducible. If $a|bc$ then either $a|b$ or $a|c$.*

Proof. By assumption, there exists $d \in D$ with

$$ad = bc.$$

Let's factor b, c, d in irreducible factors:

$$d = d_1 \cdots d_r, b = b_1 \cdots b_s, c = c_1 \cdots c_t.$$

Thus,

$$ad_1 \cdots d_r = b_1 \cdots b_s c_1 \cdots c_t$$

By uniqueness of the decomposition, we have that a must be associate to one of the factors on the right, i.e b_i or c_i for some i. But then $a|b$ or $a|c$. □

Theorem 1.7. *(Gauss' Lemma) Suppose $a \in D$ is irreducible and $a|fg$ where $f, g \in D[x]$. Then either $a|f$ or $a|g$.*

Proof. Write

$$f = b_0 + \ldots + b_n x^n, g = c_0 + \ldots + c_m x^m.$$

Arguing by contradiction, suppose $a \nmid f, a \nmid g$. Let p, q be smallest so that

$$a \nmid b_p, a \nmid c_q.$$

Then the coefficient d_{p+q} of x^{p+q} in fg can be written as follows

$$d_{p+q} = (b_0 c_{p+q} + ... + b_{p-1} c_{q+1}) + b_p c_q + (b_{p+1} c_{q-1} + ... + b_{p+q} c_0$$

By assumption a divides $b_0, ..., b_{p-1}$, therefore a divides the first term in parentheses above. Similarly. a divides the last term in parentheses. By assumption again, a divides d_{p+q}. Therefore $a|b_p c_q$. But this contradicts the last Lemma. □

Theorem 1.8. *Let K be the fraction field of D and $f \in D[x]$ irreducible. Then f is irreducible in $K[x]$.*

Proof. Suppose

$$f = g'h'$$

where $g', h' \in K[x]$ are non-constant. Take $a, b \in D$ such that

$$g := ag', h := bh' \in D[x]$$

(i.e. a, b are 'common denominators' for f, g respectively). Let $d = ab$. Then

$$df = gh$$

Let e be an irreducible factor of d. Then $e|gh$. Therefore by Gauss' Lemma, $e|g$ or $e|h$. We may assume the former. Then let $g_1 = g/e \in D[x], h_1 = h, d_1 = d/e$, so we have

$$d_1 f = g_1 f_1.$$

Continuing in this way, we may 'peel off' all irreducible factors of d and eventually reach an equality

$$f = g_k h_k$$

with $g_k, h_k \in D[x]$ nonconstant. This shows f is reducible in $D[x]$. □

Theorem 1.9. *Suppose $f, g, h \in D[x]$, f is irreducible and $f|gh$. Then $f|g$ or $f|h$.*

Proof. If $f \in D$ this is just Gauss' Lemma. So suppose f is nonconstant, hence not a unit in $K[x]$. By the previous result, f is irreducible in $K[x]$. Therefore by Cor. 1.4, either $f|g$ or $f|h$ in $K[x]$. Suppose $f|h$, so that $h = fk, k \in K[x]$. Let $a \in D$ be a common denominator for the coefficients of k, i.e $ak \in D[x]$. Thus

$$ah = afk.$$

Let $e \in D$ be an irreducible factor of a. Since e divides $f(ak)$ and f is irreducible, e divides ak. So let $a_1 = a/e \in D, k_1 = ak/e \in D[x]$. Then

$$a_1 h = f k_1.$$

Continuing to peel off factors of e as in the proof of the previous result, we get eventually

$$h = f k_n$$

so that $f|h$ in $D[x]$. The case $f|g$ is similar. □

Theorem 1.10. *If D is factorial then so is $D[x]$*

Proof. We claim first that any nonzero $f \in D[x]$ is a product of irreducible elements. Write $f = c(f)f_1$ with f_1 primitive. As $c(f) \in D$ and D is factorial, $c(f)$ is a product of irreducibles. As for f_1, if it is irreducible, we are done. If not, write $f_1 = f_2 f_3, f_2, f_3 \in D[x]$ non-units. As f_1 is primitive, f_2, f_3 cannot be constant, therefore both of them have degree $< \deg(f_1)$. By an induction on the degree, we may assume both f_2 and f_3 are products of irreducibles, hance so is $f = c(f)f_2 f_3$.

For uniqueness of the decomposition, suppose

$$f_1 \cdots f_r = g_1 \cdots g_s$$

with $f_1, ...g_s \in D[x]$ irreducible. As $g_1 | f_1 \cdots f_r$, Theorem ? implies that $g_1 | f_i$ for some i. Renumbering, we may assume $g_1 | f_1$ and since both are irreducible it follows that they are associate, i.e. $f_1 \sim g_1$. Cancelling them off, we get

$$f_2 \cdots f_r \sim g_2 \cdots g_s$$

and we may continue the argument with g_2 in place of g_1. Eventually, we conclude that up to renumbering, each g_i and f_i are associate, which proves uniqueness.

□

Proposition 1.11. *Suppose $f, g \in D[x]$ have a nonconstant common factor in $K[x]$. Then f, g have a common factor in $D[x]$.*

Proof. We may assume f, g have no nonunit common factor in D (else, factor out this factor). By assumption, there exists $h \in K[x]$ nonconstant such that $h|f, g$ in $K[x]$. Clearing denominators, we find $h_1 \in D[x]$ which we may assume is primitive, and $a \in D$ such that

$$h_1 | af, ag$$

in $D[x]$. Let's decompose h_1 in irreducible factors:

$$h_1 = p_1 \cdots p_k.$$

As h_1 primitive, each p_i is nonconstant. Because $p_i|af$, p_i must divide f for each i. Similarly, $p_i|g$ for each i. Therefore f, g have nonconstant common factors in $D[x]$. $\square$

Proposition 1.12. *Suppose $f, g \in K[x]$ have degree m, n, respectively. Then f, g have a nonconstant common factor in $K[x]$ iff there exist $u, v \in K[x]$ of degrees at most $n-1, m-1$ respectively, such that $uf + bg = 0$.*

Proof. $\Rightarrow$: if h is a nonconstant common factor of f, g, then

$$\frac{g}{h}f - \frac{f}{h}g = 0$$

so we can just take $u = g/h, v = -f/h$.

$\Leftarrow$: if $uf = -vg$ and f has no common factor with g, then f must divide v, which is impossible because $\deg(v) < \deg(f)$. $\square$

Corollary 1.13. *Let $f, g \in D[x]$ with D factorial. Then f, g have a nonconstant factor in $D[x]$ iff there exist $u, v \in K[x]$ of degrees at most $n-1, m-1$ respectively, such that $uf + bg = 0$.*

2. The resultant

Let $f = a_0 + a_1 x + \ldots + a_m x^m, g = b_0 + b_1 x + \ldots + b_n x^n \in D[x]$, where D is an factorial domain whose fraction field we denote by K. Define the *resultant matrix* of f, g, denoted

$$R = R_{m,n}(f, g)$$

as the following $(m+n) \times (m+n)$-matrix:

$$R = \begin{bmatrix} a_0 & & \ldots & a_m & 0 & \ldots & 0 \\ 0 & a_0 & \ldots & & a_m & \ldots & 0 \\ & & & \ldots & & & \\ & & & & a_0 & \ldots & a_m \\ b_0 & & \ldots & b_n & 0 & \ldots & 0 \\ 0 & b_0 & \ldots & & b_n & \ldots & 0 \\ & & & \ldots & & & \\ & & & & b_0 & \ldots & b_n \end{bmatrix} \tag{7}$$

Thus, the first n rows of R contain the coefficient vector of f, gradually shifting rightward, and similarly for the last m rows and the coefficient vector of g. The *resultant* (or *resultant determinant* is the element of D defined by

$$r(f, g) = r_{m,n}(f, g; x) := \det(R). \tag{8}$$

To simplify notation, we will omit the m, n subscripts or the $;x$ designation when understood (e.g. when m, n are *exactly* equal to the degrees of f, g, respectively). Note that $r(f, g)$ may be viewed as a polynomial with $\mathbb{Z}$ coefficients in in the coefficients $a_0, ..., b_n$ which themselves may be viewed as indeterminates (i.e. formal symbols). So there is no loss of generality in taking our domain D to be the polynomial ring $\mathbb{Z}[a_0, ..., b_n]$ with $a_0, ..., b_n$ indeterminates.

To explain the special shape of R and the meaning of $r(f, g)$, let us denote by V_i the K-vector space of all polynomials of degree $< i$ with coefficients in K. As we know, V_i is an i-dimensional vector space with standard basis $1, ..., x^{i-1}$. Given i, j, we can define another vector space, denoted $V_i \oplus V_j$ by

$$V_i \oplus V_j = \{(u, v) : u \in V_i, v \in V_j\}.$$

The vector space structure of $V_i \oplus V_j$ is such that $(u, v) = (u, 0) + (0, v)$. Then $V_i \oplus V_j$ is a vector space with basis

$$\mathcal{B} = ((1, 0), (x, 0), ..., (x^{i-1}, 0), (0, 1), (0, x), ..., (0, x^{j-1})).$$

Thus, $V_i \oplus V_j$ is a vector space of dimension $i + j$. Now, returning to our polynomials f, g, define a map

$$N(f, g) : V_n \oplus V_m \to V_{m+n},$$

by

$$N(f, g)(u, v) = uf + vg. \tag{9}$$

$N(f, g)$ is clearly a linear transformation, and note that both its source and target have the same dimension (that is, $m + n$). Then

$R(f, g)$ is the transpose of the matrix of $N(f, g)$ with respect to the basis $\mathcal{B}$ of $V_n \oplus V_m$ and the standard basis of V_{m+n}.

Now the theory of determinants tells us:

$r(f, g) = 0$ iff $R(f, g)$ is a singular matrix iff the nullspace $\ker(N(f, g))$ *is a nonzero subspace.*

We now invoke Cor 1.13 which tells us that $\ker(N(f, g))$ is nonzero precisely when f, g have a nonconstant common factor in $D[x]$ (or equivalently, in $K[x]$). We have proven:

Theorem 2.1. *Two polynomials $f, g \in D[x]$ of degrees m, n exactly, respectively, have a common factor of positive degree in $D[x]$ iff they have a common factor of positive degree in $K[x]$ iff the resultant $r(f, g) = r_{m,n}(f, g) = 0$.*

It often happens that we want to apply a resultant criterion to check for common factors but know only an upper bound on the degrees of f, g. Then we can use

Theorem 2.2. *Let $f, g \in D[x]$ be two polynomials of degrees at most m, n, respectively. Then $r_{m,n}(f,g) = 0$ iff either $\deg(f) < m$ and $\deg(g) < n$ or f, g have a common factor of positive degree in $D[x]$.*

Proof. Use induction on $m+n$. It suffices to prove that if $r_{m,n}(f,g) = 0$ but f, g have no common factor, then $\deg(f) < m$ and $\deg(g) < n$. By the previous result, we may assume one of f, g, say f, as degree $< m$. Then in (7) we have $a_m = 0$. Doing a last-column expansion of the determinant, we see that

$$r_{m,n}(f,g) = \pm b_n r_{m-1,n}(f,g) \tag{10}$$

By induction, $r_{m-1,n}(f,g) \neq 0$. Hence $b_n = 0$, i.e. $\deg(g) < n$.

□

Another way to state this result is the following.

Theorem 2.3. *Let $f, g \in D[x]$ be two polynomials of degrees at most m, n, respectively, and set*

$$F = \mathrm{hog}_m(f), G = \mathrm{hog}_n(g). \tag{11}$$

Then $r_{m,n}(f,g) = 0$ iff F, G have a common factor of positive degree in $D[x]$.

Proof. We have

$$F = X_0^m f(X_1/X_0), G = X_0^n g(X_1/X_0). \tag{12}$$

Thus X_0 is a common factor of F, G iff $\deg(f) < m$ and $\deg(g) < n$. Any common factor of F, G that is not a power of X_0 dehomogenizes to a nonconstant common factor of f, g. Thus our claim follows from the previous result. □

To get a slightly neater statement, we can work directly with homogenous polynomials and their 'homogenous resultant', defined as follows. Let $F, G \in D[X_0, X_1]$ be homogenous polynomials, of degrees m, n respectively. Then we define the 'homogenous resultant'

$$r = r^h(F,G) = r^h(F,G;X_0,X_1) = \det R \tag{13}$$

where R is the resultant matrix as in 7; in other words,

$$r = r_{m,n}(f,g)$$

where f, g are the dehomogenizations of f, g (which, in general, have degrees $\leq m, \leq n$, respectively). Then we have the following .

Theorem 2.4. *Two homogenous polynomials $F, G \in D[X_0, X_1]$ have a nonconstant common factor iff their homogenous resultant $r^h(F,G) = 0$.*

Proof. Using the notations of Thm 2.3, we have $F = h_m(f), G = h_n(g), r = r_{m,n}(f,g)$, so the result follows from Thm 2.3. Note that the case $\deg(f) < m, \deg(g) < n$ corresponds to F, G having common factor X_0^k. Any other common factor dehomogenizes to a non-constant common factor of f, g (we shall prove later that any such common factor is automatically *homogeneous*). □

Example 2.5. A nice application of resultants is to elimination theory. Thus let $(p_1(t)/q_1(t), p_2(t)/q_2(t))$ be a pair of rational functions. Together, they yield a 'rational mapping'

$$\phi(t) = (p_1(t)/q_1(t), p_2(t)/q_2(t)) : \mathbb{A}^1 \to \mathbb{A}^2$$

(defined where $q_1(t), q_2(t) \neq 0$). How can we find equations for the image C of ϕ?

To this end, consider

$$f = xq_1(t) - p_1(t), g = yq_2(t) - p_2(t) \in \mathbb{C}[x,y][t].$$

Then if $(x_0, y_0) \in \mathrm{im}(\phi)$ then the 'ordinary' (constant-coefficient) polynomials $f(x_0, y_0, t), g(x_0, y_0, y) \in \mathbb{C}[t]$ have a common zero in t, therefore they have a common factor, hence

$$r(f(x_0, y_0; t), g(x_0, y_0, t); t) = r(f, g; t)(x_0, y_0) = 0.$$

This means, at least, that C is contained in the zero-set of the polynomial $r(x,y) \in \mathbb{C}[x,y]$.

As a specific example, consider $\phi(t) = (t^2, t^3 - t^2)$. A calculation yields

$$r(f,g) = y^2 - x^2(x-1). \tag{14}$$

Exercise 2.1. *Prove (14).*