CHAPTER 1

Systems of polynomial equations

1. Solving univariate polynomial equations

A univariate polynomial,

$$f = f(x) = a_d x^d + a_{d-1} x^{d-1} + \ldots + a_1 x + a_0, \tag{1.0.1}$$

can be viewed as a function

$$f : k \to k,$$

where k is a *field*. In most examples here we assume that k is $\mathbb{Q}$,$\mathbb{R}$, or $\mathbb{C}$: i.e., the field of rational, real, or complex numbers, respectively.
Note: Each subsequent field in the sequence of three is an *extension* of the previous one. One way to continue the sequence is

$$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C} \subset \mathbb{H} \subset \mathbb{O}.$$

The last two, *quaternions* and *octonions*, are *division algebras* that are not fields (the multiplication is not commutative).

The above fields are of *characteristic* 0. Fields of characteristic p include, for instance, *finite fields*, which are extensively used *cryptography* and *coding theory*.

We will refer to the k-linear infinite-dimensional space of polynomials as the *ring of polynomials with coefficients in k* and denote it by $k[x]$. We will come back to a formal definition of a *ring* later, for now it is sufficient to know that a ring is a vector space with an operation of multiplication: indeed, in $k[x]$ a product of two polynomials is a polynomial.

The polynomials of degree at most d, i.e., polynomials of the form (1.0.1), form a linear subspace $k[x]_{\leq d}$ of $k[x]$ of dimension $d+1$, but not a subring, since $k[x]_{\leq d}$ is not closed under multiplication.

1.1. What does "solve" mean? For equations of degree at most 4, there exist formulas that express all their *roots* in terms of *radicals*; e.g., see *Cardano formulas* for cubics. A crowning achievement of *Galois theory* is showing that a quintic equation can **not** be solved in radicals.

If the demand of exactness of solutions is dropped, then the basic problem of solving equations can be rephrased in the following way.

PROBLEM 1.1.1. *For a polynomial $f \in \mathbb{C}[x]$ and fixed $\delta > 0$ and $\varepsilon > 0$ find $\tilde{x} \in \mathbb{C}$*

1. *such that $\|\tilde{x} - x^*\| < \delta$, where $x^* \in f^{-1}(0)$ is some exact root;*
2. *such that $\|f(\tilde{x})\| < \varepsilon$.*

The chosen numbers δ and ε are called the absolute error tolerance *and the* absolute residual tolerance*, respectively.*

Much of what is being said in this section will be generalized in the multivariate case, but until then the *norm* is simply the absolute value: i.e., $\|x\| = |x|$.
Note: There are numerous variations of this problem: one may

1. require one or both conditions above to hold,
2. restrict the search for a root to a specified region,
3. replace the word "absolute" with "relative".

In numerical analysis the distance $\Delta x = |\tilde{x} - x^*|$ is sometimes referred to the *backward error*, whereas $|f(\tilde{x})| = |f(\tilde{x}) - f(x^*)|$ is called the *forward error*. The errors that are *normalized* (that requires the presence of a norm in the space of solutions and/or the space of polynomials) are referred to as *relative*, e.g., $\Delta x/|x|$ is the relative error of approximation of a root.

1.2. Newton's method. One of the most common methods to solve Problem 1.1.1 is *Newton's method* described below. For a polynomial $f \in k[x]$, define *Newton's operator*

$$N_f : k \to k, \quad N_f(x) = x - \frac{x}{f'(x)}.$$

ALGORITHM 1.2.1. $\tilde{x} = \text{NEWTON}(f, x_0, \delta)$

Require: *$f \in k[x]$, a polynomial;*
$x_0 \in k$, an initial approximation;
δ, the desired absolute error tolerance;
Ensure: $\|x_n - x_{n-1}\| < \delta$.

$n \leftarrow 0$
repeat
  $n \leftarrow n + 1$
  $x_n \leftarrow N_f(x_{n-1})$
until $\|x_n - x_{n-1}\| < \delta$
$\tilde{x} \leftarrow x_n$

Keep two caveats in mind:

- this algorithm is not guaranteed to terminate;
- for the result $\tilde{x}$ of the algorithm, the error $\|\tilde{x} - x^*\|$ is not necessarily bounded by δ for any (exact) root x^* of f.

Note: The termination criterion can be easily modified to focus on the desired residual tolerance and can come in both absolute and relative flavor (see remarks following Problem 1.1.1).

The point x^* is called a *regular* root of f if $f'(x^*) \neq 0$. The following proposition is straightforward.

PROPOSITION 1.2.2. *x^* is a regular root of a polynomial f iff $x^* = N_f(x^*)$.*

Provided the sequence $x_0, x_1, \ldots$ converges to a regular root, it converges *quadratically*: roughly speaking, $|x_{n+1} - x^*| \simeq |x_n - x^*|^2$. If the root is *multiple*, i.e., non-regular, this can not be claimed.

The following exercise shows that not all initial points x_0 generate a convergent sequence.

EXERCISE 1.2.3. *Find all points x such that $x = N_f^2(x)$ for $f = x^2 - ax$.*

Note: While classically Newton's method was designed for $k = \mathbb{R}$ and $k = \mathbb{C}$, it may be used looking for roots of polynomials in other fields; for instance, look up *Puiseux series*.

1.3. Subdivision methods. Another large class of numerical techniques is *subdivision methods*: given a search domain for a solution such methods proceed by subdividing this domain until

- either all pieces are shown to have no solutions
- or a piece guaranteed to contain a solution is found and this piece is small enough so that every point is an approximation to the solution within a prescribed error tolerance.

We illustrate this class of methods by the well-known *bisection method* to find a root of a real polynomial of a real segment.

ALGORITHM 1.3.1. $\tilde{x} = \text{BISECTION}(f, a, b, \delta)$

Require: *$f \in \mathbb{R}[x]$, a polynomial;*
$a, b \in \mathbb{R}$, $a < b$, $f(a)f(b) < 0$;
δ, the desired absolute error tolerance;
Ensure: *$\tilde{x}$ is an approximation of a root of f with absolute error not exceeding δ.*

---

while $b - a > 2\delta$ ***do***
  $c \leftarrow \frac{a+b}{2}$
  if $f(c)f(a) > 0$ ***then***
    $a \leftarrow c$
  else
    $b \leftarrow c$
  end if
end while
$\tilde{x} \leftarrow \frac{a+b}{2}$

Having the values $f(a)$ and $f(b)$ of different signs implies, by continuity, that the segment $[a, b]$ contains at least one root. This algorithm is guaranteed to terminate.

1.4. Companion matrix. For a polynomial,

$$f = x^d + a_{d-1}x^{d-1} + \ldots + a_1 x + a_0 \in k[x],$$

define the *normal form* with respect to f as the following map:

$$\mathrm{NF}_f : k[x] \to k[x]_{\leq d-1}, \quad \mathrm{NF}_f(g) = \text{remainder of the division } g \text{ by } f,$$

where the remainder $r \in k[x]_{\leq d-1}$ is a unique polynomial of degree less than d satisfying $g = qf + r$, for some $q \in k[x]$.

Now define the "multiplication by x" operator:

$$M_x : k[x]_{\leq d-1} \to k[x]_{\leq d-1}, \quad M_x(g) = \mathrm{NF}_f(xg).$$

The linear map M_x is represented by the square matrix

$$A_x = \begin{bmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{d-1} \end{bmatrix}$$

with respect to the (standard) *monomial basis*,

$$\begin{aligned} e_0 &= 1, \\ e_1 &= x, \\ e_2 &= x^2, \\ &\cdots \\ e_{d-1} &= x^{d-1}, \end{aligned}$$

of $k[x]_{\leq d-1}$.

The *companion matrix* of f is defined as A_x above.

EXERCISE 1.4.1. (1) *Show that* $A_x^d e_0 = \sum -a_i A_x^i e_0$.
(2) *Suppose the roots* $b_1, \cdots, b_d \in \mathbb{C}$ *of* f *are distinct. Prove that* A_x *is diagonalizable. (Hint:* Vandermonde *matrix provides the eigenvectors of* A_x^T*.)*

(3) *Find the Jordan canonical form of* A_x^T *for* $f = (x-b)^2$.
(4) *Let* $v(x) = (1, x, x^2, \cdots, x^{d-1})^T \in \mathbb{C}^d$. *Let* b *be a root of* f *with multiplicity* m. *Show that*
$$v_\alpha(b) = \frac{1}{\alpha!}\frac{\partial^\alpha v}{\partial x^\alpha}(b)$$
is a generalized eigenvector of A_x^T *for* $\alpha = 0, \ldots, m-1$.
(5) *Find the Jordan canonical form of* A_x^T *and conclude that* f *equals the characteristic and the minimal polynomials of* A_x.

The above exercise leads us to a conclusion that the roots of f and the eigenvalues of A_x are the same set. Therefore, the problem of finding roots of f can be restated as a problem of finding the *spectrum* of the companion matrix A_x.

EXERCISE 1.4.2. *Consider the linear operator* $M_g : k[x]_{\le d-1} \to k[x]_{\le d-1}$ *of multiplication by an arbitrary polynomial* g *constructed in a way similar to the case* $g = x$ *above. Show that its* spectrum *is the set of values of* g *taken at the roots of* f.

Note: There is a trove of numerical *iterative methods* for approximating eigenvalues of matrices, including a *homotopy continuation method* that will be discussed later (see Example **??**).

1.5. Euclidean algorithm, gcd, and resultant. We define the *gcd (greatest common divisor)* of a set of polynomials $S \subset k[x]$ to be the monic polynomial g of the largest degree such that $g|f$ for all $f \in S$.

The *Euclidean algorithm* can find the gcd for a set of two polynomials. Let $\mathrm{LC}(f)$ denote the leading coefficient of $f \in k[x]$ and let $\mathrm{MONIC}(f) = f/\mathrm{LC}(f)$.

ALGORITHM 1.5.1. $g = \gcd(f_1, f_2)$

Require: $f_1, f_2 \in k[x]$, *nonzero polynomials;*
Ensure: g *is the gcd of* $S = \{f_1, f_2\}$.

---

while $f_2 \neq 0$ ***do***
  $h \leftarrow f_2$
  $f_2 \leftarrow \mathrm{NF}_h(f_1)$
  $f_1 \leftarrow h$
end while
$g \leftarrow \mathrm{MONIC}(f_1)$

Computing a gcd for any finite set of polynomials amounts to applying the above algorithm repetitively.

Note that the command
$$f_2 \leftarrow \mathrm{NF}_h(f_1)$$
finds the polynomial f_2 of the smallest degree such that $f_1 = f_2 + qh$ for a some polynomial q.

EXERCISE 1.5.2. *Describe algorithms to*

(1) *find the* quotient q *and the* remainder f_1 *in the division-with-remainder procedure described above;*
(2) *find a pair of nonzero polynomials* $(c_1, c_2) \in k[x]^2$ *of minimal possible degrees*
  (a) *such that* $g = \gcd(f_1, f_2) = c_1 f_1 + c_2 f_2$;
  (b) *such that* $c_1 f_1 + c_2 f_2 = 0$.

EXERCISE 1.5.3. *Suppose* $\gcd(f_1, f_2) = 1$. *Show that if* $(c_1, c_2) \in k[x]^2$ *satisfy* $c_1 f_1 + c_2 f_2 = 0$, *then* (c_1, c_2) *is a multiple of* $(f_2, -f_1)$*: i.e, there is* $h \in k[x]$ *such that* $c_1 = hf_2$ *and* $c_2 = -hf_1$.

Note that in part (2b) of the Exercise 1.5.2 if $g = \gcd(f_1, f_2) \neq 1$ then $\deg c_1 < d_1 = \deg f_2$ and $\deg c_2 < d_1 = \deg f_1$. Indeed, in that case $f_1 = h_1 g$ and $f_2 = h_2 g$ for some polynomials h_1 and h_2; setting $(c_1, c_2) = (h_2, h_1)$ we have a pair with degrees satisfying the specified inequalities.

This means that the set of polynomials

$$S = \left\{ f_1,\ xf_1,\ \ldots,\ x^{d_2-1} f_1,\quad f_2, xf_2,\ \ldots,\ x^{d_1-1} f_2 \right\} \subset k[x]_{\leq d_1+d_2-1}$$

is linearly dependent. Let

$$f_1 = a_{d_1} x^{d_1} + a_{d_1-1} x^{d_1-1} + \ldots + a_1 x + a_0, \quad a_i \in k, \quad a_{d_1} \neq 0;$$
$$f_2 = b_{d_2} x^{d_2} + b_{d_2-1} x^{d_2-1} + \ldots + b_1 x + b_0, \quad b_i \in k, \quad b_{d_2} \neq 0.$$

The *resultant* $\mathrm{Res}(f_1, f_2)$ is the determinant of a square matrix of size $d_1 + d_2$, the rows of which are the coefficient vectors of polynomials in the set S above. There are two blocks in this matrix:

(1.5.1)

$$\begin{array}{c} \\ f_1 \\ xf_1 \\ \ldots \\ x^{d_2-1} f_1 \end{array} \begin{array}{c} \begin{array}{cccccccccc} x^{d_1+d_2-1} & x^{d_1+d_2-2} & \ldots & \ldots & \ldots & \ldots & \ldots & x^2 & x & 1 \end{array} \\ \begin{bmatrix} & & & a_{d_1} & a_{d_1-1} & & \cdots & & a_1 & a_0 \\ & & a_{d_1} & a_{d_1-1} & & \cdots & & a_1 & a_0 & \\ & \iddots & \iddots & & & & \iddots & \iddots & & \\ a_{d_1} & a_{d_1-1} & & \cdots & & a_1 & a_0 & & & \end{bmatrix} \end{array}$$

$$\begin{array}{c} \\ f_2 \\ xf_2 \\ \ldots \\ x^{d_1-1} f_2 \end{array} \begin{array}{c} \begin{array}{cccccccccc} x^{d_1+d_2-1} & x^{d_1+d_2-2} & \ldots & \ldots & \ldots & \ldots & \ldots & x^2 & x & 1 \end{array} \\ \begin{bmatrix} & & & b_{d_2} & b_{d_2-1} & & \cdots & & b_1 & b_0 \\ & & b_{d_2} & b_{d_2-1} & & \cdots & & b_1 & b_0 & \\ & \iddots & \iddots & & & & \iddots & \iddots & & \\ b_{d_2} & b_{d_2-1} & & \cdots & & b_1 & b_0 & & & \end{bmatrix} \end{array}$$

THEOREM 1.5.4. $\mathrm{Res}(f_1, f_2) = 0$ *iff* $\gcd(f_1, f_2) \neq 1$.

PROOF. If the two polynomials share a nontrivial common factor, then following the discussion after Exercise 1.5.2 we conclude that the resultant vanishes. If not, Exercise 1.5.3 implies it does not. □

COROLLARY 1.5.5. *Let* $f_1, f_2 \in \mathbb{C}[x]$. *Then* $\mathrm{Res}(f_1, f_2) = 0$ *iff there exist* $x \in \mathbb{C}$ *such that* $f_1(x) = f_2(x) = 0$.

2. Systems of multivariate polynomials

In this section we set the notation for polynomials in n variables $x = (x_1, x_2, \cdots, x_n)$.

A *monomial* is a product of variables written in the following form:

$$x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \cdots x_n^{\alpha_n}, \quad \alpha \in \mathbb{N}^n.$$

The (total) *degree* of a monomial is $\deg x^\alpha = |\alpha| = \sum_{i=1}^n \alpha_i$.

The set of monomials together with the operation of mutiplication forms a *monoid*: in our multiindex notation, the product of two monomials is

$$x^\alpha x^\beta = x^{\alpha+\beta}.$$

The above describes an isomorphism of the monoid of monomials and the monoid $\mathbb{N}^n$ equipped with the operation of addition.

A polynomial with coefficients in k is a linear combination of monomials

$$f = \sum a_\alpha x^\alpha, \quad a_\alpha \in k,$$

with all but finitely many coefficients a_α equal to zero. It can be considered as a function from k^n to k.

The infinite-dimensional k-space of polynomials in n variables together with the operation of multiplication is called the *polynomial ring* $k[x] = k[x_1, \ldots, x_n]$. As in the univariate case, the k-subspace $k[x]_{\le d}$ of polynomials of degree at most d is finite dimensional.

EXERCISE 2.0.6. *Find* $\dim_k k[x]_{\le d}$.

A *system of polynomials* is an m-tuple of polynomials $F = (f_1, \ldots, f_m)$. We call the solution set of F a *variety* and denote it by $\mathbb{V}(F)$.

$$\begin{aligned}\mathbb{V}(F) &= \{\, x \in k^n \mid F(x) = 0 \,\} \\ &= \{\, (x_1, \ldots, x_n) \in k^n \mid f_1(x_1, \ldots, x_n) = \cdots = f_n(x_1, \ldots, x_n) = 0 \,\}\end{aligned}$$

For the moment we distinguish two types of varieties: we call $V = \mathbb{V}(F) \subset k^n$

- 0-*dimensional* if V is a finite set;
- *positive-dimensional* if V is infinite.

We will focus on the case of dimension 0 until Chapter 3.

EXERCISE 2.0.7. *The variety $V = \mathbb{V}(F)$, $F = (f_1, \ldots, f_m)$, remains the same when*

1. *the polynomials of the system F are permuted;*
2. *F is replaced by*

$$\left(\sum_j c_{1j} f_j, \ldots, \sum_j c_{mj} f_j \right),$$

   where $C = (c_{ij}) \in k^m$ is an invertible matrix.
3. *another polynomial of the form*

$$\sum_{i=1}^m g_i f_i, \quad g_i \in k[x],$$

   is appended to F.

A system $F = (f_1, \dots, f_m)$ can be considered as a map $F : k^n \to k^m$. The matrix of its partial derivatives is called the *Jacobian* (matrix) of F and denoted

$$\frac{\partial F}{\partial x} = \begin{bmatrix} \frac{\partial f_1}{\partial x_1} & \cdots & \frac{\partial f_1}{\partial x_n} \\ \cdots & \cdots & \cdots \\ \frac{\partial f_m}{\partial x_1} & \cdots & \frac{\partial f_m}{\partial x_n} \end{bmatrix}.$$

We see that $\frac{\partial F}{\partial x}$ is an $m \times n$ matrix with polynomial entries.

The solution $x^* \in \mathbb{V}(F)$ is called *regular* (or *nonsingular*) if $\frac{\partial F}{\partial x}(x^*)$ is of full rank and *singular*, otherwise.

2.1. Eigenvalues of multiplication matrices. Consider the following polynomial system:

$$F = (f_1, f_2, f_3) = \begin{pmatrix} \boxed{x^2} - y^2 \\ \boxed{y^3} - 2xy - y^2 + 2x \\ \boxed{xy^2} - 3xy + 2x \end{pmatrix}.$$

We will refer to the monomials that are highlighted as *leading monomials* of the corresponding polynomials: in this example we order monomials by their degree and see x "heavier" than y to break the ties. A precise definition of a *monomial ordering* will be given in Chapter 3.

We denote by $\mathrm{LM}(f)$ the leading monomial of a polynomial f and by $\mathrm{LT}(f)$ its *leading term*, i.e., the leading monomial together with its coefficient: e.g., for

$$f = \boxed{2x^5} - 3y + 1,$$

we have $\mathrm{LT}(f) = 2\mathrm{LM}(f) = 2x^2$. Note that if f is a part of a polynomial system, we can always replace it with f divided by the *leading coefficient*. This makes the polynomial *monic*: $\mathrm{LT}(f) = \mathrm{LM}(f)$.

The set of *standard monomials* S consists of monomials not divisible by any of the leading monomials. For our example,

$$S = \{1, x, y, xy, y^2\}.$$

For the following approach to work we need F to have special properties. In particular, it is required that S is finite and the "tails" of polynomials in F contain monomials only in S.

Let us generalize the companion matrix method of §1.4. Consider the vector space

$$V = \operatorname{Span} S = \{\, f \in k[x, y] \,|\, \operatorname{supp}(f) \subseteq S \,\}$$

of polynomials with support contained in S. Define the operator of multiplication by x:

$$M_x : V \to V, \quad M_x(g) = \mathrm{NF}_F(xg).$$

While it is not hard to define the normal form function NF_F intuitively for some elements of xS,

$$\mathrm{NF}_F(x^2) = x^2 - (x^2 - y^2) = y^2,$$
$$\mathrm{NF}_F(xy^2) = xy^2 - (xy^2 - 3xy + 2x) = 3xy - 2x,$$

there is no natural reducer, for instance, for x^2y. We can rewrite this monomial "modulo" F as

$$x^2y - y(x^2 - y^2) = y^3.$$

but $y^3 \notin S$, so we need to continue the process:

$$\mathrm{NF}_F(x^2y) = y^3 - (y^3 - 2xy - y^2 + 2x) = 2xy + y^2 - 2x.$$

Noting that $\mathrm{NF}_F(xg) = xg$ for $g \in \{1, y\}$ we construct the matrix of M_x with respect to the basis S of V:

$$A_x = \begin{array}{c} \\ 1 \\ x \\ y \\ xy \\ y^2 \end{array} \begin{array}{c} \begin{array}{ccccc} M_x(1) & M_x(x) & M_x(y) & M_x(xy) & M_x(y^2) \end{array} \\ \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & -2 & -2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 2 & 3 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix} \end{array}$$

The eigenvalues of A_x give us the x-coordinates of the points $(x, y) \in \mathbb{V}(F)$. In our example the spectrum of A_x is $\{-1, 0, 1, 2\}$. Substituting one of these values in F produces a univariate problem:

$$F|_{x=1} = \left(-y^2 + 1, y^3 - y^2 - 2y + 2, y^2 - 3y + 2\right)$$

The gcd of these polynomials is $y - 1$, which means that there is only one solution, namely $(1, 1)$, to the system F with $x = 1$.

EXERCISE 2.1.1. *Construct the matrix A_y for the system F above.*

(1) *Find the eigenvalues of A_y.*
(2) *Find all points in $\mathbb{V}(F)$ that have the y-coordinate equal to 1.*
(3) *Let $g = xy + y + 1$ and let M_g be the operator of multiplication by g constructed similarly to M_x above. Find the eigenvalues of M_g.*

2.2. Elimination of variables. Consider the system of two equations in two variables

$$F = (f_1, f_2) = \begin{pmatrix} xy - 1 \\ 4x^2 + y^2 - 5 \end{pmatrix}.$$

Let us think of f_1 and f_2 as univariate polynomials of y (with coefficients that depend on x). Then, according to Theorem 1.5.4 and Corollary 1.5.5, they have a common solution iff their resultant vanishes:

$$\mathrm{Res}_x(f_1, f_2) = \begin{vmatrix} & y & -1 \\ y & -1 & \\ 4 & & y^2 - 5 \end{vmatrix} = -y^4 + 5y^2 - 4 = 0.$$

Solving the resulting equation we get $y \in \{-2, -1, 1, 2\}$. Substituting these back in F we compute the four intersection points of the hyperbola and the ellipse:

$$\left\{ \left(-2, -\frac{1}{2}\right), (-1, -1), (1, 1), \left(2, \frac{1}{2}\right) \right\}.$$

In principle, resultants can be used to solve systems in an arbitrary number of variables simply by eliminating variables one by one. However, the size of polynomial expressions in this method typically grows very rapidly as suggested by the following exercise.

EXERCISE 2.2.1. *Show that* $\mathrm{Res}(f_1, f_2)$ *as defined by (1.5.1) in §1.5 in a (multivariate) polynomial in $d_1 + d_2 + 2$ variables of degree $d_1 + d_2$, where $d_1 = \deg f_1$ and $d_2 = \deg f_2$.*

An alternative technique using *Gröbner bases* is proposed in Chapter 4

2.3. Rewriting polynomial systems. Now that we touched upon a topic of elimination of variables, one may wonder whether anything can be gained by a reverse procedure: Can we simplify a system by introducing more variables?

The answer depends on what "simpler" means. While elimination leads to a system of equations with fewer variables, it typically increases the degrees of the polynomials. On the other hand, increasing the number of variables one can always obtain a system of quadratic equations.

EXAMPLE 2.3.1. *Consider a system of two polynomials in two variables:*

$$F = \begin{pmatrix} y^3 - 6x^2 - 2xy + 5y^2 + 2x \\ x^3 - 3x^2 - 3xy + 3y^2 + 2x \end{pmatrix}.$$

If we make substitutions $u = x^2$ and $v = y^2$, we obtain the system of four quadratic equations

$$G = \begin{pmatrix} vy - 6u - 2xy + 5v + 2x \\ ux - 3u - 3xy + 3v + 2x \\ u - x^2 \\ v - y^2 \end{pmatrix}$$

in $k[x, y, u, v]$

This transformation can be described by two maps: $\phi : k^2 \to k^4$, $(x, y) \mapsto (x, y, x^2, y^2)$, sending a point in the old coordinates to a point in the new coordinates and the monomial map

$$\begin{aligned} \psi : k[x, y, u, v] &\to k[x, y], \\ u &\mapsto x^2 \\ v &\mapsto y^2 \\ x &\mapsto x \\ y &\mapsto y \end{aligned}$$

sending the first two polynomials of G to F and the other two to zero.

The restrictions of maps ϕ and the projection $\pi : k^4 \to k^2$, $(x, y, u, v) \mapsto (x, y)$, give a bijection of the varieties $\mathbb{V}(G)$ and $\mathbb{V}(F)$.

We call a *binomial* a polynomial with two terms and a *trinomial* a polynomial with three terms.

EXERCISE 2.3.2. *Show that*

(1) *every system of binomial equations can be transformed into a system of quadratic binomial equations;*
(2) *every polynomial system can be transformed into a system of trinomials.*