Basic Algebraic Geometry, Volume 1
Chapter 1, Section 1: Algebraic Curves in the Plane

Igor R. Shafarevich

1. Plane Curves

(1) An **algebraic plane curve** is a curve consisting of the points in the plane whose coordinates (x, y) satisfy $f(x, y) = 0$, $f \in k[X, Y]$ a nonconstant polynomial.

(2) The **affine plane** is denoted $\mathbb{A}^2$. The curve just defined is an **affine** plane curve.

(3) The **degree** of f is the degree of the curve.

(4) $k[X, Y]$ is a UFD. If $f = f_1^{k_1} \cdots f_r^{k_r}$ is a prime factorization of f. The algebraic curve X given by $f = 0$ is the union of X_i given by $f_i = 0$. A curve is **irreducible** if its defining polynomial is irreducible. The decomposition $X = X_1 \cup \cdots \cup X_r$ is a decomposition of X into irreducible components.

(5) We let k be algebraically closed. Then degree is well-defined.

(6)

Lemma. *Let k be an arbitrary field, $f \in k[x, y]$ an irreducible polynomial, and $g \in k[x, y]$ an arbitrary polynomial. If g is not divisible by f then the system of equations $f(x, y) = g(x, y) = 0$ has only a finite number of solutions.*

Proof. View $f, g \in k(y)[x]$. They are relatively prime. f remains irreducible and $f \nmid g$. $(f, g) = 1$, so there exist $\tilde{u}, \tilde{v} \in k(y)[x]$ so that $\tilde{u}f + \tilde{v}g = 1$. Multiplying by $a(y) \in k[y]$, the common denominator of $\tilde{u}, \tilde{v}$, we get $a\tilde{u}f + a\tilde{v}g = a$. Let $u = a\tilde{u}$, $v = a\tilde{v} \in k[x, y]$. We have $uf + vg = a$. If $f(x, y) = g(x, y) = 0$, then $a(y) = 0$, so there are only finitely many y-coordinates. Likewise for the x-coordinate. □

(7) An algebraically closed field is infinite and if f is nonconstant, $f(x, y) = 0$ has infinitely many points.

(8) From the lemma, the polynomial for the curve is defined up to a constant multiple. If there are no repeated factors, then the degree of the curve is well-defined.

(9) Bézout's Theorem

(10) We assume k is algebraically closed throughout.

(11) If P is a point outside a circle C, construct the two tangents to C through P. The line joining their points of contact is the **polar line** of P.

(12) These usually require passing to algebraically closed fields.

   (a) $k = \mathbb{Q}$
   (b) finite fields
   (c) $k = \mathbb{C}(z)$

2. Rational Curves

(1) The curve $y^2 = x^2 + x^3$ can be parametrized by $x = t^2 - 1$, $y = t(t^2 - 1)$.

(2) An irreducible algebraic curve X defined by $f(x, y) = 0$ is rational if there exist two rational functions $\varphi(t)$, $\psi(t)$, at least one nonconstant, such that $f(\varphi(t), \psi(t)) \equiv 0$.

(3) the correspondence $t_0 \leftrightarrow (\varphi(t_0), \psi(t_0))$ is a one-to-one correspondence, provided we exclude finitely values of t where denominators are zero and finitely many points of the curve.

(4) Conversely, t can be expressed as a rational function of x, y.

(5) You can use this to reduce $\int g(x, y)\, dx$ to an integral of a rational function of t is $g(x, y)$ if a rational curve.

(6) Curves of degrees 1 and 2 are rational. For curves of degree 2, look at the pencil of lines through one point on the curve to trace out the other point on each line of the pencil.

(7) If there is one solution in a field k and the rational functions have coefficients in k, then we can find (almost) all k-points on the curve.

(8) For any rational function $g(x, y)$, the integral $\int g(x, \sqrt{ax^2 + bx + c})\, dx$ can be expressed in elementary functions. This leads to the **Euler substitutions**.

3. Relation with Field Theory

(1) For an irreducible curve defined by $f(x, y) = 0$, look at rational functions p/q, with $f \nmid q$. Two rational functions are equal if their difference is zero on the curve, i.e. f divides the difference of the two rational functions.

(2) The rational functions on X form a field. This is the **function field** or **field of rational functions** of X. It is denoted $k(X)$.

(3) $k(X)$ has transcendence degree 1 over k.

(4) If X is rational, then $k(X) = k(t)$, the field of rational functions in t. The converse is true as well.

(5) **Lüroth's Theorem**: A subfield of $k(t)$ containing k is of the form $k(g(t))$, where $g(t)$ is some rational function. This theorem can be proved by simply properties of field extensions.

(6) **Proposition**: The parametrization $x = \varphi(t)$, $y = \psi(t)$ has the following properties

  (i) Except possibly for a finite number of points, any $(x_0, y_0) \in X$ has a representation $(x_0, y_0) = (\varphi(t_0), \psi(t_0))$

  (ii) Except possibly for a finite number of points, this representation is unique.

  This is not true for any parametrization, but for a specifically constructed one.

4. Rational Maps

(1) Let X, Y be a two irreducible algebraic plane curves, $u, v \in k(X)$. The map $\varphi(P) = (u(P), v(p))$ is defined at all points P of X where both u and v are defined. This is a **rational map** from X to Y if $\varphi(P) \in Y$ for every $P \in X$ at which φ is defined.

(2) If Y has the equation $g = 0$, then $g(u, v) \in k(X)$ must vanish at all but finitely many points of X. So, $g(u, v) = 0$ in $k(X)$.

(3) A rational map $\varphi : X \to Y$ is **birational**, or is a **birational equivalence** of X to Y, if φ has a rational inverse. That is, there exists a rational map $\psi : Y \to X$ such that $\varphi \circ \psi = \mathrm{id}_Y$ and $\psi \circ \varphi = \mathrm{id}_X$ wherever these functions are defined. In this case, we say that X and Y are **birational** or **birationally equivalent**.

(4) If $f(x, y)$ is an irreducible curve of degree n all of whose terms are monomials in x, y of degree $n - 1$ and n only. Projection from the origin defines a birational map of the curve to the line.

(5) If $f(x, y)$ is an irreducible curve of degree n all of whose terms are monomials in x, y of degree $n-2$, $n-1$ and n only. $f = u_{n-2} + u_{n-1} + u_n$, u_i homogeneous of degree i. Set $y = tx$ and cancel the factor x^{n-2}, thus reducing it to $a(t)x^2 + b(t)x + c(t) = 0$. Setting $s = 2ax + b$ to complete the square (if $\text{char}(k) \neq 2$), our curve is birational to $s^2 = p(t)$, where $p = b^2 - 4ac$. A curve of this type is called a **hyperelliptic curve**. If $p(t)$ has even degree $2m$, rewriting it as $p(t) = q(t)(t - \alpha)$ and dividing both sides by $(t - \alpha)^{2m}$, the curve is birational to the curve

$$\eta^2 = h(\xi), \quad \text{where } \xi = \frac{1}{t-\alpha}, \eta = \frac{s}{(t-\alpha)^m} \text{ and } h(\xi) = \frac{q(t)}{(t-\alpha)^{2m-1}},$$

where h is a polynomial of degree $\leq 2m-1$ in ξ. This is the **Weierstrass normal form** of the equation of the cubic.

(6) If $\text{char}(k) \neq 3$, apply translation $x \mapsto x - \frac{a}{3}$ gives

$$y^2 = x^3 + px + q.$$

(7) Affine algebraic curves X and Y are birational iff $k(X) \cong k(Y)$.

5. Singular and Nonsingular Points

(1) P is a **singular point** or **singularity** of a curve $f(x, y) = 0$ if $f'_x(P) = f'_y(P) = f(P) = 0$. If we translate P to the origin, $(0, 0)$ is singular if f does not have constant of linear terms.

(2) A point is **nonsingular** if it is not singular.

(3) A curve is **nonsingular** or **smooth** if all its points are nonsingular.

(4) An irreducible curve has finitely many singular points if $\text{char}(k) = 0$. If $\text{char}(k) = p$, then $f'_x(P) = f'_y(P) = f(P) = 0$ implies f is a polynomial in x^p, and hence is reducible mod p. Hence, an irreducible curve always has only finitely many singular points.

(5) If $P = (0, 0)$ and the leading terms in the equation have degree r, then r is called the **multiplicity** of P, and we say that P is an r**-tuple point**, or a **point of multiplicity** r.

(6) A nonsingular point has multiplicity 1. If a nonsingular point has multiplicity 2 and the terms of degree 2 in the equation are $ax^2+bxy+cy^2$, there are two posibilities: (a) $ax^2 + bxy + cy^2$ factors into two distinct linear factors, in which case the singularity is a **node**, or (b) $ax^2 + bxy + cy^2$ is a perfect square, in which case the singularity is a **cusp**.

(7) A curve of degree n cannot have a singularity of multiplicity $> n$. If a curve of degree n has a singular point of multiplicity n, then the curve is a union of n lines passing through the singular point.

(8) If a curve of degree n has a point of multiplicity $n-1$, then the curve is rational.

(9) If a curve of degree n has a point of multiplicity $n-2$, then the curve is hyperelliptic.

(10) A cubic curve in Weierstrass normal form $y^2 = x^3 + px + q$ is nonsingular iff $4p^3 - 27q^2 \neq 0$. In this case it is called an **elliptic curve**.

(11) If $k = \mathbb{R}$ and $f'_y(P) \neq 0$, then y is locally a function of x. Substituting, we can express any rational function on the curve as a function of x near P.

(12) If k is a general field, suppose $P = (0, 0)$ is a nonsingular point. Then $f = \alpha x + \beta y + g$, where g contains only terms of degree ≥ 2. We distinguish the terms in f that involve x only, writing $f = x\varphi(x) + y\beta + yh$, with $h(0, 0) = 0$. Thus on the curve $f = 0$ we have $y(\beta + h) = -x\varphi(x)$, or, in other words, $y = xv$, where $v = -\varphi(x)/(\beta + h)$ is a regular function at P (because $\beta + h(P) \neq 0$).

(13) Let $u \in k(X)$ regular at P with $u(P) = 0$. Then $u = p/q$ and $p(P) = 0$ and $q(P) \neq 0$. Substituting $y = xv$ gives $p(x, y) = p(x, xv) = xr$ (because p has no constant term), where r is a regular function on the curve and hence $u = xr/q = xu_1$. If $u_1(P) = 0$, we can repeat this argument. If u is not identically zero, then this process must stop after a finite number of steps.

(14)

Theorem. *At any nonsingular point P of an irreducible algebraic curve, there exists a regular function t that vanishes at P and such that every rational function u that is not identically 0 on the curve can be written in the form $u = t^k v$, with v regular at P and $v(P) \neq 0$. The function is regular at P iff $k \geq 0$.*

(15) A function t with this property is a **local parameter** on the curve at P. Two local parameters are multiples of each other by a rational function regular at P and $v(P) \neq 0$. If $f'_y(P) \neq$ then x can be a local parameter.

(16) The number k is the **multiplicity of the zero** of u at P. It is independent of the choice of the local parameter.

(17) If X and Y are algebraic curves with equations $f = 0$ and $g = 0$, and suppose that X is irreducible and not contained in Y, and that $P \in X \cap Y$ is a nonsingular point of X. Then g defines a function on X that is not identically zero; the multiplicity of the zero of g at P. It is the **intersection multiplicity** of X and Y at P.

(18) We analyze the intersection multiplicity of a line and X. Let $P = (\alpha, \beta) \in X$, and let the equation of X be written $f(x, y) = a(x - \alpha) + b(y - \beta) + g$, where g is expanded in powers of $x - \alpha$ and $y - \beta$ has only terms of degree ≥ 2.

(19) Write the equation of a line L through P in the form $x = \alpha + \lambda t$ and $y = \beta + \mu t$, where t is a local parameter on L at P. The restriction of f to L is of the form

$$f(\alpha + \lambda t, \beta + \mu t) = (a\lambda + b\mu)t + t^2\varphi(t).$$

(20) If P is singular, then $a = b = 0$, and every line through P has intersection multiplicity > 1 with X at P.

(21) If P is nonsingular, there is only one line with multiplicity > 1 with X at P. It has equation $a(x - \alpha) + b(y - \beta) = 0$, with $a = f'_x(P)$, $b = f'_y(P)$. So the equation of the **tangent line to X at the nonsingular point** P is

$$f'_x(P)(x - \alpha) + f'_y(P)(y - \beta) = 0.$$

(22) When does the line have intersection multiplicity ≥ 3? Write

$$f(x, y) = a(x - \alpha) + b(y - \beta) + c(x - \alpha)^2 + d(x - \alpha)(y - \beta) + e(y - \beta)^2 + h$$

where h is a polynomial which has only terms of degree ≥ 3. Restricting f to L, we get

$$f = (a\lambda + b\mu)t + (c\lambda^2 + d\lambda\mu + e\mu^2)t^2 + t^3\psi(t),$$

The intersection multiplicity of L and X at P will be ≥ 3 if

$$a\lambda + b\mu = c\lambda^2 + d\lambda\mu + e\mu^2 = 0$$

(23) The first of these means the line is tangent to X at P. The second of these means that $cu^2 + duv + ev^2$ is divisible by $au + bv$. Together, this shows that $q = au + bv + cu^2 + duv + ev^2$ is reducible. The reducibility of the conic $q = au + bv + cu^2 + duv + ev^2$ is a necessary and sufficient condition for there to exist a line L through P with intersection multiplicity ≥ 3 at P. Such a point is called an **inflexion point** or **flex** of X.

(24) We can write this condition in the form

$$\begin{vmatrix} f''_{xx} & f''_{xy} & f'_x \\ f''_{xy} & f''_{yy} & f'_y \\ f'_x & f'_y & 0 \end{vmatrix} (P) = 0.$$

6. The Projective Plane

(1) Definition of homogeneous coordinates (ξ, η, ζ) on $\mathbb{P}^2$. We write $P = (\xi : \eta : \zeta)$.

(2) There is an inclusion $\mathbb{A}^2 \subset \mathbb{P}^2$ which sends $(x, y) \in \mathbb{A}^2$ to $(x : y : 1)$. This gives us all points in $\mathbb{P}^2$ with $\zeta \neq 0$. A point $(\xi : \eta : \zeta) \in \mathbb{P}^2$ with $\zeta \neq 0$ corresponds to the point $(\xi/\zeta, \eta/\zeta) \in \mathbb{A}^2$. The points complementary to this are the **points at infinity**.

(3) Every point in $\mathbb{P}^2$ is contained in $\mathbb{A}^2_1 = \{(\xi : \eta : \zeta) \,|\, \xi \neq 0\}$, $\mathbb{A}^2_2 = \{(\xi : \eta : \zeta) \,|\, \eta \neq 0\}$, or $\mathbb{A}^2_3 = \{(\xi : \eta : \zeta) \,|\, \zeta \neq 0\}$. So, every point in $\mathbb{P}^2$ can be given affine coordinates in at least one of these pieces.

(4) A **projective algebraic curve**, an algebraic curve in $\mathbb{P}^2$, is defined by a homogeneous polynomial $F(\xi, \eta, \zeta) = 0$. The corresponding affine curve is $f(x, y) = 0$ where $f(x, y) = F(x, y, 1)$.

(5) A homogeneous polynomial is called a **form**.

(6) An affine algebraic curve of degree n with equation $f(x, y) = 0$ defines a homogeneous polynomial $F(\xi, \eta, \zeta) = \zeta^n f(\xi/\zeta, \eta/\zeta)$, and hence a projective curve with equation $F(\xi, \eta, \zeta) = 0$.

(7) Euler's formula on homogeneous functions gives us

$$F'_\xi \xi + F'_\eta \eta + F'_\zeta \zeta = nF.$$

(8) The equation of the tangent is

$$F'_\xi(P)\xi + F'_\eta(P)\eta + F'_\zeta(P)\zeta = 0.$$

(9) P is an inflexion point if

$$\begin{vmatrix} F''_{\xi\xi} & F''_{\xi\eta} & F''_{\xi\zeta} \\ F''_{\eta\xi} & F''_{\eta\eta} & F''_{\eta\zeta} \\ F''_{\zeta\xi} & F''_{\zeta\eta} & F''_{\zeta\zeta} \end{vmatrix} (P) = 0.$$

The determinant on the left-hand side is called the **Hessian form** of F, and denoted by $H(F)$.

(10) A rational function is a quotient of homogeneous polynomials of the same degree. A rational map is of the form

$$(\xi, \eta, \zeta) \mapsto (A(\xi, \eta, \zeta) : B(\xi, \eta, \zeta) : C(\xi, \eta, \zeta))$$

where A, B, and C are homogeneous polynomials of the same degree. The map is regular at P if one of A, B, or C is nonzero at P.

(11)

Theorem. *A rational map from a projective plane curve C to $\mathbb{P}^2$ is regular at every nonsingular point of C.*

(12)

Corollary. *A birational map between nonsingular projective plane curves is regular at every point, and is a one-to-one correspondence.*

(13)

Theorem (Bézout's Theorem)**.** *Let X and Y be projective curves, with X nonsingular and not contained in Y. Then the sum of the multiplicities of intersection of X and Y at all points of $X \cap Y$ equals the product of the degrees of X and Y.*

(14) Statement of Pascal's Theorem

Theorem (Pascal's Theorem)**.** *For a hexagon inscribed in a conic, the 3 points of intersection of pairs of opposite sides are collinear.*

Proof. (Due to Plücker) Let ℓ_1 and m_1, ℓ_2 and m_2, ℓ_3 and m_3 be linear forms that are the equations of the opposite sides of a hexagon. Consider the cubic with equation $f_\lambda = \ell_1\ell_2\ell_3 + \lambda m_1m_2m_3$ where λ is an arbitrary parameter. This has six points of intersection with the conic, the vertices of the hexagon. Moreover, we can choose the value of λ so that $f_\lambda(P) = 0$ for any given point $P \in X$, distinct from these 6 points of intersection. We get a cubic f_λ having seven points of intersection with a conic X, and by Bézout's Theorem this must decompose as the conic X plus a line L. This line L must contain the points of intersection, $\ell_1 \cap m_1$, $\ell_2 \cap m_2$, $\ell_3 \cap m_3$. □