

COPYRIGHT NOTICE:

**J.W.P. Hirschfeld, G. Korchmáros & F. Torres:**  
**Algebraic Curves over a Finite Field**

is published by Princeton University Press and copyrighted, © 2008, by Princeton University Press. All rights reserved. No part of this book may be reproduced in any form by any electronic or mechanical means (including photocopying, recording, or information storage and retrieval) without permission in writing from the publisher, except for reading and browsing via the World Wide Web. Users are not permitted to mount this file on any network servers.

Follow links [Class Use](#) and [other Permissions](#). For more information, send email to: [permissions@pupress.princeton.edu](mailto:permissions@pupress.princeton.edu)

# Chapter One

---

---

## Fundamental ideas

In this chapter, basic facts about curves are presented. The exposition also highlights some of the peculiarities that occur for positive characteristic, such as the existence of strange curves, that is, curves whose tangent lines at non-singular points have a point in common.

### 1.1 BASIC DEFINITIONS

Over the real numbers,  $\mathbf{R}$ , consider the parabola  $\mathcal{F}$  given by  $F = Y - X^2$ ; its points form, as in Figure 1.1, the set

$$\{(t, t^2) \mid t \in \mathbf{R}\}.$$

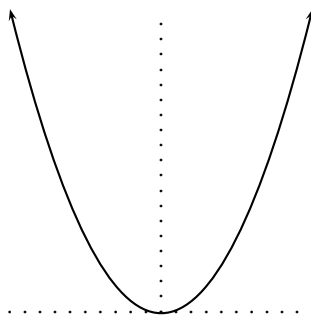


Figure 1.1 The parabola  $y = x^2$  in the real affine plane

However, there are two other types of points associated with  $\mathcal{F}$ , namely, (a) those at infinity and (b) those with coordinates in  $\mathbf{C}$ , the algebraic closure of  $\mathbf{R}$ . For example, regarding (b), the line with equation  $y + 1 = 0$  meets  $\mathcal{F}$  in the two points  $(i, -1), (-i, -1)$ , where  $i^2 = -1$ . Regarding (a), if  $F$  is homogenised to  $F^* = X_0X_2 - X_1^2$ , with  $X = X_1/X_0$ ,  $Y = X_2/X_0$ , then the line with equation  $X_0 = 0$  meets the corresponding projective curve  $\mathcal{F}^*$  at the point  $(0, 0, 1)$ .

All these ideas need to be considered for a general curve and a general field. First, some notation and fundamental definitions for the spaces that appear are explained.

**DEFINITION 1.1** (i) For a field  $K$ , let  $K^n = \{(x_1, x_2, \dots, x_n) \mid x_i \in K\}$ , the  $n$ -fold Cartesian product of  $K$ .

- (ii) Let  $V(n, K)$  be  $n$ -dimensional vector space over  $K$ , which may be regarded as  $(K^n, +, \cdot)$ , where, for  $x_i, y_i, \lambda \in K$ ,

$$(x_1, x_2, \dots, x_n) + (y_1, y_2, \dots, y_n) = (x_1 + y_1, x_2 + y_2, \dots, x_n + y_n),$$

$$\lambda(x_1, x_2, \dots, x_n) = (\lambda x_1, \lambda x_2, \dots, \lambda x_n).$$

- (iii) The *affine plane*  $\text{AG}(2, K) = \mathbf{A}^2(K)$  is a pair  $(\mathcal{P}, \mathcal{L})$ , where

$$\mathcal{P} = \{P = (x, y) \mid x, y \in K\},$$

$$\mathcal{L} = \{\ell = aX + bY + c \mid a, b, c \in K, (a, b) \neq (0, 0)\},$$

and a point  $P = (x, y)$  lies on a line  $\ell = aX + bY + c$  if  $ax + by + c = 0$ .

- (iv) More generally, *affine space of  $n$ -dimensions* is  $\text{AG}(n, K) = \mathbf{A}^n(K)$  with points  $x = (x_1, x_2, \dots, x_n)$  and  $r$ -dimensional subspaces  $x + S$ , for  $r$ -dimensional subspaces  $S$  of  $V(n, K)$ .

- (v) The *projective plane*  $\text{PG}(2, K) = \mathbf{P}^2(K)$  is a pair  $(\mathcal{P}, \mathcal{L})$ , where

$$\mathcal{P} = \{P = (x, y, z) = (\lambda x, \lambda y, \lambda z) \mid (x, y, z) \in K^3 \setminus \{(0, 0, 0)\},$$

$$\lambda \in K \setminus \{0\}\},$$

$$\mathcal{L} = \{\ell = aX + bY + cZ = \lambda aX + \lambda bY + \lambda cZ \mid a, b, c, \lambda \in K,$$

$$(a, b, c) \neq (0, 0, 0), \lambda \neq 0\},$$

and a point  $P = (x, y, z)$  lies on a line  $\ell = aX + bY + cZ$  if  $ax + by + cz = 0$ .

- (vi) More generally, *projective space of  $n$ -dimensions* is  $\text{PG}(n, K) = \mathbf{P}^n(K)$  with points,

$$\mathbf{x} = (x_0, x_1, x_2, \dots, x_n) = (\lambda x_0, \lambda x_1, \lambda x_2, \dots, \lambda x_n),$$

$$(x_0, x_1, x_2, \dots, x_n) \neq (0, 0, 0, \dots, 0), \lambda \neq 0, \text{ and } r\text{-dimensional subspaces } S,$$

for  $(r + 1)$ -dimensional subspaces  $S$  of  $V(n + 1, K)$ .

In each type of space, it is important to consider the structure-preserving transformations.

**DEFINITION 1.2** (i) A *linear transformation*  $T : V(n, K) \rightarrow V(n, K)$ , is given as follows:

$$T(x) = x' \quad \text{where } {}^t x' = A {}^t x \text{ for a suitable non-singular matrix } A,$$

with  $x = (x_1, x_2, \dots, x_n)$ ,  $x' = (x'_1, x'_2, \dots, x'_n)$ , and  ${}^t x$  the transpose of  $x$ . The linear transformations of  $V(n, K)$  constitute the *the general linear group*  $\text{GL}(n, K)$ .

A *semilinear transformation*  $T : V(n, K) \rightarrow V(n, K)$ , is given as follows:

$$T(x) = x', \quad \text{where } {}^t x' = A {}^t \sigma(x) \text{ for a suitable non-singular matrix } A,$$

with  $\sigma(x) = (\sigma(x_1), \sigma(x_2), \dots, \sigma(x_n))$  for some automorphism  $\sigma$  of  $K$ .

The semilinear transformations of  $V(n, K)$  constitute its *general semilinear group*  $\Gamma L(n, K)$ .

- (ii) An *affine transformation*  $S : \text{AG}(n, K) \rightarrow \text{AG}(n, K)$  is given as follows:

$$S(x) = x' = T(x) + b,$$

where  $T$  is a linear transformation and  $b = (b_1, b_2, \dots, b_n)$ . The affine transformations of  $\text{AG}(n, K)$  constitute its *affine group*  $\text{AGL}(n, K)$ .

An *affine collineation*  $S : \text{AG}(n, K) \rightarrow \text{AG}(n, K)$  is given as follows:

$$S(x) = x' = T(\sigma(x)) + b,$$

with  $T$  as above and  $\sigma(x)$  as in (i).

- (iii) A *projectivity*  $T : \text{PG}(n, K) \rightarrow \text{PG}(n, K)$  is given as follows:

$$T(\mathbf{x}) = \mathbf{x}', \quad \text{where } {}^t\mathbf{x}' = A^t\mathbf{x},$$

with

$$\mathbf{x} = (x_0, x_1, \dots, x_n), \quad \mathbf{x}' = (x'_0, x'_1, \dots, x'_n),$$

and  $A$  a suitable non-singular matrix. It is also called a *projective transformation* or *linear collineation*. The projectivities of  $\text{PG}(n, K)$  constitute its *projective general linear group*  $\text{PGL}(n+1, K)$ .

A *collineation*  $T : \text{PG}(n, K) \rightarrow \text{PG}(n, K)$  is given as follows:

$$T(\mathbf{x}) = \mathbf{x}', \quad \text{where } {}^t\mathbf{x}' = A^t\sigma(\mathbf{x}),$$

with  $A$  as above and  $\sigma(\mathbf{x}) = (\sigma(x_0), \dots, \sigma(x_n))$ .

The collineations of  $\text{PG}(n, K)$  constitute its *projective semilinear group*  $\text{PTL}(n+1, K)$ .

- (iv) When  $K$  contains the finite field  $\mathbf{F}_q$ , the mapping

$$\begin{aligned} \Phi : \mathbf{F}_q &\rightarrow \mathbf{F}_q, \\ x &\mapsto x^q, \end{aligned}$$

is the *Frobenius automorphism*. The  $n$ -th *Frobenius automorphism* of  $K$  is the map  $\Phi^n$  that takes  $x \in K$  to  $x^{q^n} \in K$ . Then  $\mathbf{F}_{q^n}$  consists of all elements in  $K$  which are fixed by  $\Phi^n$ .

The *Frobenius collineation* associated to the Frobenius automorphism is the collineation of  $\text{PG}(n, K)$  with  $\sigma = \Phi$ ; that is,

$$\mathbf{x} \mapsto \mathbf{x}', \quad {}^t\mathbf{x}' = A^t\Phi(\mathbf{x}),$$

with  $\Phi(\mathbf{x}) = (x_0^q, x_1^q, \dots, x_n^q)$ , for some non-singular matrix  $A$ .

**REMARK 1.3** (i) When  $K = \mathbf{F}_q$ , it is customary to replace  $K$  by  $q$  in the notation for all the spaces and groups; so  $V(n, q)$  means  $V(n, K)$ , and similarly for  $\text{AG}(r, q)$ ,  $\text{PG}(r, q)$ ,  $\text{GL}(r, q)$ ,  $\text{GL}(r, q)$ ,  $\text{AGL}(r, q)$ ,  $\text{PGL}(r, q)$ , and  $\text{PTL}(r, q)$ .

- (ii) When  $K$  is algebraically closed and has characteristic  $p > 0$ , then  $K$  contains the finite field  $\mathbf{F}_q$  for every power of  $q$  of  $p$ .

## 1.2 POLYNOMIALS

**DEFINITION 1.4** (i) A polynomial  $f$  in the ring  $K[X_1, X_2, \dots, X_n]$  of polynomials in the indeterminates  $X_1, X_2, \dots, X_n$  is *reducible* if there exist non-constant  $f_1, f_2$  in  $K[X_1, X_2, \dots, X_n]$  with  $f = f_1 f_2$ ; otherwise,  $f$  is *irreducible*.

(ii) The *degree* of a monomial  $X_1^{r_1} X_2^{r_2} \dots X_n^{r_n}$  is  $r_1 + r_2 + \dots + r_n$ .

(iii) A polynomial is *homogeneous* if all its terms have the same degree.

(iv) The *degree* of a polynomial  $f$  is the largest degree of all its terms; write  $\deg f$ .

## 1.3 AFFINE PLANE CURVES

In the first instance, a curve is associated both to a set of points and to a polynomial. Let  $K$  be an algebraically closed field, and let  $F \in K[X, Y]$ . Then an affine curve is viewed as a set of points.

**DEFINITION 1.5** (i) The *plane affine curve*

$$\mathcal{F} = \mathbf{v}_a(F) = \{P = (x, y) \in \text{AG}(2, K) \mid F(x, y) = 0\}.$$

(ii) The *degree* of  $\mathcal{F}$ , written  $\deg \mathcal{F}$ , is  $\deg F$ .

Any affine transformation sends an affine curve to another having the same degree. Therefore  $\deg \mathcal{F}$  of an affine curve  $\mathcal{F}$  is an affine invariant.

**DEFINITION 1.6** (i) A *component* of the affine curve  $\mathcal{F} = \mathbf{v}_a(F)$  is an affine curve  $\mathcal{G} = \mathbf{v}_a(G)$  such that  $G$  divides  $F$ .

(ii) The affine curve  $\mathcal{F} = \mathbf{v}_a(F)$  is *irreducible* when it has no proper component, that is, when  $F$  is irreducible.

Components are covariant, that is, the diagram below is commutative for any affine transformation  $T$  of  $\text{AG}(2, K)$ .

$$\begin{array}{ccc} \mathcal{F} = \mathbf{v}_a(F) & \xrightarrow{T} & \mathcal{F}' = \mathbf{v}_a(F') \\ \text{component of } \mathcal{F} \downarrow & & \text{component of } \mathcal{F}' \downarrow \\ \mathcal{G} = \mathbf{v}_a(G) & \xrightarrow{T} & \mathcal{G}' = \mathbf{v}_a(G') \end{array}$$

Any line containing at least  $n + 1$  points from an affine curve  $\mathcal{F}$  of degree  $n$  is a component of  $\mathcal{F}$ . To show this, it may be assumed by covariance that  $\ell = \mathbf{v}_a(Y)$ . Let  $\mathcal{F} = \mathbf{v}_a(F(X, Y))$ . Then  $|\ell \cap \mathbf{v}_a(F)| \geq n + 1$  implies that  $F(X, 0)$  has more than  $n$  roots. Therefore  $F(X, 0) = 0$ , and hence  $X$  divides  $F(X, Y)$ .

Let  $\mathcal{F} = \mathbf{v}_a(F)$  be an affine curve with  $\deg F = d$ , and let  $\ell = bX - aY + c$  be a line containing the point  $P_0 = (x_0, y_0)$  on  $\mathcal{F}$ . Then, for any point  $P = (x, y) \in \ell$ ,

$$\begin{aligned} bx - ay &= bx_0 - ay_0, \\ b(x - x_0) &= a(y - y_0) = abt, \\ x &= x_0 + at, \quad y = y_0 + bt \end{aligned}$$

for some  $t \in K$ . Then

$$\begin{aligned} F(x, y) &= F(x_0 + at, y_0 + bt) = G(t) = G_0 + G_1 t + G_2 t^2 + \cdots + G_d t^d \\ &= G_m t^m + \cdots + G_d t^d, \end{aligned} \quad (1.1)$$

with  $G_m \neq 0$ ,  $G_d \neq 0$ .

**LEMMA 1.7** *The two irreducible curves  $\mathcal{F}_1 = \mathbf{v}_a(F_1)$  and  $\mathcal{F}_2 = \mathbf{v}_a(F_2)$  are the same if and only if  $F_2 = \lambda F_1$  for some  $\lambda \in K \setminus \{0\}$ .*

*Proof.* This is a consequence of Theorem 2.10. □

**DEFINITION 1.8** If  $F \in K[X, Y]$  satisfies

$$F = F_1^{n_1} F_2^{n_2} \cdots F_s^{n_s}$$

with each  $F_i$  irreducible, then  $\mathcal{F} = \mathbf{v}_a(F)$  has *components*  $\mathcal{F}_i = \mathbf{v}_a(F_i)$  with *multiplicity*  $n_i$  for  $i = 1, \dots, s$ .

The multiplicity of a component is an affine invariant.

**DEFINITION 1.9** Let  $\ell$  be a line which is not a component of  $\mathcal{F}$ .

- (i) The integer  $m$  of (1.1) is the *intersection number of  $\ell$  and  $\mathcal{F}$  at  $P_0$* : write

$$m = I(P_0, \ell \cap \mathcal{F});$$

- (ii) if  $m = 1$  for some line  $\ell$  through  $P_0$ , then  $P_0$  is a *simple* or *non-singular* point of  $\mathcal{F}$ ;
- (iii) if  $m \geq 2$  for all lines  $\ell$  through  $P_0$ , then  $P_0$  is a *singular* or *multiple* point of  $\mathcal{F}$ ;
- (iv) if  $m_0 = \min\{m \mid \ell \text{ a line through } P_0\}$ , then  $m_0$  is the *multiplicity of  $P_0$  on  $\mathcal{F}$* , or  $P_0$  is an  *$m_0$ -fold point of  $\mathcal{F}$* , and write

$$m_0 = m_{P_0}(\mathcal{F}) = m_{P_0}(F);$$

- (v) if  $m > m_0$  for a line  $\ell$ , then  $\ell$  is a *tangent to  $\mathcal{F}$  at  $P_0$* .

The intersection number and the multiplicity of a point are affine invariants.

**DEFINITION 1.10** If  $m_P(\mathcal{F}) = 2$ , then  $P$  is a *double* point of  $\mathcal{F}$ . A double point  $P$  with two distinct tangents to  $\mathcal{F}$  at  $P$  is a *node*, and with only one tangent to  $\mathcal{F}$  at  $P$  is a *cuspidal* point. If  $m_P(\mathcal{F}) = 3$ , then  $P$  is a *triple* point of  $\mathcal{F}$ .

**REMARK 1.11** Let  $M$  be a subfield of  $K$  and suppose that  $\mathcal{F}$  is defined over  $M$ , that is,  $\mathcal{F} = \mathbf{v}(f(X, Y))$  with  $f(X, Y) \in M[X, Y]$ . If  $P$  is a double point with two distinct tangents, neither of them defined over  $M$ , then  $P$  is an *isolated double point over  $M$* .

**LEMMA 1.12** If  $P_0$  is a simple point of  $\mathcal{F}$ , then, in (1.1),

$$G_1 = \left. \frac{\partial F}{\partial X} \right|_{P_0} a + \left. \frac{\partial F}{\partial Y} \right|_{P_0} b.$$

**COROLLARY 1.13** The tangent to  $\mathcal{F}$  at a simple point  $P = (x, y)$  is

$$\ell_P = \left. \frac{\partial F}{\partial X} \right|_P (X - x) + \left. \frac{\partial F}{\partial Y} \right|_P (Y - y).$$

Note the meaning of this corollary: the line  $\ell_P$  has intersection multiplicity at least 2 with  $\mathcal{F}$  at  $P$ .

**DEFINITION 1.14** A non-singular point  $P$  of  $\mathcal{F}$  is a *point of inflexion* of  $\mathcal{F}$  if

$$I(P, \ell_P \cap \mathcal{F}) \geq 3.$$

Here,  $P$  is also called an *inflexion* or, in some sources, a *flex*; the tangent  $\ell_P$  at  $P$  is the *inflexional tangent*. Tangents and inflexional tangents are covariant.

**REMARK 1.15** The behaviour of  $P = (0, 0)$  for an affine curve  $\mathcal{F} = \mathbf{v}_a(F)$  follows simply from the form of  $F$ . Write

$$F(X, Y) = F_m + F_{m+1} + \cdots + F_d,$$

where  $F_i$  is homogeneous of degree  $i$  in  $X$  and  $Y$ , and  $F_m \neq 0$ . Then

- (i) if  $m > 0$ , the point  $P$  lies on  $\mathcal{F}$ ;
- (ii) if  $m = 1$ , the point  $P$  is simple and  $F_1$  is the tangent at  $P$ ;
- (iii) if  $m \geq 2$ , the term  $F_m = \prod \ell_i$ , where  $\ell_1, \dots, \ell_m$  are the tangents at  $P$ ;
- (iv) if  $\ell_1, \dots, \ell_m$  are distinct, then  $P$  is an *ordinary multiple point*.

**EXAMPLE 1.16** (i) If  $F = Y - X^3$ , then  $\mathcal{F} = \mathbf{v}_a(F)$  has no singular points but  $(0, 0)$  is an inflexion.

- (ii) If  $F = Y^2 - X^3$ , then  $\mathcal{F} = \mathbf{v}_a(F)$  has a singular point  $(0, 0)$  of multiplicity 2 with the repeated tangent  $Y$ ; so it is a cusp.

See Figure 1.2.

**DEFINITION 1.17** An affine curve  $\mathcal{F} = \mathbf{v}_a(f(X, Y))$  is *rational* if there exist rational functions  $a(T)/c(T)$  and  $b(T)/c(T)$  with  $a(T), b(T), c(T) \in K[T]$  such that  $f(a(T)/c(T), b(T)/c(T)) = 0$ .

Lines and conics, that is, curves of degree 1 and irreducible curves of degree 2, are rational curves.

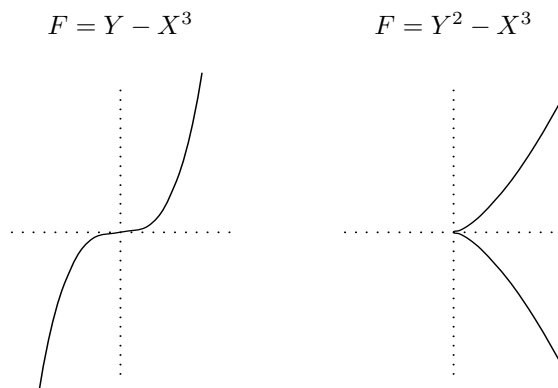


Figure 1.2 Plane cubics

### 1.4 PROJECTIVE PLANE CURVES

Let  $K$  be an algebraically closed field. For any polynomial  $F \in K[X, Y]$  of degree  $d$ , associate the homogeneous polynomial  $F^* \in K[X_0, X_1, X_2]$ , given by

$$X = X_1/X_0, \quad Y = X_2/X_0, \quad F^*(X_0, X_1, X_2) = X_0^d F(X_1/X_0, X_2/X_0).$$

Similarly, for any homogeneous polynomial  $F \in K[X_0, X_1, X_2]$ , associate the polynomial  $F_* \in K[X, Y]$ , given by

$$F_*(X, Y) = F(1, X, Y).$$

**DEFINITION 1.18** Given  $F \in K[X, Y]$ , the *projective plane curve* of affine equation  $F(X, Y) = 0$ , or homogeneous equation  $F^*(X_0, X_1, X_2) = 0$ , is

$$\mathcal{F} = \mathbf{v}(F) = \mathbf{v}(F^*) = \{(x_0, x_1, x_2) \in \text{PG}(2, K) \mid F^*(x_0, x_1, x_2) = 0\}.$$

This definition implies that the projective curve consists of the affine points plus the points at infinity; that is,

$$\mathbf{v}(F) = \{(1, x, y) \mid (x, y) \in \mathbf{v}_a(F)\} \cup \{(0, x, y) = (0, \lambda x, \lambda y) \mid F^*(0, x, y) = 0\}.$$

**REMARK 1.19** (i) For a linear form  $L = a_0X_0 + a_1X_1 + a_2X_2$ , the corresponding line is indicated both by  $L$  and  $\mathbf{v}(L)$ .

(ii) The notions of irreducibility, component, and degree extend in a natural way from affine curves to projective curves. It also follows, for any projective curve  $\mathcal{F} = \mathbf{v}(F(X, Y))$  not containing the line  $\mathbf{v}(X_0)$  as a component, that  $\mathcal{F}$  is irreducible if and only if the affine curve  $\mathcal{F}' = \mathbf{v}_a(F(X, Y))$  is irreducible.

**DEFINITION 1.20** (i) With  $F$  homogeneous, a point  $P = (x_0, x_1, x_2)$  of  $\mathcal{F}$  is *singular* if

$$\frac{\partial F}{\partial X_0} = \frac{\partial F}{\partial X_1} = \frac{\partial F}{\partial X_2} = 0$$

at  $P$ .

(ii) Otherwise,  $P$  is simple and the *tangent at  $P$*  is

$$\frac{\partial F}{\partial X_0} \Big|_P X_0 + \frac{\partial F}{\partial X_1} \Big|_P X_1 + \frac{\partial F}{\partial X_2} \Big|_P X_2.$$

Throughout, write

$$X_\infty = (0, 1, 0), \quad Y_\infty = (0, 0, 1), \quad O = (1, 0, 0), \quad E = (1, 1, 1).$$

Here,  $X_\infty$  is the *point at infinity* on the  $X$ -axis,  $Y_\infty$  is the *point at infinity* on the  $Y$ -axis, and  $O$  is the *origin*.

In Example 1.16 (i),  $Y_\infty$  is a cusp on  $\mathcal{F}$  and  $F^* = YZ^2 - X^3$ ; in (2),  $Y_\infty$  is an inflexion and  $F^* = Y^2Z - X^3$ . So the curves are projectively equivalent.

In general, to determine the behaviour of a point, translate it to the origin, and use Remark 1.15.

Sometimes, it is convenient to use the notation

$$\mathbf{U}_0 = (1, 0, 0), \quad \mathbf{U}_1 = (0, 1, 0), \quad \mathbf{U}_2 = (0, 0, 1), \quad \mathbf{U} = (1, 1, 1).$$

**REMARK 1.21** The properties of projective curves such as the degree, multiplicity of singular points, multiplicity of contact of a tangent are *covariant*, that is, invariant under projective transformations.

Let  $\mathcal{F} = \mathbf{v}(F(X_0, X_1, X_2))$  be a projective plane curve of degree  $d$ .

**DEFINITION 1.22** For any point  $P = (x_0, x_1, x_2)$ , if

$$G(X_0, X_1, X_2) = \frac{\partial F}{\partial X_0} x_0 + \frac{\partial F}{\partial X_1} x_1 + \frac{\partial F}{\partial X_2} x_2 \quad (1.2)$$

is not the zero polynomial, the plane curve  $\mathcal{G} = \mathbf{v}(G(X_0, X_1, X_2))$  of degree  $d - 1$  is the *polar curve of  $P$*  with respect to  $\mathcal{F}$ . Otherwise, the polar curve of  $P$  is *vanishing*.

**THEOREM 1.23** *The polar curve is covariant.*

*Proof.* If  $(X'_0, X'_1, X'_2)$  is a new homogeneous coordinate system, the link between the old frame and the new one is given by a linear substitution  $X_i = \sum_{j=0}^2 a_{ij} X'_j$ ,  $i = 0, 1, 2$ , such that the matrix  $(a_{ij})$  is non-singular. Under this change, the image of  $\mathcal{F}$  is the curve  $\mathcal{F}' = \mathbf{v}(F')$  with

$$F'(X'_0, X'_1, X'_2) = F(\sum_{j=0}^2 a_{0j} X'_j, \sum_{j=0}^2 a_{1j} X'_j, \sum_{j=0}^2 a_{2j} X'_j),$$

while the image of  $P$  is the point  $P' = (\sum_{j=0}^2 a_{0j} x_j, \sum_{j=0}^2 a_{1j} x_j, \sum_{j=0}^2 a_{2j} x_j)$ . Covariance means that the diagram below is commutative, which is now shown.

$$\begin{array}{ccc} \mathcal{F} = \mathbf{v}(F) & \xrightarrow{(a_{ij})^{-1}} & \mathcal{F}' = \mathbf{v}(F') \\ \text{polar of } P \downarrow & & \text{polar of } P' \downarrow \\ \mathcal{G} = \mathbf{v}(G) & \xrightarrow{(a_{ij})^{-1}} & \mathcal{G}' = \mathbf{v}(G') \end{array}$$

By the usual rules of the derivatives of composite functions,

$$\frac{\partial F'}{\partial X'_k} = \sum_{i=0}^2 a_{ik} \frac{\partial F}{\partial X_i}, \quad k = 0, 1, 2.$$

Therefore

$$\sum_{k=0}^2 \frac{\partial F'}{\partial X'_k} x'_k = \sum_{i=0}^2 \frac{\partial F}{\partial X_i} x_i. \quad \square$$

**THEOREM 1.24** *Suppose that the polar curve  $\mathcal{F}'$  of  $P$  with respect to  $\mathcal{F}$  is not vanishing.*

- (i) *If  $A$  is a non-singular point of  $\mathcal{F}$ , then  $A \in \mathcal{F}'$  if and only if the tangent to  $\mathcal{F}$  at  $A$  passes through  $P$ .*
- (ii) *Let  $A$  be an  $r$ -fold point of  $\mathcal{F}$ , with  $r > 1$ . Then*
  - (a)  *$A$  is at least an  $(r - 1)$ -fold point of  $\mathcal{F}'$ ;*
  - (b) *if there are infinitely many points  $P$  for which  $A$  is at least an  $r$ -fold point of  $\mathcal{F}'$ , every tangent to  $\mathcal{F}$  at  $A$  has multiplicity divisible by  $p$ .*

*Proof.* Let  $A = (a_0, a_1, a_2)$ . The tangent line to  $\mathcal{F}$  at  $A$  is

$$\frac{\partial F}{\partial X_0} X_0 + \frac{\partial F}{\partial X_1} X_1 + \frac{\partial F}{\partial X_2} X_2,$$

where the partial derivatives are evaluated at  $(a_0, a_1, a_2)$ . Thus (i) is a consequence of the definition of a polar curve.

To show (ii), note that the covariance of the polar curve allows  $A$  to be mapped to the origin. Write

$$F = \Phi_0 X_0^d + \Phi_1 X_0^{d-1} + \cdots + \Phi_i X_0^{d-i} + \cdots + \Phi_d,$$

where  $\Phi_i$  is a homogeneous polynomial in  $X_1$  and  $X_2$  of degree  $i$ . Since  $A$  is an  $r$ -fold point,  $\Phi_0 = \cdots = \Phi_{r-1} = 0$ , but  $\Phi_r \neq 0$ . Then, with  $G$  as in (1.2),

$$G = X_0^{d-r} G_1 + G_2,$$

where

$$G_1 = \frac{\partial \Phi_r}{\partial X_1} x_1 + \frac{\partial \Phi_r}{\partial X_2} x_2,$$

and where the terms in  $G_2$  have degree at least  $r$  in  $X_1$  and  $X_2$ . Since  $G_1$  has degree at least  $r - 1$ , so (a) follows.

If there are infinitely many points  $P$  for which  $A$  is an  $s$ -fold point of  $\mathcal{F}'$  with  $s \geq r$ , then both  $\partial \Phi_r / \partial X_1$  and  $\partial \Phi_r / \partial X_2$  vanish. This can occur only when  $\Phi_r$  is a  $p$ -th power of some polynomial  $\Psi_r$ . But then every tangent to  $\mathcal{F}$  at  $A$  has multiplicity divisible by  $p$ .  $\square$

**THEOREM 1.25** *If  $\mathcal{F}$  is irreducible of degree  $d$ , then there is at most one point  $P$  with vanishing polar curve  $\mathcal{F}'$ .*

*Proof.* Assume, on the contrary, that the polar curves of two distinct points are vanishing. By the covariance of polar curves, let these points be  $X_\infty$  and  $Y_\infty$ . Then  $\partial F/\partial X_1$  and  $\partial F/\partial X_2$  are both zero. Hence the general term in  $F(X_0, X_1, X_2)$  is

$$a_{ij} X_0^{d-(i+j)} X_1^i X_2^j$$

with both  $i$  and  $j$  divisible by  $p$ . Then  $p$  divides  $d$ , as otherwise  $X_0$  divides  $F$ , contradicting the irreducibility of  $\mathcal{F}$ . So  $p$  also divides  $d - (i + j)$ . Now define the coefficients  $b_{ij}$  by  $b_{ij}^p = a_{ij}$ , and the polynomial

$$L = \sum b_{ij} X_0^{(d-(i+j))/p} X_1^{i/p} X_2^{j/p}.$$

Then  $F = L^p$  and  $\mathcal{F}$  is reducible, a contradiction.  $\square$

Points with vanishing polar curves are characterised by a purely geometric property.

**THEOREM 1.26** *If  $\mathcal{F}$  is irreducible, then the polar curve of  $P$  is vanishing if and only if the tangents to  $\mathcal{F}$  at non-singular points pass through  $P$ .*

*Proof.* By the covariance, suppose that  $P$  is the point  $Y_\infty$ . With  $\mathcal{F}$  in its inhomogeneous form  $F(X, Y) = \sum a_{ij} X^i Y^j$ , the polar curve of  $P$  is vanishing if and only if  $a_{ij} = 0$  whenever  $j \not\equiv 0 \pmod{p}$ . This occurs if and only if there is no  $X_2$ -term in the form of the tangent to  $\mathcal{F}$  at any non-singular point.  $\square$

This condition can be weakened.

**THEOREM 1.27** *If  $\mathcal{F}$  is irreducible, then the polar curve of  $P$  is vanishing if and only if infinitely many tangents to  $\mathcal{F}$  pass through  $P$ .*

*Proof.* If the polar curve  $\mathcal{F}'$  of  $P$  is vanishing, the assertion follows from Theorem 1.26. If  $\mathcal{F}$  is not vanishing, then the weak form of Bézout's Theorem 3.13 applied to  $\mathcal{F}$  and  $\mathcal{F}'$  implies that there are finitely many common points. Since  $\mathcal{F}$  has a finite number of singular points,  $P$  lies only on finitely many tangents to  $\mathcal{F}$ .  $\square$

As becomes apparent later, vanishing polar curves can cause serious difficulties in certain situations, especially when the point lies on the curve. Here, some examples are given after formalising these concepts.

**DEFINITION 1.28** (i) A point is the *nucleus* of a projective irreducible curve  $\mathcal{F}$  if it is the common point of all tangents to  $\mathcal{F}$  at non-singular points.

(ii) A curve  $\mathcal{F}$  is *strange* if it admits a nucleus  $N$ .

Following this definition, Theorem 1.26 states that a point  $P$  is a nucleus of  $\mathcal{F}$  if and only if the polar curve of  $P$  with respect to  $\mathcal{F}$  is vanishing. Theorem 1.25 has the following corollary.

**THEOREM 1.29** *An irreducible curve has at most one nucleus.*

The simplest example of a strange curve is an irreducible conic in characteristic 2. Note that the nucleus does not lie on the conic.

**EXAMPLE 1.30** An example of a strange curve  $\mathcal{F}$  whose nucleus lies on the curve is the following. Let  $p = 2$  and  $q = 2^r$ . For an integer  $k < q$  with  $\gcd(k, q-1) = 1$ , let  $k = 2^s u$  with  $1 < s < r$ ,  $u > 1$  and  $u$  odd. Let  $\mathcal{F}$  be the irreducible curve  $\mathbf{v}(f(X, Y))$ , where

$$\begin{aligned} & (X^k + 1)(Y + 1) + (Y^k + 1)(X + 1) \\ & = f(X, Y)(X + 1)(Y + 1)(X + Y). \end{aligned} \quad (1.3)$$

To show that  $N = (1, 1, 1)$  is a nucleus of  $\mathcal{F}$ , write (1.3) as follows:

$$\begin{aligned} & (X^u)^{2^s} Y + (Y^u)^{2^s} X + (X^u + Y^u)^{2^s} + X + Y \\ & = f(X, Y)(X + 1)(Y + 1)(X + Y). \end{aligned} \quad (1.4)$$

Using this form, the tangent to  $\mathcal{F}$  at a non-singular point  $A = (a_0, a_1, a_2)$  of  $\mathcal{F}$  is

$$(a_1^k + a_2^k)X_0 + (a_0^k + a_2^k)X_1 + (a_0^k + a_1^k)X_2.$$

This shows that the tangent passes through the point  $N$ .

**EXAMPLE 1.31** An example in odd characteristic is the following.

Let  $p > 2$ , and  $\mathcal{F} = \mathbf{v}(Y^m - g(X))$  with  $m \not\equiv 0 \pmod{p}$ . Then  $\mathcal{F}$  is strange if and only if one of the following hold:

- (i)  $g(X) = f(X^p) + cX$ , where  $f \in K[X]$  and  $c \in K$  with  $c = 0$  for  $m \neq 1$ ;
- (ii)  $g(X) = (X + a)^r f(X^p)$  where  $a \in K$ ,  $f \in K[X]$  and  $1 \leq r < p$  with  $r \equiv m \pmod{p}$ .

Strange curves have exceptional behaviour with respect to duality; this is treated in Section 5.11. They also cause difficulties in the resolution of singularities; see the last part of the proof of Theorem 3.27.

### 1.5 THE HESSIAN CURVE

Let  $\mathcal{F} = \mathbf{v}(F(X_0, X_1, X_2))$  be a projective curve of degree  $d$ . Write

$$F_i = \frac{\partial F}{\partial X_i}, \quad F_{ij} = \frac{\partial^2 F}{\partial X_i \partial X_j}. \quad (1.5)$$

**DEFINITION 1.32** If the determinant

$$H(X_0, X_1, X_2) = \begin{vmatrix} F_{00} & F_{01} & F_{02} \\ F_{01} & F_{11} & F_{12} \\ F_{02} & F_{12} & F_{22} \end{vmatrix}$$

is not vanishing, then the projective curve  $\mathcal{H} = \mathbf{v}(H(X_0, X_1, X_2))$  is the *Hessian* curve of  $\mathcal{F}$ ; it has degree  $3(d - 2)$ . Otherwise, the Hessian curve is *vanishing*.

Strange curves have vanishing Hessian; see Exercise 3. Other relevant examples of curves with vanishing Hessian are the Hermitian curves.

**THEOREM 1.33** *The Hessian curve is covariant.*

*Proof.* Arguing as in the proof of Theorem 1.23, for  $0 \leq i, j \leq 2$ ,

$$\frac{\partial^2 F'}{\partial X'_i \partial X'_j} = \sum_{k=0}^2 \sum_{m=0}^2 a_{ki} a_{mj} \frac{\partial^2 F}{\partial X_k \partial X_m}.$$

This shows that

$$H'(X'_0, X'_1, X'_2) = H(X_0, X_1, X_2) \cdot \det(a_{ij})^2.$$

Since  $\det(a_{ij}) \neq 0$ , the assertion follows.  $\square$

**THEOREM 1.34** *If  $d \equiv 1 \pmod{p}$ , then the Hessian curve is vanishing.*

*Proof.* Let  $G \in K[X_0, X_1, X_2]$  be a homogeneous polynomial of degree  $m$ . By Euler's formula,

$$\frac{\partial G}{\partial X_0} X_0 + \frac{\partial G}{\partial X_1} X_1 + \frac{\partial G}{\partial X_2} X_2 = mG.$$

When  $G = F$ , this becomes

$$\frac{\partial F}{\partial X_0} X_0 + \frac{\partial F}{\partial X_1} X_1 + \frac{\partial F}{\partial X_2} X_2 = dF, \quad (1.6)$$

while for  $G = \partial F / \partial X_i$  with  $i = 0, 1, 2$ ,

$$\frac{\partial^2 F}{\partial X_i \partial X_0} X_0 + \frac{\partial^2 F}{\partial X_i \partial X_1} X_1 + \frac{\partial^2 F}{\partial X_i \partial X_2} X_2 = (d-1) \frac{\partial F}{\partial X_i}. \quad (1.7)$$

Then, with the notation of (1.5),

$$X_0 H(X_0, X_1, X_2) = \begin{vmatrix} (d-1)F_0 & F_{01} & F_{02} \\ (d-1)F_1 & F_{11} & F_{12} \\ (d-1)F_2 & F_{12} & F_{22} \end{vmatrix}.$$

Therefore  $H(X_0, X_1, X_2) = 0$  when  $d \equiv 1 \pmod{p}$ .  $\square$

The fundamental property of the Hessian curve is stated in the following theorem.

**THEOREM 1.35** *Assume that  $\mathcal{H}$  is not vanishing.*

- (i) *Let  $p \neq 2$ . Then a non-singular point of  $\mathcal{F}$  is an inflexion if and only if it is a common point of  $\mathcal{F}$  and  $\mathcal{H}$ .*
- (ii) *Every singular point of  $\mathcal{F}$  lies on  $\mathcal{H}$ .*

*Proof.* Let  $P$  be a non-singular point of  $\mathcal{F}$ . Again by the covariance, suppose that  $P$  is the origin and that the tangent line  $\ell$  to  $\mathcal{F}$  at  $P$  is the  $X$ -axis. Then

$$F(X_0, X_1, X_2) = X_0^{d-1} X_2 + X_0^{d-2} (a_{20} X_1^2 + a_{11} X_1 X_2 + a_{02} X_2^2) + \cdots,$$

where the other terms are powers of  $X_0$  with exponent at most  $d-3$ . A straightforward calculation shows that

$$H(X_0, X_1, X_2) = -2(d-1)^2 a_{20} X_0^{3(d-2)} + \cdots,$$

where the other terms are powers of  $X_0$  with exponent less than  $3(d-2)$ . Since  $p \neq 2$  and  $d \not\equiv 1 \pmod{p}$  by Theorem 1.34,  $\mathcal{H}$  passes through  $P$  if and only if  $a_{20} = 0$ ; that is,  $P$  an inflexion. If  $P$  is singular, then the above computation shows that no term containing only  $X_0$  appears in  $H(X_0, X_1, X_2)$ . Hence  $P \in \mathcal{H}$ .  $\square$

In affine form, when  $\mathcal{F} = \mathbf{v}(f(X, Y))$ , write

$$f_X = \frac{\partial f}{\partial X}, \quad f_Y = \frac{\partial f}{\partial Y}, \quad f_{XX} = \frac{\partial^2 f}{\partial X^2}, \quad f_{XY} = \frac{\partial^2 f}{\partial X \partial Y}, \quad f_{YY} = \frac{\partial^2 f}{\partial Y^2}.$$

**LEMMA 1.36** *Let  $d \not\equiv 1 \pmod{p}$ . If  $\mathcal{F} = \mathbf{v}(f(X, Y))$ , then  $\mathcal{H} = \mathbf{v}(h(X, Y))$ , where*

$$h(X, Y) = (f_X)^2 f_{YY} + (f_Y)^2 f_{XX} - 2f_X f_Y f_{XY} - d(d-1)^{-1} (f_{XX} f_{YY} - (f_{XY})^2) f.$$

*Proof.* As in the proof of Theorem 1.34, equations (1.6) and (1.7) are used. Substituting in  $H(X_0, X_1, X_2)$ , the expression reduces to the following:

$$X_0^2 H(X_0, X_1, X_2) = \begin{vmatrix} (d-1)dF & F_1 & F_2 \\ (d-1)^2 F_1 & F_{11} & F_{12} \\ (d-1)^2 F_2 & F_{12} & F_{22} \end{vmatrix}.$$

In inhomogeneous coordinates, this becomes the determinant

$$h(X, Y) = \begin{vmatrix} (d-1)df & f_X & f_Y \\ (d-1)^2 f_X & f_{XX} & f_{XY} \\ (d-1)^2 f_Y & f_{XY} & f_{YY} \end{vmatrix}.$$

Expansion of the determinant and division by  $-(d-1)^2$  give the result.  $\square$

When studying the inflexion points of  $\mathcal{F}$  or, more generally, the intersection of  $\mathcal{H}$  and  $\mathcal{F}$ , the last term of the polynomial in Theorem 1.36 can be omitted. So it is also possible to define the Hessian curve as  $\mathcal{H}' = \mathbf{v}(h'(X, Y))$ , with

$$h'(X, Y) = (f_X)^2 f_{YY} + (f_Y)^2 f_{XX} - 2f_X f_Y f_{XY}. \quad (1.8)$$

An advantage is that the Hessian curve in this form is no longer necessarily vanishing when  $\mathcal{F}$  has degree  $d \equiv 1 \pmod{p}$ ; see Exercise 2. Therefore curves with such degrees can be considered in the study of inflexion points. With this approach, just two remarks are needed.

- (1) Theorem 1.33 holds true if  $\mathcal{H}$  is given by (1.8).
- (2) Rewording the proof of Theorem 1.35 in terms of inhomogeneous coordinates,  $h(X, Y) = -2a_{20} + \dots$ , which shows that condition  $d \not\equiv 1 \pmod{p}$  depending on Theorem 1.34 disappears.

Therefore the following result is established.

**THEOREM 1.37** *Let  $p \neq 2$ . If either (1.8) is identically zero or the Hessian  $\mathcal{H}$  of  $\mathcal{F}$  as in (1.8) contains all points of  $\mathcal{F}$ , then every non-singular point of  $\mathcal{F}$  is an inflexion. The converse also holds.*

**REMARK 1.38** The form (1.8) of the Hessian curve is inadequate to deal with the even characteristic case. What is actually needed is to modify the definition of the second partial derivatives, as suggested by Hasse. If  $f = \sum a_{ij}X^iY^j$  then the Hasse second partial derivatives are as follows:

$$\frac{\partial^{(2)}f(X, Y)}{\partial X^{(2)}} = \sum a_{ij} \binom{i}{2} X^{i-2}Y^j, \quad \frac{\partial^{(2)}f(X, Y)}{\partial Y^{(2)}} = \sum a_{ij} \binom{j}{2} X^iY^{j-2}.$$

Put  $f = f(X, Y)$  for brevity. If  $p \neq 2$ , then

$$\frac{\partial^2 f}{\partial X^2} = 2 \frac{\partial^{(2)}f}{\partial X^{(2)}}, \quad \frac{\partial^2 f}{\partial Y^2} = 2 \frac{\partial^{(2)}f}{\partial Y^{(2)}}.$$

Now the Hessian curve  $\mathcal{H} = \mathbf{v}(\tilde{h})$  with inhomogeneous form  $\tilde{h}$  is defined to be the curve with

$$\tilde{h}(X, Y) = \left(\frac{\partial f}{\partial X}\right)^2 \frac{\partial^{(2)}f}{\partial Y^{(2)}} + \left(\frac{\partial f}{\partial Y}\right)^2 \frac{\partial^{(2)}f}{\partial X^{(2)}} - \frac{\partial f}{\partial X} \frac{\partial f}{\partial Y} \frac{\partial^2 f}{\partial X \partial Y}. \quad (1.9)$$

With this definition,  $\mathcal{H}$  is still covariant, and Theorem 1.35 holds true for  $p = 2$ .

**REMARK 1.39** The vanishing of the Hessian is related to exceptional behaviour of the dual curve in positive characteristic. This is treated in Section 5.11. The Hasse derivatives are useful in several other contexts; see Sections 5.10 and 7.6.

**EXAMPLE 1.40** Let  $n$  be a positive integer which is not divisible by  $p$ . The curve

$$\mathcal{F} = \mathbf{v}(X_0^n + X_1^n + X_2^n)$$

is the *Fermat curve of degree  $n$* .

When  $K = \overline{\mathbf{F}}_q$  with  $q$  a power of  $p$  and  $n = q + 1$ , then the Fermat curve is the *Hermitian curve* and denoted by  $\mathcal{H}_q$ ; that is,

$$\mathcal{H}_q = \mathbf{v}(X_0^{q+1} + X_1^{q+1} + X_2^{q+1}).$$

The properties of the Hermitian curve are further developed in Section 12.3.

The Fermat curve is the set of its inflexion points if and only if (a)  $n \equiv 1 \pmod{p}$  for  $p \neq 2$  or (b)  $n \equiv 1 \pmod{2^2}$  when  $p = 2$ . In particular, this holds for the Hermitian curve  $\mathcal{H}_q$  when  $p \neq 2$ .

**EXAMPLE 1.41** Let  $p \neq 0$ . Choose a power  $q$  of  $p$  such that  $q \equiv -1 \pmod{3}$ . Let  $\mathcal{F} = \mathbf{v}(F)$  be the plane curve with homogeneous form

$$F(X_0, X_1, X_2) = X_0^q X_2 + X_1^q X_0 + X_2^q X_1 - 3(X_0 X_1 X_2)^{(q+1)/3}.$$

It is first shown that  $\mathcal{F}$  is an irreducible curve with only ordinary singularities.

Each of the fundamental lines meets  $\mathcal{F}$  in only two points. If  $\mathcal{G}$  is a component of  $\mathcal{F}$  then  $\mathcal{G}$  meets each fundamental line in at least one point, and so at least two of the vertices of the fundamental triangle are on  $\mathcal{G}$ . If  $\mathcal{G}_1$  is another component of  $\mathcal{F}$ , then it also passes through two of the vertices of the fundamental triangle. So one of these points is common to  $\mathcal{G}$  and  $\mathcal{G}_1$ , and hence is a singular point of  $\mathcal{F}$ . However, this is not the case, since a first partial derivative of  $F$  is not zero at each of these points. More precisely,  $F_{X_0}(0, 1, 0) = F_{X_1}(0, 0, 1) = F_{X_2}(1, 0, 0) = 1 \neq 0$ .

Next, it is shown that  $\mathcal{F}$  has exactly  $(q^2 - q + 1)/3$  singular points, each of which is an ordinary double point. This requires some typical computations involving polynomials and their partial derivatives.

Since no vertex of the fundamental triangle is a singular point of  $\mathcal{F}$ , it suffices to consider affine points. So put  $X = X_1/X_0$ ,  $Y = X_2/X_0$ ; then  $\mathcal{F} = \mathbf{v}(f(X, Y))$  with

$$f(X, Y) = Y + X^q + XY^q - 3(XY)^{(q+1)/3}.$$

Let  $A = (a, b)$  be a singular point of  $\mathcal{F}$ . Then  $ab \neq 0$  and  $f_X(a, b) = f_Y(a, b) = 0$ . A direct calculation shows that this implies that

$$1 = a^{(q-2)/3}b^{(1-2q)/3}, \quad (1.10)$$

$$1 = a^{(q+1)/3}b^{(q-2)/3}. \quad (1.11)$$

Thus  $a^{(q-2)/3}b^{(1-2q)/3} = a^{(q+1)/3}b^{(q-2)/3}$ , whence  $a = b^{1-q}$ . Now (1.11) implies the following:

$$b^{(q^2-q+1)/3} = 1, \quad a = b^{-q^2}.$$

Conversely, if  $a, b \in K$  satisfy these conditions, then  $f_X(a, b) = f_Y(a, b) = 0$ , showing that every point  $A = (a, b)$  such that  $b^{(q^2-q+1)/3} = 1$ ,  $a = b^{1-q} = b^{-q^2}$  is a singular point of  $\mathcal{F}$ . Also,

$$f_{XX}(a, b) = \frac{2}{3} a^{(q-5)/3}b^{(q+1)/3},$$

$$f_{YY}(a, b) = \frac{2}{3} a^{(q+1)/3}b^{(q-5)/3},$$

$$f_{XY}(a, b) = \frac{1}{3} (ab)^{(q-2)/3},$$

$$f_{XX}(a, b)f_{YY}(a, b) - f_{XY}(a, b)^2 = \frac{1}{3} (ab)^{(2q-4)/3}.$$

It follows that, if  $p \neq 2$ , then  $A$  is a double point, more precisely, a node. The same holds true for  $p = 2$ , but the proof requires Hasse partial derivatives, as explained in Remark 1.38.

Finally, the Hessian  $\mathcal{H}$  of  $\mathcal{F}$  is  $\mathbf{v}((X_0X_1X_2)^{(2q-4)/3})$ , which shows that  $\mathcal{H}$  splits into three linear components, each counted  $(2q - 4)/3$  times.

**EXAMPLE 1.42** For a divisor  $k \geq 2$  of  $q - 1$ , and  $u, v \in K$  with  $uv \neq 1$ , the plane curve  $\mathcal{F} = \mathbf{v}(vX^kY^k - X^k - Y^k + u)$  is irreducible and has the following properties.

(i)  $\mathcal{F}$  has two singular points, namely  $X_\infty$  and  $Y_\infty$ , both ordinary  $k$ -fold points.

(ii) The Hessian  $\mathcal{H} = \mathbf{v}(H)$  of  $\mathcal{F}$  has

$$H = k^3 X^{k-2} Y^{k-2} (X^k u - 1)(Y^k u - 1)(2X^k Y^k u + (k - 1)(X^k + Y^k)).$$

In particular,  $\mathcal{F}$  is not the locus of its inflexions.

(iii) For each  $a \in K$  with  $a^k = u$ , the points  $A_1 = (1, 0, a)$  and  $A_2 = (1, a, 0)$  of  $\mathcal{F}$  are inflexions. For  $i = 1, 2$ , the tangent to  $\mathcal{F}$  at  $A_i$  is  $\ell_i = \mathbf{v}(X_i - aX_0)$ . Also,  $I(A_i, \mathcal{F} \cap \ell_i) = k$ .

## 1.6 PROJECTIVE VARIETIES IN HIGHER-DIMENSIONAL SPACES

**DEFINITION 1.43** (i) Given a homogeneous  $F \in K[X_0, X_1, \dots, X_n]$ , the *projective hypersurface*

$$\mathcal{F} = \mathbf{v}(F) = \{(x_0, x_1, \dots, x_n) \in \text{PG}(n, K) \mid F(x_0, x_1, \dots, x_n) = 0\}.$$

When  $\deg F = 1$ , the hypersurface is a *hyperplane*.

(ii) Given homogeneous  $F_1, \dots, F_r \in K[X_0, X_1, \dots, X_n]$ , the *projective variety*

$$\mathcal{F} = \mathbf{v}(F_1, \dots, F_r) = \{\mathbf{x} = (x_0, x_1, \dots, x_n) \in \text{PG}(n, K) \mid F_1(\mathbf{x}) = \dots = F_r(\mathbf{x}) = 0\}.$$

When  $n = 2$ , a projective hypersurface is just a projective plane curve. Varieties can also be curves in a higher-dimensional space; this is explained in Section 7.17.

## 1.7 EXERCISES

1. Let  $p > 2$  and let  $\mathcal{C} = \mathbf{v}(F)$ , where

$$F(X_0, X_1, X_2) = X_0^{q+1} + X_1^{q+1} + X_2^{q+1} + X_0^{q-1} X_1 X_2.$$

Show that the Hessian curve  $\mathcal{H}$  of  $\mathcal{C}$  in its inhomogeneous form (1.8) is non-vanishing.

2. Let  $K$  have characteristic 2. Show that the Hessian curve  $\mathcal{H}$  of the Hermitian curve  $\mathcal{H}_2$  in its inhomogeneous form (1.9) is non-vanishing.
3. If  $p > 3$ , show that the Hessian of a strange curve vanishes.
4. Prove that a plane curve  $\mathcal{F}$  of degree  $k \geq 2$  is irreducible if it has both the following properties.
- $\mathcal{F}$  contains a point  $A$  such that  $I(A, \mathcal{F} \cap \ell) = k$  for the tangent  $\ell$  of  $\mathcal{F}$  at  $A$  when  $A$  is a simple point, and for at least one tangent  $\ell$  to  $\mathcal{F}$  at  $A$  when  $A$  is a singular point. In the latter case,  $\ell$  is required to have multiplicity 1.
  - $\mathcal{F}$  contains no linear component through the point  $A$ .
5. Prove that an irreducible plane cubic curve is rational if and only if it is singular.
6. Prove that an irreducible plane curve of degree  $n$  with an  $(n - 1)$ -fold point is rational.
7. Prove that any plane curve of degree at least 3 whose tangent lines at collinear points are concurrent is either strange or projectively equivalent to the Hermitian curve.

8. With  $\mathcal{F}$  as in Example 1.30, show that the necessary and sufficient condition for  $N$  to lie on  $\mathcal{F}$  is that  $s > 1$ . Also, show that the singular points of  $\mathcal{F}$  are as follows:
- (a)  $N$  is an ordinary  $(2^s - 2)$ -fold point with tangents
 
$$(m + 1)X_0 + mX_1 + X_2$$
 for  $m^{2^s - 1} = 1$  but  $m \neq 1$ ;
  - (b) for each  $b$  with  $b^u = 1$  but  $b \neq 1$ , the point  $P = (1, b, 1)$  is a  $(2^s - 1)$ -fold point with a single tangent;
  - (c) for each  $c$  with  $c^u = 1$  but  $c \neq 1$ , the point  $P = (1, 1, c)$  is a  $(2^s - 1)$ -fold point with a single tangent;
  - (d) for all  $b, c$  with  $b^u = c^u = 1$  but  $b \neq 1, c \neq 1, b \neq c$ , the point  $P = (1, b, c)$  is a  $2^s$ -fold point with a single tangent;
  - (e) for  $b$  with  $b^u = 1$  but  $b \neq 1$ , the point  $P = (1, b, b)$  is a  $(2^s - 1)$ -fold point with a single tangent.

### 1.8 NOTES

There are many works on the elements of algebraic curves: Abhyankar [8], Baker [26], Bertini [49], Coolidge [85], Enriques [122], Fischer [128], Fulton [135], Lefschetz [301], Hartshorne [193], Hilton [212], Kirwan [269], Reid [368], Salmon [380], Segre [399], Seidenberg [400], Semple and Kneebone [402], Semple and Roth [403], Severi [408], Walker [497].

For the historical development of algebraic geometry, see Coolidge [86] and Dieudonné [104, 105].

Example 1.31 comes from [230]. For Exercise 7, see [236].

For strange curves, as in Section 1.4, see Hartshorne [192, Chapter IV].

In [37], strange curves invariant under a cyclic projective group fixing a triangle are investigated.

A survey paper on Fermat curves in positive characteristic is [429].

In the classical literature, polar curves and their generalisations, the  $m$ -ic polar curves, together with Hessian curves, are used to establish the Plücker formulas and their generalisations. These are equations linking numerical parameters of curves, such as the number of nodes, cusps, inflexion points, singularities of higher multiplicities, and other constants; see [85, Chapter 9]. Polar curves in positive characteristic are studied in [202]; see also [203].

Hessian curves are also important in investigating the number of points of curves defined over a finite field. For instance, let  $\mathcal{F} = \mathbf{v}(F)$  be a projective irreducible curve of degree  $d$ , where  $F \in \mathbf{F}_q[X_0, X_1, X_2]$ . If its Hessian curve is non-vanishing, then the number of points of  $\mathcal{F}$  lying in  $\text{PG}(2, q)$  is bounded above by  $\frac{1}{2}d(q + d - 1)$ ; see Theorem 8.41. For  $q$  square and  $d = \sqrt{q} + 1$ , this upper bound is  $\frac{1}{2}\sqrt{q}(\sqrt{q} + 1)^2$ .

On the other hand, the Hermitian curve  $\mathcal{H}_{\sqrt{q}}$  has vanishing Hessian and has  $q\sqrt{q} + 1$  points lying in  $\text{PG}(2, q)$ ; see Example 8.67. Also, the polar curve of any

point with respect to  $\mathcal{H}_{\sqrt{q}}$  is reducible, being a line counted  $\sqrt{q}$  times. See Chapter 12 for more examples of plane curves in positive characteristic with properties that a complex algebraic curve cannot have.