is regular everywhere except at the point [0, 1, 0], where it is not regular (cf. 3.3).

Example 3.7. Let V be the variety

$$V: Y^2Z = X^3 + X^2Z,$$

and consider the rational maps

$$\psi: \mathbb{P}^1 \to V \qquad \phi: V \to \mathbb{P}^1$$
$$\psi = [(S^2 - T^2)T, (S^2 - T^2)S, T^3] \qquad \phi = [Y, X].$$

Here ψ is a morphism, while ϕ is not regular at [0, 0, 1]. Not coincidently (see II.2.1), [0, 0, 1] is a singular point of V. Notice that the compositions $\phi \circ \psi$ and $\psi \circ \phi$ are the identity map whenever they are defined, but nonetheless ϕ and ψ are not isomorphisms.

Example 3.8. Consider the varieties

$$V_1: X^2 + Y^2 = Z^2 \qquad V_2: X^2 + Y^2 = 3Z^2.$$

They are not isomorphic over $\mathbb{Q}$, since $V_2(\mathbb{Q}) = \varnothing$ (2.5), while $V_1(\mathbb{Q})$ contains lots of points. (More precisely, $V_1(\mathbb{Q}) \simeq \mathbb{P}^1(\mathbb{Q})$ from (3.5).) However, V_1 and V_2 are isomorphic over $\mathbb{Q}(\sqrt{3})$, an isomorphism being given by

$$\phi: V_2 \to V_1$$
$$\phi = [X, Y, \sqrt{3}Z].$$

EXERCISES

1.1. Let $A, B \in \bar{K}$. Characterize the values of A and B for which each of the following varieties is singular. In particular, as (A, B) ranges over $\mathbb{A}^2$, the "singular values" lie on a one-dimensional subset of $\mathbb{A}^2$, so "most" values of (A, B) give a non-singular variety.
(a) $V: Y^2Z + AXYZ + BYZ^2 = X^3$.
(b) $V: Y^2Z = X^3 + AXZ^2 + BZ^3$ (char $K \neq 2$).

1.2. Find the singular point(s) on each of the following varieties, and sketch $V(\mathbb{R})$.
(a) $V: Y^2 = X^3$ in $\mathbb{A}^2$.
(b) $V: 4X^2Y^2 = (X^2 + Y^2)^3$ in $\mathbb{A}^2$.
(c) $V: Y^2 = X^4 + Y^4$ in $\mathbb{A}^2$.
(d) $V: X^2 + Y^2 = (Z - 1)^2$ in $\mathbb{A}^3$.

1.3. Let $V \subset \mathbb{A}^n$ be a variety given by a single equation (cf. 1.4). Prove that a point $P \in V$ is non-singular if and only if

$$\dim_{\bar{K}} M_P/M_P^2 = \dim V.$$

[*Hint*: Let $f = 0$ be the equation of V, and define the *tangent plane to V at P* by

$$T = \{(y_1, \ldots, y_n) \in \mathbb{A}^n : \textstyle\sum (\partial f/\partial X_i(P))y_i = 0\}.$$

Show that the map

$$M_P/M_P^2 \times T \to \bar{K}, \qquad (g, y) \to \textstyle\sum (\partial g/\partial X_i(P))y_i$$

is a well-defined perfect pairing of $\bar{K}$-vector spaces. Now use (1.5).]

1.4. Let $V/\mathbb{Q}$ be the variety

$$V: 5X^2 + 6XY + 2Y^2 = 2YZ + Z^2.$$

Prove that $V(\mathbb{Q}) = \varnothing$.

1.5. Let $V/\mathbb{Q}$ be the projective variety

$$V: Y^2 = X^3 + 17,$$

and let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be distinct points of V. Let L be the line through P_1 and P_2.
(a) Show that $V \cap L = \{P_1, P_2, P_3\}$, and express $P_3 = (x_3, y_3)$ in terms of P_1 and P_2. (If L is tangent to V, then P_3 may equal P_1 or P_2.)
(b) Calculate P_3 for $P_1 = (-1, 4)$ and $P_2 = (2, 5)$.
(c) Show that if $P_1, P_2 \in V(\mathbb{Q})$, then $P_3 \in V(\mathbb{Q})$.

1.6. Let V be the variety

$$V: Y^2Z = X^3 + Z^3.$$

Show that the map

$$\phi: V \to \mathbb{P}^2, \qquad \phi = [X^2, XY, Z^2]$$

is a morphism. (Notice ϕ does not give a morphism $\mathbb{P}^2 \to \mathbb{P}^2$.)

1.7. Let V be the variety

$$V: Y^2Z = X^3,$$

and let ϕ be the map

$$\phi: \mathbb{P}^1 \to V, \qquad \phi = [S^2T, S^3, T^3].$$

(a) Show that ϕ is a morphism.
(b) Find a rational map $\psi: V \to \mathbb{P}^1$ so that $\phi \circ \psi$ and $\psi \circ \phi$ are the identity map wherever they are defined.
(c) Is ϕ an isomorphism?

1.8. Let $K = \mathbb{F}_q$, and let $V \subset \mathbb{P}^n$ be a variety which is defined over K.
(a) Show that the q^{th}-power map

$$\phi = [X_0^q, \ldots, X_n^q]$$

is a morphism $\phi: V \to V$. It is called the *Frobenius morphism*.
(b) Show that ϕ is one-to-one and onto.
(c) Show that ϕ is not an isomorphism.
(d) Show that

$$\{P \in V : \phi(P) = P\} = V(K).$$

1.9. If $m > n$, prove that there are no non-constant morphisms $\mathbb{P}^m \to \mathbb{P}^n$. [*Hint*: Use the dimension theorem [Har, I.7.2].]

1.10. For each prime $p \geq 3$, let V_p be the variety in $\mathbb{P}^2$ given by the equation

$$V_p: X^2 + Y^2 = pZ^2.$$

(a) Prove that V_p is isomorphic to $\mathbb{P}^1$ over $\mathbb{Q}$ if and only if $p \equiv 1 \pmod 4$.
(b) Prove that for $p \equiv 3 \pmod 4$, no two of the V_p's are isomorphic over $\mathbb{Q}$.

1.11. (a) Let $f \in K[X_0, \ldots, X_n]$ be a homogeneous polynomial, and let

$$V = \{P \in \mathbb{P}^n : f(P) = 0\}$$

be the hypersurface defined by f. Prove that if a point $P \in V$ is singular, then

$$\partial f/\partial X_0(P) = \cdots = \partial f/\partial X_n(P) = 0.$$

(Thus in projective space, one can check for smoothness using homogeneous coordinates.)

(b) Let $W \subset \mathbb{P}^n$ be a smooth algebraic set of dimension $n-1$. Prove that W is a variety. [*Hint*: First use Krull's Hauptidealsatz ([A–M] p. 122) to show that W is the zero set of a single homogeneous polynomial.]

1.12. (a) Let V/K be an affine variety. Prove that

$$K[V] = \{f \in \bar{K}[V] : f^\sigma = f \text{ for all } \sigma \in G_{\bar{K}/K}\}.$$

[*Hint*: One inclusion is clear. For the other, choose some $F \in \bar{K}[X]$ with $F \equiv f \pmod{I(V)}$. Show that the map $G_{\bar{K}/K} \to I(V)$ defined by $\sigma \to F^\sigma - F$ is a 1-cocycle (cf. B §2). Now use (B.2.5a) to conclude that there exists a $G \in I(V)$ such that $F + G \in K[X]$.]

(b) Prove that

$$\mathbb{P}^n(K) = \{P \in \mathbb{P}^n(\bar{K}) : P^\sigma = P \text{ for all } \sigma \in G_{\bar{K}/K}\}.$$

[*Hint*: Write $P = [x_0, \ldots, x_n]$. If $P = P^\sigma$, then there is a $\lambda_\sigma \in \bar{K}^*$ such that $x_i^\sigma = \lambda_\sigma x_i$ for $0 \leq i \leq n$. Show that the map $\sigma \to \lambda_\sigma$ gives a 1-cocycle from $G_{\bar{K}/K}$ to $\bar{K}^*$. Now use Hilbert's theorem 90 (B.2.5b) to find an $\alpha \in \bar{K}^*$ so that $[\alpha x_0, \ldots, \alpha x_n] \in \mathbb{P}^n(K)$.]

(c) Let $\phi: V_1 \to V_2$ be a rational map of projective varieties. Prove that ϕ is defined over K if and only if $\phi^\sigma = \phi$ for every $\sigma \in G_{\bar{K}/K}$. [*Hint*: Use (a) and (b).]

CHAPTER II
Algebraic Curves

In this chapter we present the basic facts about algebraic curves (i.e. projective varieties of dimension 1) which will be needed for our study of elliptic curves. (Actually, since elliptic curves are curves of genus 1, one of our tasks will be to define the genus of a curve.) As in Chapter I, we give references for those proofs which are not included. There are many books where the reader can find more material on the subject of algebraic curves, for example [Har, Ch. IV], [Sha 2], [G–H, Ch. 2], [Wa].

We recall the following notation from Chapter I, which will be used in this chapter. (C is a curve and $P \in C$.)

C/K	C is defined over K
$K(C)$, $\bar{K}(C)$	the function field of C
$\bar{K}[C]_P$	the local ring of C at P
M_P	the maximal ideal of $\bar{K}[C]_P$

§1. Curves

By a *curve* we will always mean a projective variety of dimension 1. We will generally deal with curves which are smooth. Examples of smooth curves are provided by $\mathbb{P}^1$, (I.2.3), and (I.2.8). We start by describing the local rings of a smooth curve.

Proposition 1.1. *Let C be a curve and $P \in C$ a smooth point. Then $\bar{K}[C]_P$ is a discrete valuation ring.*