CHAPTER 2

ALGEBRAIC CURVES

Throughout the chapter, k is a perfect field (think of $k = \mathbb{F}_q$).

2.1. Smoothness of curves

2.1.1. Reminder and setup. — Let C be an affine variety of dimension 1 in $\mathbb{A}^n$ defined over k, with corresponding prime ideal $I \subset \overline{k}[x_1, \dots, x_n]$ and $I(C/k) \subset k[x_1, \dots, x_n]$. Recall that the coordinate ring of C is the quotient $\overline{k}[C] := \overline{k}[x_1, \dots, x_n]/I(C/k)$ (it is an integral domain). Hilbert's Nullstellensatz says that there is a one-to-one correspondence between maximal ideals in $\overline{k}[C]$ and points on C: to a point $P \in C$, this correspondence associates the ideal $\mathfrak{M}_P := \{f \in \overline{k}[C] : f(P) = 0\}$.

The function field of C is then the quotient field of $\overline{k}(C)$. Elements of $\overline{k}(C)$ are called rational functions on C. By assumption on the dimension of C, the extension $\overline{k}(C)/\overline{k}$ has transcendence degree 1.

Example 2.1. — One has $\overline{k}[\mathbb{A}^1] = \overline{k}[x]$ and $\overline{k}(\mathbb{A}^1) = \overline{k}(x)$, the field of rational functions with coefficients in $\overline{k}$.

Let P be a point on an affine curve C, the set of rational functions on C that are regular at P (or defined at P) is a subring of $\overline{k}(C)$, called the local ring of C at P, and denoted by $\mathcal{O}_P$: it is the localization at $\mathfrak{M}_P$ of $\overline{k}[C]$ or, more explicitely,

$$\mathcal{O}_P = \left\{ f \in \overline{k}(C) \ : \ f = \frac{g}{h} \text{ with } g, h \in \overline{k}[C] \text{ and } h(P) \neq 0 \right\}.$$

The ring $\mathcal{O}_P$ is indeed a local ring: its unique maximal ideal is $\mathfrak{M}_P$ (or rather the localization of $\mathfrak{M}_P$ at $\mathfrak{M}_P$, *i.e.* the image of $\mathfrak{M}_P$ under the localization map $\overline{k}[C] \to \mathcal{O}_P$). The quotient field $\mathcal{O}_P/\mathfrak{M}_P$ is then a finite extension of $\overline{k}$, and thus it has to be $\overline{k}$.

If C is a projective curve and $P \in C$ is a point, one defines the local ring of C at P to be the local ring of an affine part C' of C containing P.

2.1.2. Smoothness. — We now formalize the notion of smoothness of a curve. We start by defining this in terms of the Jacobian criterion for the existence of a tangent plane:

Definition 2.2. — Let $C \subset \mathbb{A}^n$ be an affine curve and $f_1, \dots, f_m \in \overline{k}[x_1, \dots, x_n]$ be a set of generators for $I(C)$. For a point $P \in C$, we say that C is smooth (or nonsingular) at P if the $m \times n$ matrix (the Jacobian matrix)

$$\left[\frac{\partial f_i}{\partial x_j}(P) \right]_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$$

has rank $n-1$. If C is nonsingular at every point, then we say that C is nonsingular (or smooth).

Note that the rank of the matrix above is independent of the choice of generators $f_1, \ldots, f_m$ for $I(C)$ (but the matrix itself does depend on that choice). See below for a more intrinsic characterization.

***Example 2.3* (Plane curves).** — Let $C \subset \mathbb{A}^2$ be given by a single nonconstant polynomial $f \in \overline{k}[x, y]$:

$$C : f(x, y) = 0.$$

By definition, a point $P \in C$ is smooth if and only if

$$\left(\frac{\partial f}{\partial x}(P), \frac{\partial f}{\partial y}(P)\right) \neq (0, 0).$$

In other words, C is smooth at P if the tangent vector does not vanish. If $P = (x, y)$ is smooth, the line given by the equation (in the (X, Y)-plane $\mathbb{A}^2$):

$$T_P C : \frac{\partial f}{\partial x}(P) \cdot (X - x) + \frac{\partial f}{\partial y}(P) \cdot (Y - y) = 0$$

is then called the tangent line of C at P. (If P was singular, this linear subspace $T_P C$ is actually the whole of $\mathbb{A}^2$). On the other hand, the singular points $Q = (x, y)$ of C are solutions of the system of equations:

$$\begin{cases} f(Q) & = 0 \\ \frac{\partial f}{\partial x}(Q) & = 0 \\ \frac{\partial f}{\partial y}(Q) & = 0. \end{cases}$$

This system gives 3 polynomial relations between the 2 coordinates of Q. Thus, it doesn't seem absurd that there are not many singular points on a plane curve (see a Proposition later on).

Example 2.4. — Consider the three curves

$$V_1 : y^2 = x^3 + x \qquad V_2 : y^2 = x^3 + x^2 \qquad V_3 : y^2 = x^3.$$

Using the previous example, we see that any singular point on V_1 (resp. V_2, V_3) satisfies the extra equations

$$V_1^{sing} : 2y = 0 = 3x^2 + 1 \qquad V_2^{sing} : 2y = 0 = 3x^2 + 2x \qquad V_3^{sing} : 2y = 0 = 3x^2.$$

Thus V_1 is nonsingular (because no $(x, y) \in V_1$ satisfies those extra relations), while V_2 and V_3 both have one singular point (namely $(0, 0)$). Draw a picture of $V_1(\mathbb{R})$, $V_2(\mathbb{R})$ and $V_3(\mathbb{R})$ to see the difference.

There is another characterization of smoothness, in terms of rational functions on the curve C. More precisely, given an affine curve $C \subset \mathbb{A}^n$ and a point $P = (a_1, \ldots, a_n) \in C$, we define the following map:

$$f \in \overline{k}[x_1, \ldots, x_n] \mapsto f_P^{(1)} := \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(P) \cdot (x_i - a_i) \in \overline{k}[x_1, \ldots, x_n],$$

which to a polynomial f associates the "first order part of f at P" (in the Taylor expansion of f at P). Note that the derivatives involved in the definition of $T_P C$ are formal derivatives of polynomials ($\partial/\partial X_i : X_i^n \mapsto n X_i^{n-1}$ and $X_j \mapsto 0$ for all $j \neq i$), and that no calculus is used.

Now define the tangent space of C at P to be the intersection

$$T_P C := \bigcap_{f \in I(C)} Z(f_P^{(1)}) \subset \mathbb{A}^n.$$

First, we remark that $f_P^{(1)}$ is a polynomial of degree 1 in $x_1, \ldots, x_n$; as such, it defines an affine function $\mathbb{A}^n \to \overline{k}$ (a "linear form" except that it has a "constant part"). Secondly, note that if $I(C)$ is generated by $f_1, \ldots, f_m$, then, for any $g \in I(C)$, the linear part $g_P^{(1)}$ is a linear combination of

$f^{(1)}_{1,P}, \ldots, f^{(1)}_{m,P}$. In particular, $T_P C = \bigcap_{i=1}^m Z(f^{(1)}_{i,P})$ is actually a finite intersection of translates of kernels of linear forms. Since $f^{(1)}_P$ is a polynomial of degree 1 for all $f \in I(C)$, the intersection $T_P C$ is actually an affine subspace of $\mathbb{A}^n$, and $P \in T_P C$ (make a picture). Therefore, up to translation by P, $T_P C$ is a sub-$\overline{k}$-vector space of $\overline{k}^n = \mathbb{A}^n$: in particular, it has a well-defined dimension as a $\overline{k}$-vector space. It follows easily from this discussion that

Proposition 2.5. — *The curve C is smooth at P if and only if* $\dim_{\overline{k}} T_P C = 1$.

Exercise 12. — Consider the function $d : C \to \mathbb{N}$, defined by $P \mapsto \dim_{\overline{k}} T_P C$. For each $r \in \mathbb{N}$, let $S(r) := \{P \in C : d(P) = r\}$. Show that $S(r)$ is an affine algebraic subset of $C \subset \mathbb{A}^n$.

Hint: use minors to express the fact that the Jacobian matrix $\left[\frac{\partial f_i}{\partial x_j}(P)\right]$ has rank $\leq n - r$.

Show that $d(P) = 1$ for "almost all points P".

We now give an alternative description of $T_P C$, which is more intrisic to C and can be used to defined the tangent space a point on a projective curve. For each point $P \in C$, recall that $\mathfrak{M}_P$ is a maximal ideal, and that there is an isomorphism $\overline{k}[C]/\mathfrak{M}_P \to \overline{k}$ (given by $f \mod \mathfrak{M}_P \mapsto f(P)$). The quotient abelian group $\mathfrak{M}_P/\mathfrak{M}_P^2$ then aquires the structure of a $\overline{k}$-vector space (sometimes called the cotangent space of C at P).

Proposition 2.6. — *Let C be a variety and $P \in C$. The point P is nonsingular if and only if* $\dim_{\overline{k}} \left(\mathfrak{M}_P/\mathfrak{M}_P^2\right) = 1$.

Proof. — Let us set up more notations. Suppose $P = (a_1, \ldots, a_n) \in C \subset \mathbb{A}^n$: by using a linear coordinate change $x'_i = x_i - a_i$, we can assume that P is the origin $(0, , \ldots, 0)$. In particular, $T_P C \subset \mathbb{A}^n$ is a sub vector space of $\overline{k}^n$ (and not only an affine subspace). We write $\mathfrak{M}_P$ (resp. M_P) for the maximal ideal of P in $\overline{k}[C]$ (resp. in $\overline{k}[x_1, \ldots, x_n]$. Indeed, recall that the Nullstellensatz gives a bijection between maximal ideals of $\overline{k}[C]$ (resp. $\overline{k}[x_1, \ldots, x_n]$) and points on C (resp. on $\mathbb{A}^n$). By our assumption that $P = (0, \ldots, \ldots)$, we have $M_P = \langle x_1, \ldots, x_n \rangle$. By writing down the definitions, one can check that $\mathfrak{M}_P \simeq M_P/I(C) \subset \overline{k}[C] = \overline{k}[x_1, \ldots, x_n]/I(C)$.

We write $(\overline{k}^n)^*$ for the dual of $\overline{k}^n$ (as a $\overline{k}$-vector space): it has basis $x_1, \ldots, x_n$. Since $P = (0, 0, \ldots, 0)$, the linear part $f^{(1)}_P$ at P of any polynomial $f \in \overline{k}[x_1, \ldots, x_n]$ is an element of $(\overline{k}^n)^*$: we can define the map

$$d : M_P \to (\overline{k}^n)^*, \quad f \mapsto f^{(1)}_P.$$

Now, d is surjective because $f = x_i$ is sent to x_i (the natural basis of $(\overline{k}^n)^*$). Moreover, $\ker d = M_P^2$ (because $f^{(1)}_P = 0$ if and only if f starts with quadratic terms in $x_1, \ldots, x_n$, which is equivalent to $f \in M_P^2$). The linear map d thus provides an isomorphism of $\overline{k}$-vector spaces $M_P/M_P^2 \simeq (\overline{k}^n)^*$.

Since $T_P C$ is a subvector space of $\overline{k}^n$, there is a restriction map $(\overline{k}^n)^* \to (T_P C)^*$ $(\lambda \mapsto \lambda\,|_{T_P C})$. Composing this restriction with the isomorphism induced by d, we get a linear map

$$D : M_P \to (\overline{k}^n)^* \to (T_P C)^*, \quad f \mapsto f^{(1)}_P.$$

As a composition of two surjective maps, D is itself surjective. I claim that $\ker D = I(C) + M_P^2$, so that $\mathfrak{M}_P/\mathfrak{M}_P^2 \simeq M_P/(M_P^2 + I(C)) \simeq (T_P C)^*$. Assuming the claim for the moment, and noticing that $\dim(T_P C)^* = \dim T_P C = n - \mathrm{rank} J_P$ (where J_P denotes the jacobian matrix of C at P), we obtain that

$$\dim \mathfrak{M}_P/\mathfrak{M}_P^2 + \mathrm{rank} J_P = \dim \mathbb{A}^n = n,$$

which implies the desired equivalence.

We now prove the claim. Let $f \in M_P$, then $f \in \ker D$ if and only if $f^{(1)}_P\,|_{T_P C} = 0$, if and only if $f^{(1)}_P$ is of the form $f^{(1)}_P = \sum a_i g^{(1)}_{i,P}$ for some $g_i \in I(C)$ (because $T_P C \subset \overline{k}^n$ is the vector space defined by $g^{(1)}_P = 0$ for all $g \in I(C)$). But f is of this form if and only if $f - \sum a_i g_i$ is in the kernel of d, *i.e.* if and only if $f - \sum a_i g_i$ is in M_P^2. Which concludes the proof of our claim that $\ker D = I(C) + M_P^2$. $\square$

We have actually proved above that tangent space of C at P is isomorphic to the dual of the cotangent space $T_P C \simeq \mathrm{Hom}_{\overline{k}-vs}(\mathfrak{M}_P/\mathfrak{M}_P^2, \overline{k})$. A curve C is smooth at P if and only if the tangent space $T_P C$ has the right dimension (*i.e.* 1), which is equivalent to the Jacobian matrix having maximal rank (*i.e.* $n-1$). Note that $\dim T_C V$ is always ≥ 1 for all $P \in C$ (and there is a nonempty open subset $U \subset C$ such that equality holds for all $P \in U$ – see exercise above or [**Har77**, I.5, Prop. 2A]).

Example 2.7. — Consider the point $P = (0,0)$ on the varieties V_1 and V_2 of the example above. In both cases, the ideal $\mathfrak{M}_P$ is generated by X and Y, and $\mathfrak{M}_P^2$ is thus generated by X^2, XY and Y^2. For V_1 we have $X \equiv Y^2 - X^3 \equiv 0 \bmod \mathfrak{M}_P^2$ so $\mathfrak{M}_P/\mathfrak{M}_P^2$ is generated by Y alone. For V_2 though, there are no nontrivial relation between X and Y modulo $\mathfrak{M}_P^2$ so $\mathfrak{M}_P/\mathfrak{M}_P^2$ requires X and Y as generators (*i.e.* dimension 2). This proves again that V_1 is nonsingular at $(0,0)$, but V_2 is singular.

The proposition above gives us an intrinsic criterion for smoothness of a curve at a point: it only depends on the local ring of C at P (up to isomorphism). We can now extend the definition of smoothness to projective curves.

Definition 2.8. — Let C be a projective curve, and $P \in C$ be a point. Given an affine part C' of C containing P (in more details: assume that $C \subset \mathbb{P}^n$ and that $P \in C \cap U_i$ for some i, then $C' = \phi_i^{-1}(C \cap U_i) \subset \mathbb{A}^n$), one says that C is smooth at P if and only if C' is smooth at P. Since the definition only depends on the local ring $\mathcal{O}_P$ of C at P (which is, by definition, that of C' at P), this notion makes sense because it does not depend on the choice of an affine part C' of C containing P.

Example 2.9. — It is sometimes easier to rely on explicit (affine or projective) equations. Assume here that $C \subset \mathbb{P}^2$ is given by a unique homogeneous equation $F \in \overline{k}[x_0, x_1, x_2]$ of degree d, and that $P = [a_0 : a_1 : a_2] \in C$.

Then $\sum \frac{\partial F}{\partial x_i}(P) x_i = 0$ is the equation of a hyperplane in $\mathbb{P}^2$ (*i.e.* a projective algebraic set defined by a linear homogeneous equation). This hyperplane plays the role of the tangent space of C at P: if $P \in C \cap U_i$ (some $U_i \simeq \mathbb{A}^n$), then this hyperplane is the projective closure of the affine tangent space to $C \cap U_i$ at P. This last claim can be checked using Euler's formula for homogeneous polynomials of degree d:

$$\sum x_i \frac{\partial F}{\partial x_i} = d \cdot F.$$

Example 2.10. — Given a field k of odd characteristic, consider the affine curve $C_0 \subset \mathbb{A}^2$ defined over k by the equation $C_0 : y^2 = x^4 + 1$. It is easily checked that C_0 is smooth.

The projective closure $\overline{C_0} \subset \mathbb{P}^2$ of C_0 is given by the equation

$$\overline{C_0} : \quad y^2 z^2 = x^4 + z^4.$$

One can check that $\overline{C_0}$ is singular at $[0:1:0]$ and that this is the only singular point.

We leave the proof of the following proposition as an exercise (you may want to restrict to the case where C is an affine curve defined by the vanishing of a single polynomial)

Proposition 2.11. — *A curve C has only finitely many singular points.*

See [**NX09**, Thm. 3.1.7], or [**Rei88**].

2.1.3. Interlude: definition of discrete valuations. — We add ∞ to the field of real numbers $\mathbb{R}$ to form the set $\mathbb{R} \cup \{\infty\}$, and we put $\infty + \infty = \infty + c = c + \infty = \infty$ for all $c \in \mathbb{R}$ and we agree that $c < \infty$.

Definition 2.12. — A discrete (normalized) valuation on a field K is a map $v : K \to \mathbb{Z} \cup \{\infty\}$ such that:

(i) $v(z) = \infty$ if and only if $z = 0$,
(ii) $v(yz) = v(y) + v(z)$ for all $y, z \in K$,
(iii) $v(y + z) \geq \min\{v(y), v(z)\}$ (ultrametric triangle inequality),
(iv) $v(K^*) = \mathbb{Z}$ (normalization).

Conditions (ii) and (iv) are equivalent to requiring that $v : K^* \to \mathbb{Z}$ be a surjective group homomorphism. Given a discrete valuation v on a field K, the set consisting of 0 and all $x \in K^*$ such that $v(x) \geq 0$ is a ring, called the valuation ring of v.

An integral domain R is called a dicrete valuation ring if there is a discrete valuation v on its field of fractions K such that R is the valuation ring of v. One can check that such a ring is local (*i.e.* it has a unique maximal ideal) with maximal ideal

$$\{0\} \cup \{x \in K^* : v(x) > 0\} = \{x \in K : v(x) > 0\}.$$

2.1.4. Consequences of smoothness. — There is a more algebraic interpretation of the last characterization of smoothness:

Proposition 2.13. — *Let C be a curve and $P \in C$ be a point at which C is smooth. Then $\mathcal{O}_P$ is a discrete valuation ring.*

Proof. — By definition of smoothness, the vector space $\mathfrak{M}_P/\mathfrak{M}_P^2$ is a one-dimensional vector space over $\overline{k} = \mathcal{O}_P/\mathfrak{M}_P$. Then use [**AM69**, Prop. 9.2]:

Lemma 2.14. — *Let R be a Noetherian local domain that is not a field, let $\mathfrak{M}$ be its maximal ideal, and $\kappa = R/\mathfrak{M}$ be its residue field. The following statement are equivalent:*

(i) R is a discrete valuation ring,
(ii) $\mathfrak{M}$ is principal,
(iii) $\dim_\kappa \mathfrak{M}/\mathfrak{M}^2 = 1$.

Here $\mathcal{O}_P$ is local (its only maximal ideal is $\mathfrak{M}_P$) and noetherian (because the localization of the quotient of a polynomial ring is), so the proposition follows. □

In the setting of the previous proposition, one can actually give an explicit description of the discrete valuation in question:

Definition 2.15. — Let C be a curve and $P \in C$ be a smooth point. The normalized discrete valuation on $\mathcal{O}_P$ is the map $\mathrm{ord}_P : \mathcal{O}_P \to \mathbb{N} \cup \{\infty\}$ given by:

$$\forall f \in \mathcal{O}_P, \qquad \mathrm{ord}_P(f) = \sup\left\{d \in \mathbb{N} : f \in \mathfrak{M}_P^d\right\}.$$

One can extend ord_P to the whole of $\overline{k}(C)$ by putting $\mathrm{ord}_P(f/g) = \mathrm{ord}_P(f) - \mathrm{ord}_P(g)$ (since $\overline{k}(C)$ is the fraction field of $\mathcal{O}_P$). We denote this extension by the same letter.

A uniformizer for C at P is any function $\pi \in \overline{k}(C)$ with $\mathrm{ord}_P(\pi) = 1$ (exercise: check that π generates $\mathfrak{M}_P$). Intuitively, π is a "local coordinate function for C around P" coming from a function $C \to \overline{k}$ having a simple zero at P.

Given a valuation ord_P on $\overline{k}(C)$ as above, one can recover $\mathcal{O}_P$ and $\mathfrak{M}_P$:

$$\mathcal{O}_P = \left\{f \in \overline{k}(C) : \mathrm{ord}_P(f) \geq 0\right\} \quad \text{and} \quad \mathfrak{M}_P = \left\{f \in \overline{k}(C) : \mathrm{ord}_P(f) > 0\right\}.$$

Notice that the nonzero elements of $\overline{k} \subset \overline{k}(C)$ have valuation 0. If P and Q are distinct nonsingular points on a projective curve C, then the corresponding valuations ord_P and ord_Q

are not the same (*i.e.* they have distinct valuation rings). Indeed, if $C \subset \mathbb{P}^n$, we can assume that $P = [a_0 : a_1 : \ldots : a_{n-1} : 1]$ and $Q = [b_0 : b_1 : \ldots : b_{n-1} : 1]$ with $a_0 \neq b_0$. Consider the function $f := (x_0/x_n - a_0)^{-1} \bmod I(C)$: $f \notin \mathcal{O}_P$ since $\mathrm{ord}_P f = -1$, but $f \in \mathcal{O}_Q$ since $\mathrm{ord}_Q f = 0$. Later on, we will see that it is possible to (almost) reconstruct a point $P \in C$ if we are given a discrete valuation on $\overline{k}(C)$.

Remark 2.16. — Let C be a curve defined over k. If P is a k-rational point on C, then it is not hard to show that $k(C)$ contains uniformizers for P. See [**Sil09**, Exercise II.16], or a Lemma below.

Definition 2.17. — Let C be a curve and $P \in C$ be a smooth point, and let $f \in \overline{k}(C)$. Then f can be seen as a function $f : C \to \mathbb{P}^1$, sending P to $[f(P) : 1]$ if f is regular at P and to $[1 : 0] = \infty$ otherwise.

The order of f at P is $\mathrm{ord}_P(f)$. If $\mathrm{ord}_P(f) > 0$, one says that f has a zero at P (or that P is a zero of f) and if $\mathrm{ord}_P(f) < 0$, one says that f has a pole at P (or that P is a pole of f).

If $\mathrm{ord}_P(f) \geq 0$, then f is regular (or defined) at P and one can evaluate f at P: writing $f(P)$ makes sense. Otherwise, f has a pole at P and we write $f(P) = \infty$.

Example 2.18. — Let $C = \mathbb{P}^1$ and choose $P = (a) \in \mathbb{A}^1 \subset \mathbb{P}^1$. Let $f \in \overline{k}(C) = \overline{k}(x)$. The valuation of f at P is the multiplicity of a as a root or pole of f. If a is a pole of f, the mutliplicity of a as a pole is taken with a minus sign. If $P = \infty \in \mathbb{P}^1 \smallsetminus \mathbb{A}^1$, then the valuation of f at $P = \infty$ is $-\deg f$, where deg means degree as a polynomial in x.

Proposition 2.19. — *Let C be a smooth curve (affine or projective) and $f \in \overline{k}(C)$ with $f \neq 0$. Then there are only finitely many points of C at which f has a pole or a zero. Furthermore, if f has no poles (or no zeros), then $f \in \overline{k}$.*

Proof. — Assume we have proved that f has finitely many poles, then using the result with $1/f$ will show that f has only finitely many zeros. So we need only prove the finiteness of poles of f. The proof of this can be found, for example, in [**Har77**]: see I.6.5, II.6.1 and I.3.4(a) there. □

Example 2.20. — Consider the two curves

$$C_1 : Y^2 = X^3 + X \qquad C_2 : Y^2 = X^3 + X^2.$$

Remember our earlier convention concerning affine equations for projective varieties: each of C_1, C_2 has a unique point at infinity. Let $P = (0, 0)$. Then C_1 is smooth at P, but C_2 is not. The maximal ideal $\mathfrak{M}_P$ of $\overline{k}[C_1]_P$ has the property that $\mathfrak{M}_P/\mathfrak{M}_P^2$ is generated by Y (see an example above), so for example

$$\mathrm{ord}_P(Y) = 1, \quad \mathrm{ord}_P(X) = 2, \quad \mathrm{ord}_P(2Y^2 - X) = 2, ...$$

(for the last, note that $2Y^2 - X = 2X^3 + X = X(2X^2 + 1)$). On the other hand, $\mathcal{O}_P$ is not a discrete valuation ring.

2.1.5. A lemma in Galois cohomology. —

Lemma 2.21. — *Let V be a $\overline{k}$-vector space, and assume that G_k acts continuously on V in a manner that is compatible with its action on $\overline{k}$. Let*

$$V_k := V^{G_k} = \{v \in V : \sigma(v) = v \ \forall \sigma \in G_k\}.$$

Then, $V \simeq \overline{k} \otimes_k V_k$. In words, the vector space V has a basis consisting of G_k-invariants vectors.

The hypothesis of "continuity" means that, for all $v \in V$, the subgroup

$$H_v := \{\sigma \in \mathrm{Gal}(\overline{k}/k) : \sigma(v) = v\} \subset G_k$$

of elements fixing v has finite index in G_k. In particular, this implies that, for all $v \in V$, there is a finite Galois extension L/k such that $\tau(v) = v$ for all $\tau \in \mathrm{Gal}(\overline{k}/L)$ (namely, take L to be the Galois closure of the fixed field of H_v).

Proof. — It is not hard to check that V_k is a vector space over k. We need to show that any $v \in V$ is a $\overline{k}$-linear combination of elements of V_k (the converse inclusion being obvious). Let $v \in V$ and choose a finite Galois extension L/k (inside $\overline{k}$) such that $\tau(v) = v$ for all $\tau \in \mathrm{Gal}(\overline{k}/L)$ (*i.e.* "v is defined over L"). Now let $\alpha_1, \dots, \alpha_n$ be a k-basis of L (seen as a vector space over k), and let $\sigma_1, \dots, \sigma_n$ denote the elements of $\mathrm{Gal}(L/k)$. For all $i = 1, \dots, n$, consider

$$w_i := \sum_{j=1}^{n} \sigma_j(\alpha_i \cdot v) = \sum_{\sigma \in \mathrm{Gal}(L/k)} \sigma(\alpha_i \cdot v) = \mathrm{Trace}_{L/k}(\alpha_i \cdot v).$$

The, by construction, $\sigma(w_i) = w_i$ for all $\sigma \in \mathrm{Gal}(\overline{k}/k)$, which means that $w_i \in V_k$. By a classical lemma (sometimes called Dedekind's lemma, or Artin's Lemma), the matrix $[\sigma_j(\alpha_i)]_{1 \le i,j \le n}$ is nonsingular, and thus invertible. This fact is often proved in a course about Galois theory (see the lecture notes for *Algebra 3*, Lemma 23.15). We then deduce that each of the $\sigma_j(v)$ can be written as a L-linear combination of $w_1, \dots, w_n$. Which concludes the proof.

As a remark, note that a fancy way of stating this Lemma is: $H^1\left(\mathrm{Gal}(\overline{k}/k), \mathrm{GL}_n(\overline{k})\right) = 0$. If you know a bit of Galois cohomology, you can reprove the Lemma as a consequence of Hilbert's theorem 90. □

2.1.6. Smoothness and extensions of function fields. — The next proposition is useful when one deals with curves over finite fields (of positive characteristic):

Proposition 2.22. — *Let C be a curve defined over k and let $\pi \in k(C)$ be a uniformizer of C at a smooth point $P \in C(k)$. Then $k(C)$ is a finite separable extension of $k(\pi)$.*

Proof. — The field $k(C)$ is clearly a finite algebraic extension of $k(\pi)$, since it is finitely generated over k, has transcendence degree one over k (since C is a curve), and $\pi \notin k$. Now let $f \in k(C)$, the claim is that f is separable over $k(\pi)$.

In any case, f is algebraic over $k(\pi)$, so it satisfies a polynomial relation

$$\Phi(\pi, f) = 0, \qquad \text{with } \Phi(\Pi, X) = \sum a_{i,j} \Pi^i X^j \in k[\Pi, X].$$

We may further assume that Φ is chosen so as to have minimal degree in X (*i.e.* $\Phi(\pi, X)$ is a minimal polynomial for f over $k(\pi)$). We denote by $p > 0$ the characteristic of k.

If $\Phi(\Pi, X)$ contains a nonzero term $a_{i,j}\Pi^i X^j$ where p does not divide j, then $\partial\Phi(\pi, X)/\partial X$ is not identically zero, so f is separable over $k(\pi)$.

We now need to show that this actually holds. Suppose instead that $\Phi(\Pi, X)$ has the form $\Psi(\Pi, X^p)$ and let us find a contradiction. The main point is that, for all $F(\Pi, X) \in k[\Pi, X]$, $F(\Pi^p, X^p)$ is a p-th power (this is true because we have assumed that the base-field k is perfect of characteristic p, which implies that every element of k is a p-th power, thus if $F = \sum a_{i,j}\Pi^i X^j$ and if $b_{i,j}^p = a_{i,j}$, then $F(\Pi^p, X^p) = \left(\sum b_{i,j}\Pi^i X^j\right)^p$). Back to $\Phi(\Pi, X) = \Psi(\Pi, X^p)$, we regroup the terms according to powers of X modulo p:

$$\Phi(\Pi, X) = \Psi(\Pi, X^p) = \sum_{k=0}^{p-1} \left(\sum_{i,j} b_{i,j,k} \Pi^{ip} X^{jp} \right) X^k = \sum_{k=0}^{p-1} \phi_k(\Pi^p, X^p) \cdot X^k = \sum_{k=0}^{p-1} \phi_k(\Pi, X)^p \cdot X^k.$$

By assumption, we have $\Phi(\pi, f) = 0$ and, since π is a uniformizer for C at P, we also have

$$\mathrm{ord}_P(\phi_k(\pi, f)^p f^k) = p \cdot \mathrm{ord}_P(\phi_k(\pi, f)) + k \cdot \mathrm{ord}_P \pi \equiv k \bmod p.$$

In particular, each of the terms in $\sum \phi_k(\pi, f) \cdot f^k$ has a distinct order at P, so every term must vanish (because the sum does). But at least one of the $\phi_k(\Pi, X)$ must involve X and for that k, the relation $\phi_k(\pi, f) = 0$ contradicts our choice of $\Phi(\Pi, X)$ as a minimal polynomial for f over $k(\pi)$ (note that $\deg_\Pi \phi_k(\Pi, X) \le \frac{1}{p} \deg_\Pi \Phi(\Pi, X)$. The contradiction completes the proof. □

2.1.7. Example. —

Example 2.23. — Let us consider the case $d = 4$ of hyperelliptic curves: C_0 has an affine equation

$$C_0 : y^2 = a_0x^4 + a_1x^3 + a_2x^2 + a_3x + a4.$$

We define a map: $\Phi = [1 : x : y : x^2] : C_0 \to \mathbb{P}^3$. Letting $\Phi = [X_0 : X_1 : X_2 : X_3]$, the ideal of the image clearly contains the following two homogeneous polynomials:

$$F = X_3X_0 - X_1^2, \quad G = X_2^2X_0^2 - a_0X_1^4 - a_1X_1^3X_0 - a_2X_1^2X_0^2 - a_3X_1X_0^3 - a_4X_0^4.$$

However, the zero set of these two polynomials cannot be the desired curve C, since it includes the lines $X_0 = X_1 = 0$. So we substitute $X_1^2 = X_0X_3$ in G an cancel an X_0^2 to obtain the quadratic polynomial (homogeneous of degree 2):

$$H = X_2^2 - a_0X_3^2 - a_1X_1X_3 - a_2X_0X_3 - a_3X_0X_1 - a_4X_0^2.$$

We claim that the ideal generated by F and H gives a smooth curve C.

To see this, note first that, if $X_0 \neq 0$, then dehomogenization with respect to X_0 gives the affine curve (setting $x = X_1/X_0$, $y = X_2/X_0$ and $z = X_3/X_0$):

$$C_0' : z = x^2 \text{ and } y^2 = a_0z^2 + a_1xz + a_2z + a_3x + a_4.$$

Substituting the first equation into the second gives us back the equation for the original curve C_0. So $C_0' = C_0 = C \cap \{X_0 \neq 0\}$.

Next, if $X_0 = 0$ then necessarily $X_1 = 0$, and then $X_2 = \pm\sqrt{a_0} \cdot X_3$. Thus, C has two points $[0 : 0 : \pm\sqrt{a_0} : 1]$ on the hyperplane $\{X_0 = 0\}$ (note that $a_0 \neq 0$ since we have assumed that f has exactly degree 4). To check that C is nonsingular, it suffices to do so at these two points (because of the previous paragraph). To prove nonsingularity at these two points, we start by dehomogenizing with respect to X_3: setting $u = X_0/X_3$, $v = X_1/X_3$ and $w = X_2/X_3$, we obtain the equations:

$$C_3' : u = v^2 \text{ and } w^2 = a_0 + a_1v + a_2u + a_3uv + a_4u^2,$$

from which we obtain the single affine equation:

$$C_3' : w^2 = a_0 + a_1v + a_2v^2 + a_3v^3 + a_4v^4.$$

Again using the assumption that the polynomial f has no double roots, we see that the points $(v, w) = (0, \pm\sqrt{a_0})$ are nonsingular.

We summarize the preceding discussion:

Proposition 2.24. — *Let $f \in k[x]$ be a polynomial of degree $d \geq 4$ with* $\operatorname{disc}(f) \neq 0$. *There exists a smooth projective curve $C \subset \mathbb{P}^3$ with the following properties:*

(a) The intersection of C with $\mathbb{A}^3 = \{X_0 \neq 0\}$ is isomorphic to the affine curve $y^2 = f(x)$.
(b) The intersection of C with the hyperplane $\{X_0 = 0\}$ consists of the two points $[0 : 0 : \pm\sqrt{a_0} : 1]$, where a_0 is the leading coefficient of f.

See the first homework assignment for a more general discussion on hyperelliptic curves.

2.2. Exercises for Chapter 2

Exercise 13. — For each of the following algebraic varieties V, find the singular points of V and sketch $V(\mathbb{R})$:

(a) $V_1 : y^2 = x^3$ in $\mathbb{A}^2$,
(b) $V_2 : 4x^2y^2 = (x^2 + y^2)^3$ in $\mathbb{A}^2$,
(c) $V_3 : y^2 = x^4 + y^4$ in $\mathbb{A}^2$,
(d) $V_4 : x^2 + y^2 = (z - 1)^2$ in $\mathbb{A}^3$.

Exercise 14. — Let V be the projective variety

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

Show that the rational map $\phi : V \to \mathbb{P}^2$ given by $\phi = [X^2 : XY : Z^2]$ is a morphism.

Exercise 15. — Let W be the projective variety

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

Let $\phi : \mathbb{P}^1 \to W$ be the rational map given by $\phi = [S^2T : S^3 : T^3]$. Show that ϕ is a morphism. Then find a rational map $\psi : V \to \mathbb{P}^1$ such that $\phi \circ \psi$ and $\psi \circ \phi$ are the identity map wherever they are defined. Is ϕ an isomorphism?

Exercise 16. — 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 projective hypersurface in $\mathbb{P}^n$ defined by f. Prove that, if a point $P \in V$ is singular, then

$$\frac{\partial f}{\partial x_0}(P) = \frac{\partial f}{\partial x_1}(P) = \cdots = \frac{\partial f}{\partial x_n}(P) = 0.$$

(Thus, for hypersurfaces in $\mathbb{P}^n$, we can check for smoothness directly in homogeneous coordinates).

Exercise 17. — Determine the singular points on the following curves in $\mathbb{A}^2$:

(a) $y^2 = x^3 - x$,
(b) $y^2 = x^3 - 6x^2 + 9x$,
(c) $x^2y^2 + x^2 + y^2 + 2xy(x + y + 1) = 0$,
(d) $x^2 = x^4 + y^4$,
(e) $xy = x^6 + y^6$,
(f) $x^3 = y^2 + x^4 + y^4$,
(g) $x^2y + xy^2 = x^4 + y^4$.

Exercise 18. — Show that the hypersurface $X_d \subset \mathbb{P}^n$ defined by $x_0^d + \cdots + x_n^d = 0$ is nonsingular if the characteristic of k does not divide $d \in \mathbb{Z}_{\geq 1}$.

Exercise 19. — Prove that the intersection of a hypersurface $V \subset \mathbb{A}^n$ (that is not a hyperplane) with the tangent hyperplane T_PV to V at $P \in V$ is singular at P.