Chapter 10

Ex. 10.1 *If K is an infinite field and $f(x_1, x_2, \ldots, x_n)$ is a non-zero polynomial with coefficients in K, show that f is not identically zero on $A_n(K)$. (Hint: Imitate the proof of Lemma 1 in Section 2.)*

Proof. Assume that f vanishes on all of $A_n(K)$. We have to prove that f is the zero polynomial.

The proof is by induction on n. If $n = 1$, then f is a polynomial with one variable, which vanishes on $A_1(K) = K$. Since K is infinite, f have more than d roots, where $d = \deg(f)$, thus f is the zero polynomial.

Suppose that we have proved the result for $n - 1$ and write

$$f(x_1, \ldots, x_n) = \sum_{i=0}^{s-1} g_i(x_1, \ldots, x_{n-1}) x_n^i,$$

where the x_i are variables, and g_i are polynomials in $x_1, \ldots, x_{n-1}$.

For all $(a_1, \ldots, a_n) \in K^n$,

$$0 = f(a_1, \ldots, a_n) = \sum_{i=0}^{s-1} g_i(a_1, \ldots, a_{n-1}) a_n^i.$$

From the result for $n = 1$, we obtain that the polynomial $\sum_{i=0}^{s-1} g_i(a_1, \ldots, x_{a-1}) x_n^i$ is null, thus for all $(a_1, \ldots, a_{n-1}) \in K^{n-1}$,

$$g_i(x_1, \ldots, x_{n-1}) = 0.$$

The induction hypothesis shows that $g_i(x_1, \ldots, x_{n-1}) = 0$, thus $f(x_1, \ldots, x_n) = 0$. $\square$

Ex. 10.2 *In section 1 it was asserted that H, the hyperplane at infinity in $P_n(F)$, has the structure of $P_{n-1}(F)$. Verify this by constructing a one-to-one, onto map from $P_{n-1}(F)$ to H.*

Proof. Note that if one representative $(x_0, \ldots, x_n)$ of a projective point satisfies $x_0 = 0$, then it is the same for all representatives of this point, so we can define

$$\overline{H} = \{[x_0, \ldots, x_n] \in P_n(F) \mid x_0 = 0\},$$

where we write for simplicity $[x_0, \ldots, x_n]$ for $[(x_0, \ldots, x_n)]$.

Consider

$$\psi \left\{ \begin{array}{ccc} \overline{H} & \to & P_{n-1}(F) \\ [0, x_1, \ldots, x_n] & \mapsto & [x_1, \ldots, x_n] \end{array} \right.$$

Then ψ is well-defined. Indeed, if $(0, x_1, \ldots, x_n) \sim (0, y_1, \ldots, y_n)$, then there is some $\lambda \in F^*$ such that $(0, y_1, \ldots, y_n) = \lambda(0, x_1, \ldots, x_n)$, thus $(y_1, \ldots, y_n) = \lambda(x_1, \ldots, x_n)$, and $[x_1, \ldots, x_n] = [y_1, \ldots, y_n]$.

If $\psi([0, x_1, \ldots, x_n]) = \psi([0, y_1, \ldots, y_n])$, then $[(x_1, \ldots, x_n)] = [(y_1, \ldots, y_n)]$, so ther is some $\lambda \in F^*$ such that $y_i = \lambda x_i$, $i = 1, \ldots, n$. Since $0 = \lambda 0$, $(0, y_1, \ldots, y_n) \sim (0, x_1, \ldots, x_n)$, therefore $[0, x_1, \ldots, x_n] = [0, y_1, \ldots, y_n]$, so ψ is injective.

Moreover if $[x_1, \ldots, x_n]$ is any projective point of $P_{n-1}(F)$, then $[x_1, \ldots, x_n] = \psi([0, x_1, \ldots, x_n])$ so ψ is surjective.

To conclude, ψ is a bijection. $\square$

Ex. 10.3 *Suppose that F has q elements. Use the decomposition of $P_n(F)$ into finite points and points at infinity to give another proof of the formula for the number of points in $P_n(F)$.*

Proof. By exercise 2, the bijection ψ shows that $|\overline{H}| = |P_{n-1}(F)|$. Therefore

$$|P_n(F)| = |P_n(F) \setminus \overline{H}| + |\overline{H}| = |A_n(F)| + |P_{n-1}(F)| = q^n + |P_{n-1}(F)|.$$

Moreover $|P_0(F)| = 1$. Consequently,

$$|P_n(F)| = |P_0(F)| + \sum_{k=1}^{n}(|P_k(F)| - |P_{k-1}(F)|) = 1 + \sum_{k=1}^{n} q^k = q^n + q^{n-1} + \cdots + q + 1,$$

This gives another proof of the formula for the number of points in $P_n(F)$. $\square$

Ex. 10.4 *The hypersurface defined by a homogeneous polynomial of degree 1, $a_0x_0 + a_1x_1 + \cdots + a_nx_n$ is called a hyperplane. Show that any hyperplane in $P_n(F)$ has the same number of elements as $P_{n-1}(F)$.*

Proof. Define the hyperplane $\overline{K}$ by

$$\overline{K} = \{[x_0, \ldots, x_n] \in P_n(F) \mid a_0x_0 + \cdots + a_nx_n = 0\},$$

where $(a_0, \ldots, a_n) \neq (0, \ldots, 0)$ (if $(a_0, \ldots, a_n) \neq (0, \ldots, 0)$, then $\overline{K} = P_n(F)$ is not a hyperplane). Note that, if $(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n)$, there is $\lambda \in F^*$ such that $y_i = \lambda x_i,\ i = 0, \ldots, n$, thus $a_0x_0 + \cdots + a_nx_n \iff 0 = a_0y_0 + \cdots + a_ny_n = 0$, so that the condition does'nt depends of the choice of the representative of the projective point.

Since $(a_0, \ldots, a_n) \neq (0, \ldots, 0)$, suppose, without loss of generality, that $a_0 \neq 0$. Consider

$$\chi \left\{ \begin{array}{ccc} \overline{K} & \to & P_{n-1}(F) \\ [x_0, \ldots, x_n] & \mapsto & [x_1, \ldots, x_n] \end{array} \right.$$

Then χ is well defined. Indeed, if $(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n)$, there is some $\lambda \in F^*$ such that $(y_0, \ldots, y_n) = \lambda(x_0, \ldots, x_n)$. In particular, $(y_1, \ldots, y_n) = \lambda(x_1, \ldots, x_n)$, thus $[x_1, \ldots, x_n] = [y_1, \ldots, y_n]$.

If $\chi([x_0, \ldots, x_n]) = \chi([y_0, \ldots, y_n])$, where $[x_0, \ldots, x_n]$ and $[y_0, \ldots, y_n]$ are in $\overline{K}$, then $[x_1, \ldots, x_n] = [y_1, \ldots, y_n]$, thus there is $\lambda \in F^*$ such that $(y_1, \ldots, y_n) = \lambda(x_1, \ldots, x_n)$. Since $a_0 \neq 0$,

$$y_0 = -\frac{1}{a_0}(a_1y_1 + \cdots + a_ny_n) = -\lambda\frac{1}{a_0}(a_1x_1 + \cdots + a_nx_n) = \lambda x_0,$$

therefore $[x_0, \ldots, x_n] = [y_0, \ldots, y_n]$. So φ is injective.

At last, let $[x_1, \ldots, x_n]$ be any point of $P_{n-1}(F)$. Define $x_0 = -\frac{1}{a_0}(a_1x_1 + \cdots + a_nx_n)$. Then $a_0x_0 + \cdots + a_nx_n = 0$, so that $[x_0, \ldots, x_n] \in \overline{K}$, and $\chi([x_0, \ldots, x_n]) = [x_1, \ldots, x_n]$. This proves that χ is surjective.

To conclude, χ is a bijection, therefore $|\overline{K}| = |P_{n-1}(F)| = q^{n-1} + \cdots + q + 1$. $\square$

Ex. 10.5 *Let $f(x_0, x_1, x_2)$ be a homogeneous polynomial of degree n in $F(x_0, x_1, x_2]$. Suppose that not every zero of $a_0x_0 + a_1x_1 + a_2x_2$ is a zero of f. Prove that there are at most n common zeros of f and $a_0x_0+a_1x_1+a_2x_2$ in $P_2(F)$. In more geometric language this says that a curve of degree n and a line have at most n points in common unless the line is contained in the curve.*

Proof. Let $\mathscr{C}$ be the curve with equation $f(x_0, x_1, x_2) = 0$.

Since $a_0x_0 + a_1x_1 + a_2x_2 = 0$ is the equation of a line l, $(a_0, a_1, a_2) \neq 0$, so that we can suppose without loss of generality that $a_0 \neq 0$. Then

$$\begin{aligned} [u_0, u_1, u_2] \in l &\iff a_0u_0 + a_1u_1 + a_2u_2 = 0 \\ &\iff u_0 = -\frac{a_1}{a_0}u_1 - \frac{a_2}{a_0}u_2 \\ &\iff u_0 = \alpha u_1 + \beta u_2, \end{aligned}$$

where $\alpha = -\frac{a_1}{a_0}$, $\beta = -\frac{a_2}{a_0}$. Therefore

$$\begin{aligned} [u_0, u_1, u_2] \in \mathscr{C} \cap l &\iff \begin{cases} a_0u_0 + a_1u_1 + a_2u_2 & = 0, \\ f(u_0, u_1, u_2) & = 0, \end{cases} \\ &\iff \begin{cases} u_0 = \alpha u_1 + \beta u_2, & \\ f(\alpha u_1 + \beta u_2, u_1, u_2) & = 0. \end{cases} \end{aligned}$$

Let $[u_0, u_1, u_2] \in \mathscr{C} \cap l$.

We show that $u_1 \neq 0$. If $u_1 = 0$, then $u_0 = \beta u_2$, therefore $[u_0, u_1, u_2] = [\beta u_2, 0, u_2] = [\beta, 0, 1]$, and $f(\beta u_2, 0, u_2) = 0$. Therefore $p = [\beta, 0, 1] \in \mathscr{C} \cap l$.

Since $[1, 0, 0]$ and $[\beta, 0, 1]$ are two distinct points of l, an equation of l is

$$\begin{vmatrix} 1 & 0 & 0 \\ \beta & 0 & 1 \\ x_0 & x_1 & x_2 \end{vmatrix} = -x_1,$$

thus an equation of l is given by x_1, therefore no equation $a_0x_0+a_1x_1+a_2x_2$ of l satisfies $a_0 \neq 0$, and this is in contradiction with $a_0 \neq 0$. We have proved $u_1 \neq 0$.

Since f is homogeneous of degree n,

$$0 = u_1^n f\left(\alpha + \beta\frac{u_2}{u_1}, 1, \frac{u_2}{u_1}\right),$$

and using $u_1 \neq 0$,

$$0 = f\left(\alpha + \beta\frac{u_2}{u_1}, 1, \frac{u_2}{u_1}\right).$$

□

Consider the formal polynomial $P(x) = f(\alpha + \beta x, 1, x) \in F[x]$.

Then $\deg(P) \leq n$. If $P \neq 0$, then P has at most n roots $\lambda_1, \dots, \lambda_k$, where $k \leq n$. In this case, $u_2 = \lambda_i u_1$ and $u_0 = \alpha u_1 + \beta u_2 = u_1(1 + \alpha\lambda_i)$, therefore

$$[u_0, u_1, u_2] = [1 + \alpha\lambda_i, 1, \lambda_i], \ 1 \leq i \leq k,$$

so that $\mathscr{C}$ and l have at most n points in common.

Therefore, if $|\mathscr{C} \cap l| > n$, then $P = f(\alpha + \beta x, 1, x) = 0$.

Similarly, by exchanging the roles of u_1, u_2, if $|\mathscr{C} \cap l| > n$, then $u_2 \neq 0$, and

$$0 = f\left(\alpha\frac{u_1}{u_2} + \beta, u\frac{u_1}{u_2}, 1\right),$$

so that the same reasoning gives $Q(x) = f(\alpha x + \beta, x, 1) = 0$.

Let $[v_0, v_1, v_2]$ be any point on l.

If $v_1 \neq 0$,

$$f(v_0, v_1, v_2) = f(\alpha v_1 + \beta v_2, v_1, v_2) = v_1^n f\left(\alpha + \beta\frac{v_2}{v_1}, 1, \frac{v_2}{v_1}\right) = v_1^n P\left(\frac{v_2}{v_1}\right) = 0.$$

If $v_1 = 0$, then $[v_0, v_1, v_2] = [\beta, 0, 1] = p$, thus

$$f(\beta, 0, 1) = Q(0) = 0.$$

This proves that $l \subset \mathscr{C}$.

To conclude, if $l \not\subset \mathscr{C}$, then $|l \cap \mathscr{C}| \leq n :$ a curve of degree n and a line have at most n points in common unless the line is contained in the curve.

Ex. 10.6 *Let F be a field with q elements. Let $M_n(F)$ be the set of $n \times n$ matrices with coefficients in F. Let $\mathrm{SL}_n(F)$ be the subset of those matrices with determinant equal to one. Show that $\mathrm{SL}_n(F)$ can be considered as a hypersurface in $A^{n^2}(F)$. Find a formula for the number of points on this hypersurface. [Answer:$(q-1)^{-1}(q^n-1)(q^n-q)\cdots(q^n-q^{n-1})$.]*

Proof. If $M = (a_{i,j})_{1\leq i\leq n, 1\leq j\leq n} \in M_n(F)$,

$$M \in \mathrm{SL}_n(F) \iff \sum_{\sigma\in S_n} \mathrm{sgn}(\sigma) a_{\sigma(1)1}\cdots a_{\sigma(n)n}.$$

if $f(x_{1,1}, \ldots, x_{n,n}) = \sum_{\sigma\in S_n} \mathrm{sgn}(\sigma) x_{\sigma(1)1}\cdots x_{\sigma(n)n}$, then $M \in \mathrm{SL}_n(F)$ if and only if $f(a_{1,1}, \ldots, a_{n,n}) = 0$, where f is a non zero polynomial, since it contains the non zero term $x_{1,1}\cdots x_{n,n}$. Therefore $\mathrm{SL}_n(F)$ is an hypersurface of $M_n(F)$.

Since a matrix $M \in M_n(F)$ is inversible if and only if its columns $(C1, \ldots, C_n)$ is a basis of F^n, the number of matrices in $\mathrm{GL}_n(F)$ is

$$(q^n-1)(q^n-q)\cdots(q^n-q^{n-1}).$$

Indeed we choose C_1 between (q^n-1) non zero scalars, then we choose C_2 between the q^n-q vectors $v \notin \langle C_1\rangle$. If $C_1, \ldots, C_k$ are chosen, we take C_{k+1} between the q^n-q^k vectors $v \notin \langle C_1, \ldots, C_k\rangle$. At last, we choose $C_n \notin \langle C_1, \ldots C_{n-1}\rangle$. This gives

$$|\mathrm{GL}_n(F)| = (q^n-1)(q^n-q)\cdots(q^n-q^{n-1}).$$

Moreover, $\mathrm{SL}_n(F)$ is the kernel of the group homomorphism

$$\begin{cases} \mathrm{GL}_n(F) & \to & F^* \\ M & \mapsto & \det(M). \end{cases}$$

Therefore $F^* \simeq \mathrm{GL}_n(F)/\mathrm{SL}_n(F)$. This gives

$$|\mathrm{SL}_n(F)| = |\mathrm{GL}_n(F)|/|F^*| = (q-1)^{-1}(q^n-1)(q^n-q)\cdots(q^n-q^{n-1}).$$

$\square$

Ex. 10.7 *Let $f \in F[x_0, \dots, x_n]$. One can define the partial derivatives $\partial f/\partial x_0, \dots, \partial f/\partial x_n$ in a formal way. Suppose that f is homogeneous of degree m. Prove that $\sum_{i=0}^n x_i(\partial f/\partial x_i) = mf$. This result is due to Euler. (Hint: Do it first for the case that f is a monomial.)*

Proof. For the case that $f = x_1^{a_1} \cdots x_n^{a_n}$ is a monomial, where $a_1 + \ldots + a_n = m = \deg(f)$, then

$$\frac{\partial f}{\partial x_i} = a_i x_1^{a_1} \cdots x_i^{a_i - 1} \cdots x_n^{a_n}, \qquad i = 1, \dots, n.$$

Therefore $x_i \partial f/\partial x_i = a_i f$, and

$$\sum_{i=1}^n x_i \frac{\partial f}{\partial x_i} = \left(\sum_{i=1}^n a_i \right) f = mf.$$

Since the maps $f \mapsto \sum_{i=1}^n x_i \frac{\partial f}{\partial x_i}$ and $f \mapsto mf$ are $FG-$ linear, and since every homogeneous polynomial f is a linear combination of monomial with degree m, the relation is true for all such polynomials.

To conclude, every homogeneous polynomial $f \in F[x_0, \dots, x_n]$ of degree m satisfies

$$\sum_{i=1}^n x_i \frac{\partial f}{\partial x_i} = mf.$$

□

Ex. 10.8 *(continuation) If f is homogeneous, a point $\overline{a}$ on the hypersurface defined by f is said singular if it is simultaneously a zero of all the partial derivatives of f. If the degree of f is prime to the characteristic, show that a common zero of all the partial derivatives of f is automatically a zero of f.*

Proof. If $\frac{\partial f}{\partial x_i}(\overline{a}) = 0$ for all $i = 1, \dots, n$, then $mf(\overline{a}) = \sum\limits_{i=1}^n x_i \frac{\partial f}{\partial x_i}(\overline{a}) = 0$. Since $m = \deg(f)$ is prime with the characteristic, then m is non zero in the field F, thus $f(\overline{a}) = 0$. □

Ex. 10.9 *If m is prime to the characteristic of F, show that the hypersurface defined by $a_0 x_0^m + a_1 x_1^m + \cdots + a_n x_n^m$ has no singular points.*

Note: The sentence is not true if some coefficient a_i is zero. To give an counterexample, the projective curve given by $f(x_0, x_1, x_2) = x_1^2 - x_2^2$ is the union of two lines, and the intersection point $a = [1, 0, 0]$ of these two lines is singular : $\partial f/\partial x_0(a) = \partial f/\partial x_1(a) = \partial f/\partial x_2(a) = 0$. We must assume that $a_i \neq 0$ for every index i (see the hint p. 371).

Proof. Let V be the projective hypersurface defined by $f(x_0, \dots, x_n) = a_0 x_0^m + a_1 x_1^m + \cdots + a_n x_n^m$.

If $m = 1$, V is an hyperplane, without singularity since $\frac{\partial f}{\partial x_i}(a) = a_i \neq 0$ for some index i.

We assume now that $m > 1$. If $a = [u_0, \dots, u_n] \in V$ is a singular point,

$$\frac{\partial f}{\partial x_i}(a) = m a_i u_i^{m-1} = 0 \qquad (i = 1, \dots, n).$$

Since m is prime with the characteristic, $m \neq 0$ in F, and $a_i \neq 0$, thus $u_i = 0$ for all indices i. Then $[u_0, \dots, u_n]$ is not a projective point. This prove that V has no singular point. □

Ex. 10.10 *A point on an affine hypersurface is said to be singular if the corresponding point on the projective closure is singular. Show that this is equivalent to the following definition. Let $f \in F[x_1, x_2, \dots, x_n]$, not necessarily homogeneous, and $a \in H_f(F)$. Then a is singular if it is a common zero of $\partial f/\partial x_i$ for $i = 1, 2, \dots, n$.*

Proof. Let $H_f(F)$ an affine hypersurface defined by $f(x_1, \dots, x_n)$, with $\deg(f) = d$, and $a = (u_1, \dots, u_n) \in F$.

- Suppose that the corresponding point $\overline{a} = [1, u_1, \dots, u_n] \in \overline{F}$ is singular, and let

$$\overline{f}(y_0, \dots, y_n) = y_0^d f\left(\frac{y_1}{y_0}, \dots, \frac{y_i}{y_0}, \dots, \frac{y_n}{y_0}\right)$$

be the homogeneous polynomial defining $\overline{F}$. Then the chain rule gives

$$\frac{\partial \overline{f}}{\partial y_i}(x_0, \dots, x_n) = x_0^{d-1} \frac{\partial f}{\partial x_i}\left(\frac{x_1}{x_0}, \dots, \frac{x_i}{x_0}, \dots, \frac{x_n}{x_0}\right).$$

Since $\overline{a}$ is singular,

$$0 = \frac{\partial \overline{f}}{\partial y_i}(\overline{a}) = \frac{\partial \overline{f}}{\partial y_i}(1, u_1, \dots, u_n) = \frac{\partial f}{\partial x_i}(u_1, \dots, u_n) = \frac{\partial f}{\partial x_i}(a).$$

This proves that a is a common zero of $\partial f/\partial x_i$ for $i = 1, 2, \dots, n$

- Conversely, suppose that $\partial f/\partial x_i(a) = 0$ for $i = 1, \dots, n$. Then

$$\frac{\partial \overline{f}}{\partial y_i}(\overline{a}) = \frac{\partial \overline{f}}{\partial y_i}(1, u_1, \dots, u_n) = \frac{\partial f}{\partial x_i}(u_1, \dots, u_n) = 0,$$

which proves that $\overline{a}$ is singular.

□

Ex. 10.11 *Show that the origin is a singular point on the curve defined by $y^2 - x^3 = 0$.*

Proof. If $f(x, y) = y^2 - x^3$, then

$$\frac{\partial f}{\partial x} = 3x^2, \qquad \frac{\partial f}{\partial y} = 2y,$$

thus $\partial f/\partial x(0, 0) = \partial f/\partial y(0, 0) = 0$. This proves that the origin is a singular point for the curve defined by f. □

Ex. 10.12 *Show that the affine curve defined by $x^2 + y^2 + x^2y^2 = 0$ has two points at infinity and that both are singular.*

Proof. The homogeneous equation of this curve is

$$\overline{f}(t, x, y) = x^2t^2 + y^2t^2 + x^2y^2,$$

where $t = 0$ is the equation of the line at infinity.

The point $\overline{a} = [u_0, u_1, u_2]$ is a point at infinity if $u_0 = 0$. This gives the equation

$$\overline{f}(0, u_1, u_2) = u_1^2u_2^2 = 0,$$

where $u_1 \neq 0$ or $u_2 \neq 0$ (otherwise $u_0 = u_1 = u_2 = 0$, and $[u_0, u_1, u_2]$ is not a projective point).

If $u_1 \neq 0$, then $u_2 = 0$, and if $u_2 \neq 0$, then $u_1 = 0$.

Therefore $\overline{a} = [0, u_1, 0] = [0, 1, 0]$, or $\overline{a} = [0, 0, u_2] = [0, 0, 1]$.

$p = [0, 1, 0]$ and $q = [0, 0, 1]$ are the two points at infinity of the curve.

$$\frac{\partial \overline{f}}{\partial t} = 2t(x^2 + y^2), \qquad \frac{\partial \overline{f}}{\partial x} = 2x(t^2 + y^2), \qquad \frac{\partial \overline{f}}{\partial y} = 2y(t^2 + x^2).$$

Therefore

$$\frac{\partial \overline{f}}{\partial t}(0,1,0) = \frac{\partial \overline{f}}{\partial x}(0,1,0) = \frac{\partial \overline{f}}{\partial y}(0,1,0) = 0,$$

and

$$\frac{\partial \overline{f}}{\partial t}(0,0,1) = \frac{\partial \overline{f}}{\partial x}(0,0,1) = \frac{\partial \overline{f}}{\partial y}(0,0,1) = 0.$$

This proves that the two points at infinity p, q are singular. □

Ex. 10.13 *Suppose that the characteristic of F is not 2, and consider the curve defined by $ax^2 + bxy + cy^2 = 1$, where $a, b, c \in F^*$. If $b^2 - 4ac \in F^2$, show that there are one or two points at infinity depending on whether $b^2 - 4ac$ is zero. If $b^2 - 4ac = 0$, show that the point at infinity is singular.*

Proof. Let $\mathscr{C}$ be the curve defined by $f(x, y) = ax^2 + bxy + cy^2 - 1$. The homogeneous equation of the projective closure $\overline{\mathscr{C}}$ of $\mathscr{C}$ is

$$\overline{f}(t, x, y) = ax^2 + bxy + cy^2 - t^2.$$

The points $[0, u, v]$ at infinity are given by the equation

$$au^2 + buv + cv^2 = 0.$$

Assume that $\Delta = b^2 - 4ac = \delta^2 \in F^2$. Since $a \neq 0$,

$$\begin{aligned}
au^2 + buv + cv^2 &= a\left[\left(u + \frac{b}{2a}v\right)^2 - \frac{b^2 - 4ac}{4a^2}v^2\right] \\
&= a\left[\left(u + \frac{b}{2a}v\right)^2 - \frac{\delta^2}{4a^2}v^2\right] \\
&= a\left(u - \frac{-b+\delta}{2a}v\right)\left(u - \frac{-b-\delta}{2a}v\right) \\
&= a(u - \alpha v)(u - \beta v),
\end{aligned}$$

where $\alpha = \frac{-b+\delta}{2a}, \beta = \frac{-b-\delta}{2a}$ are the two roots of $aX^2 + bX + c$.

Therefore the points at infinity are $p = [0, \alpha, 1]$ and $q = [0, \beta, 1]$.

- If $b^2 - 4ac \neq 0$ (hyperbolic case), then $\alpha \neq \beta$ and $p \neq q$, so that $\mathscr{C}$ has two points at infinity.

- If $b^2 - 4ac = 0$ (parabolic case), then $\alpha = \beta$, and $\mathscr{C}$ has one (double) point at infinity $r = [0, \alpha, 1,]$, where $\alpha = -\frac{b}{2a}$ is the root of multiplicity 2 of $aX^2 + bX + c$. Thus $r = [0, -b, 2a]$.

Since

$$\frac{\partial \overline{f}}{\partial t}(t,x,y) = -2t, \qquad \frac{\partial \overline{f}}{\partial x}(t,x,y) = 2ax + by, \qquad \frac{\partial \overline{f}}{\partial y}(t,x,y) = bx + 2cy,$$

then

$$\frac{\partial \overline{f}}{\partial t}(0,-b,2a) = 0, \qquad \frac{\partial \overline{f}}{\partial x}(0,-b,2a) = -2ab+2ab = 0, \qquad \frac{\partial \overline{f}}{\partial y}(0,-b,2a) = -(b^2-4ac) = 0.$$

This shows that the point at infinity $r = [0,-b,2a]$ is singular.

$\square$

Ex. 10.14 *Consider the curve defined by* $y^2 = x^3+ax+b$. *Show that it has no singular points (finite or infinite) if* $4a^3 + 27b^2 \neq 0$.

Proof. Let $\mathscr{C}$ be the curve defined by $f(x,y) = y^2 - x^3 - ax - b$. The homogeneous equation of the projective closure $\overline{\mathscr{C}}$ of $\mathscr{C}$ is

$$\overline{f}(t,x,y) = y^2t - x^3 - axt^2 - bt^3.$$

The only point at infinity is given by $t = 0, -x^3 = 0$, thus is the point $p = [0,0,1]$. Since

$$\frac{\partial \overline{f}}{\partial t}(t,x,y) = y^2 - 2axt - 3bt^2, \qquad \frac{\partial \overline{f}}{\partial x}(t,x,y) = -3x^2 - at^2, \qquad \frac{\partial \overline{f}}{\partial y}(t,x,y) = 2yt,$$

then $\frac{\partial \overline{f}}{\partial t}(0,0,1) = 1$, thus the point at infinity p is not singular.

For some other points $a = (u,v)$ on $\overline{C}$ not at infinity, it is sufficient by Exercise 10 to verify $(\partial f/\partial x(u,v), \partial f/\partial y(u,v)) \neq (0,0)$. Since

$$\frac{\partial f}{\partial x}(u,v) = -3u^2 - a, \qquad \frac{\partial f}{\partial y}(u,v) = 2v,$$

a is singular if

$$\begin{cases} v^2 & = u^3 + au + b, \\ -3u^2 - a & = 0, \\ 2v & = 0. \end{cases}$$

Therefore

$$\begin{cases} 0 & = u^3 + au + b, \\ -\frac{a}{3} & = u^2, \end{cases}$$

If $a = 0$, then $u = v = 0$, thus $b = 0$, so that $4a^3 + 27b^2 = 0$.

If $a \neq 0$, we eliminate u between these two equations to obtain,

$$0 = u(u^2 + a) + b = \frac{2}{3}au + b,$$

thus $u = -\frac{3b}{2a}$, and $u^2 = \frac{9b^2}{4a^2} = -\frac{a}{3}$, which gives $4a^3 + 27b^2 = 0$. To conclude, if $4a^4 + 27b^2 \neq 0$, then the curve defined by $y^2 = x^3 + ax + b$ has no singular points, finite or infinite. $\square$