# 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 $\sum_{i=0}^{s-1} g_i(a_1, \ldots, a_{n-1})x_n^i$ 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 $\psi$ 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 there 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 $\psi$ 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 $\psi$ is surjective.

To conclude, $\psi$ 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 $\psi$ 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 $(a_0, \ldots, a_n) = (0, \ldots, 0)$, 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 doesn't depend on the choice of the projective point representative.

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 $\chi$ 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 $\varphi$ 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 $\chi$ is surjective.

To conclude, $\chi$ 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

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

- Suppose first that every point $[u_0, u_1, u_2]$ of $\mathscr{C} \cap l$ is such that $u_1 \neq 0$.

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 $\lambda_1, \ldots, \lambda_k$, where $k \leq n$. In this case, $u_2 = \lambda_i u_1$ and $u_0 = \alpha u_1 + \beta u_2 = u_1(\alpha + \beta\lambda_i)$, therefore

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

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

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

- Now suppose that some point $[u_0, u_1, u_2] \in \mathscr{C} \cap l$ satisfies $u_1 = 0$. Then $[u_0, u_1, u_2] = [\beta u_2, 0, u_2] = [\beta, 0, 1]$. There is exactly one point on $\mathscr{C} \cap l$ with $u_1 = 0$.

By the previous computation, the other points $[u_0, u_1, u_2] \in \mathscr{C} \cap l$, such that $u_1 \neq 0$, satisfy

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

Where $P(x) = f(\alpha + \beta x, 1, x)$

In this case, we prove that $\deg(P) \leq n - 1$.

Since $f$ is an homogeneous polynomial, with $\deg(f) = n$, we can write

$$f(x, y, z) = \sum_{(i,j)\in [\![0,n]\!]^2, i+j\leq n} a_{i,j}\, x^i y^j z^{n-i-j}.$$

In the present case, $[\beta, 0, 1]$ is on the curve $\mathscr{C}$, thus

$$\sum_{i=0}^{n} a_{i,0}\beta^i = 0.$$

Moreover,

$$\begin{aligned} P(x) &= f(\alpha + \beta x, 1, x) \\ &= \sum_{(i,j)\in [\![0,n]\!]^2, i+j\leq n} a_{i,j}\,(\alpha+\beta x)^i x^{n-i-j} \\ &= \sum_{(i,k)\in [\![0,n]\!]^2} a_{i,k-i}(\alpha+\beta x)^i x^{n-k} \qquad\qquad (k = i+j). \end{aligned}$$

If $j > 0$, then $\deg((\alpha+\beta x)^i x^{n-i-j}) < n$. Therefore the coefficient of $x^n$ in $P(x)$ is $\sum_{i=0}^{n} a_{i,0}\beta^i = 0$, thus $\deg(P) \leq n-1$. If $P \neq 0$, then $P$ has at most $n-1$ roots, and so $\mathscr{C}$ has at most $n-1$ points $[u_0, u_2, u_2]$ such that $u_1 \neq 0$ on $l$. With the unique point $[\beta, 0, 1]$ such that $u_1 = 0$, we obtain at most $n$ points in $\mathscr{C} \cap l$.

In both cases, if $|\mathscr{C} \cap l| > n$, then $P(x) = f(\alpha + \beta x, 1, x) = 0$. We show that this implies that $l \subset \mathscr{C}$.

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 $[v_0, v_1, v_2] = [\beta, 0, 1]$. Consider the reciprocal polynomial $Q(x) = x^n P\left(\frac{1}{x}\right)$ of $P(x)$. Then

$$\begin{aligned} Q(x) &= x^n \sum_{(i,k)\in [\![0,n]\!]^2} a_{i,k-i}\left(\alpha + \beta\frac{1}{x}\right)^i \frac{1}{x^{n-k}} \\ &= \sum_{(i,k)\in [\![0,n]\!]^2} a_{i,k-i}\,(\alpha x+\beta)^i\, x^{n-k}. \end{aligned}$$

If $P = 0$ ,then $Q = 0$, and

$$f(\beta, 0, 1) = \sum_{i=0}^{n} a_{i,0}\beta^i = Q(0) = 0.$$

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.

$\square$

**Second proof** (with same beginning.)

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

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

Consider the polynomial $g(x, y) = f(\alpha x + \beta y, x, y)$. For all $\lambda \in F$, $g(\lambda x, \lambda y) = f(\lambda(\alpha x+\beta y), \lambda x, \lambda y) = \lambda^n g(x, y)$, thus $g$ is homogeneous of degree $n$. A point $[u_0, u_1, u_2]$ of $l$ is on $\mathscr{C}$ if and only if $g(u_1, u_2) = 0$.

Suppose that $|\mathscr{C} \cap l| = m$, and write $[u_0^{(1)}, u_1^{(1)}, u_2^{(1)}], \ldots, [u_0^{(m)}, u_1^{(m)}, u_2^{(m)}]$ the $m$ distinct points of $\mathscr{C} \cap l$. Then $1 \leq i < j \leq m \Rightarrow (u_1^{(i)}, u_2^{(i)}) \not\sim (u_1^{(j)}, u_2^{(j)})$ : the $m$ pairs $[u_1^{(i)}, u_2^{i}]$ are distinct, since $u_0^{(i)} = \alpha u_1^{(i)} + \beta u_2^{(i)}$.

Then $g(u_1^{(1)}, u_2^{(1)}) = 0$, where $u_1, u_2$ cannot be 0 simultaneously . We show first that $g(x, y) = (u_2^{(1)}x - u_1^{(1)}y)h_1(x, y)$, where $h_1 \in F[x, y]$ is a homogeneous polynomial.

If $u_2^{(1)} \neq 0$, then $g\left(\frac{u_1^{(1)}}{u_2^{(1)}}, 1\right) = 0$. Therefore $\frac{u_1^{(1)}}{u_2^{(1)}}$ is a root of the polynomial $g(t, 1) \in F[t]$, thus $g(t, 1) = \left(t - \frac{u_1^{(1)}}{u_2^{(1)}}\right) h(t)$, where $h(t) \in F[t]$.

Then

$$\begin{aligned}
g(x, y) = y^n g\left(\frac{x}{y}, 1\right) &= y^n \left(\frac{x}{y} - \frac{u_1^{(1)}}{u_2^{(1)}}\right) h\left(\frac{x}{y}\right)\\
&= (u_2^{(1)}x - u_1^{(1)}y)h_1(x, y),
\end{aligned}$$

where $h_1(x, y) = \frac{1}{u_1^{(1)}}y^{n-1}h\left(\frac{x}{y}\right)$ is homogeneous of degree $n - 1$. Same proof if $u_1^{(1)} \neq 0$. Since $u_2^{(1)}u_1^{(2)} - u_1^{(1)}u_2^{(2)} \neq 0$, then $h_1(u_1^{(2}, u_2^{(2)}) = 0$, and we can continue we $h_1$ in place of $g$. By induction

$$g(x, y) = (u_2^{(1)}x - u_1^{(1)}y)(u_2^{(2)}x - u_1^{(2)}y) \cdots (u_2^{(m)}x - u_1^{(m)}y)h_m(x, y), \qquad h_m(x, y) \in F[x, y].$$

This equality shows that either $g(x, y) = 0$, or $n = \deg(g) \geq m$. This proves that if $m = |\mathscr{C} \cap l| > n$, then $g(x, y) = 0$. In this case, every point $[u_0, u_1, u_2] \in l$ satisfies $f(\alpha u_1 + \beta u_2, u_1, u_2) = g(u_1, u_2) = 0$, thus $l \subset \mathscr{C}$.

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

$$M \in \mathrm{SL}_n(F) \iff \sum_{\sigma\in S_n} \mathrm{sgn}(\sigma) a_{\sigma(1)1}\cdots a_{\sigma(n)n} - 1 = 0.$$

if $f(x_{1,1},\ldots,x_{n,n}) = \sum_{\sigma\in S_n} \mathrm{sgn}(\sigma) x_{\sigma(1)1}\cdots x_{\sigma(n)n} - 1$, 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

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

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

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

∎

**Ex. 10.7** *Let $f \in F[x_0,\ldots,x_n]$. One can define the partial derivatives $\partial f/\partial x_0,\ldots,\partial f/\partial x_n$ 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

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

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 $f \in F[x_0,\ldots,x_n]$ 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 $i = 1, \ldots, n$, then $mf(\overline{a}) = \sum_{i=1}^{n} x_i \frac{\partial f}{\partial x_i}(\overline{a}) = 0$. 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 $f(x_0, \ldots, x_n) = a_0 x_0^m + a_1 x_1^m + \cdots + a_n x_n^m$.

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 $a = [u_0, \ldots, u_n] \in V$ is a singular point,

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

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 $[u_0, \ldots, u_n]$ 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 $f \in F[x_1, x_2, \ldots, x_n]$, 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 $i = 1, 2, \ldots, n$.*

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

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

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

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

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

  Since $\overline{a}$ is singular,

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

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

- 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

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

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

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

if $a$ is singular, then

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

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. □

**Ex. 10.15** *Let $\mathbb{Q}$ be the field of rational numbers and $p$ a prime. Show that the form $x_0^{n+1} + px_1^{n+1} + p^2x_2^{n+1} + \cdots + p^nx_n^{n+1}$ has no zeros in $P^n(\mathbb{Q})$. (Hint: If $\overline{a}$ is a zero, one can assume that the components of $a$ are integers and that they are not all divisible by $p$.)*

*Proof.* Write $f(x_0,\ldots,x_n) = x_0^{n+1} + px_1^{n+1} + p^2x_2^{n+1} + \cdots + p^nx_n^{n+1}$.

Reasoning by contradiction, suppose that $\overline{a} = [\alpha_0,\ldots,\alpha_n]$ is a zero of $f$, where $\alpha_i \in \mathbb{Q}$ for $i = 0,\ldots,n$. Using a common denominator $c$ for these rational numbers, we can write

$$\begin{aligned} \overline{a} &= [\alpha_0,\ldots,\alpha_n] \\ &= \left[\frac{b_0}{c},\ldots,\frac{b_n}{c}\right] \qquad (b_i \in \mathbb{Z}) \\ &= \left[d\frac{a_0}{c},\ldots,d\frac{a_n}{c}\right] \\ &= [a_0,\ldots,a_n], \end{aligned}$$

where $d = b_0 \wedge \cdots \wedge b_n$ is the gcd of the $b_i$, so that the $a_i \in \mathbb{Z}$ satisfy $a_0 \wedge \cdots \wedge a_n = 1$.

Then

$$a_0^{n+1} + pa_1^{n+1} + p^2 a_2^{n+1} + \cdots + p^n a_n^{n+1} = 0,$$

where the integers $a_i$ are not all divisible by $p$.

To obtain a contradiction, we will show that all the $a_i$ are divisible by $p$.

$p \mid -pa_1^{n+1} - p^2 a_2^{n+1} + \cdots - p^n a_n^{n+1} = a_0^{n+1}$, thus $p \mid a_0$.

Reasoning by induction, suppose that $p$ divides $a_0, \ldots, a_k$, where $k < n$. Then $p^{n+1} \mid a_0^{n+1} + pa_1^{n+1} + p^2 a_2^{n+1} + \cdots + p^k a_k^{n+1}$, therefore

$$p^{n+1} \mid p^{k+1} a_{k+1}^{n+1} + p^{k+2} a_{k+2}^{n+1} + \cdots + p^n a_n^{n+1} = p^{k+1}(a_{k+1}^{n+1} + pa_{k+2}^{n+1} + \cdots + p^{n-k-1} a_n^{n+1}).$$

Since $n > k$, $p \mid a_{k+1}^{n+1} + pa_{k+2}^{n+1} + \cdots + p^{n-k-1} a_n^{n+1}$, therefore $p \mid a_{k+1}^{n+1}$, thus $p \mid a_{k+1}$.

The induction is done. This proves that $p \mid a_0, \ldots, p \mid a_n$. This is a contradiction, since the $a_i$ are not all divisible by $p$. So the form $x_0^{n+1} + px_1^{n+1} + p^2 x_2^{n+1} + \cdots + p^n x_n^{n+1}$ has no zeros in $P_n(\mathbb{Q})$. $\square$

**Ex. 10.16** *Show by explicit calculation that every cubic form in two variables over $\mathbb{Z}/2\mathbb{Z}$ has a non trivial zero.*

Note : this assertion seems false (or I don't understood the sentence).

*Proof.* We can write a cubic form on $P_1(\mathbb{F}_2)$ under the form

$$f(x_0, x_1) = ax_0^3 + bx_0^2 x_1 + cx_0 x_1^2 + dx_1^3, \qquad a, b, c, d \in \mathbb{F}_2.$$

Thus there are 15 such cubic forms.

This small Sage program computes the set of non trivial solutions for each of these forms

```
F2 = GF(2)
R.<x0,x1>= F2[]
l = [a*x0^3 + b * x0^2 * x1 + c * x0 * x1^2 + d * x1^3
      for a in F2 for b in F2 for c in F2 for d in F2
      if not [a,b,c,d] == [0,0,0,0]]
l
```

$[x_1^3, x_0x_1^2, x_0x_1^2 + x_1^3, x_0^2x_1, x_0^2x_1 + x_1^3, x_0^2x_1 + x_0x_1^2, x_0^2x_1 + x_0x_1^2 + x_1^3, x_0^3, x_0^3 + x_1^3, x_0^3 + x_0x_1^2, x_0^3 + x_0x_1^2 + x_1^3, x_0^3 + x_0^2x_1, x_0^3 + x_0^2x_1 + x_1^3, x_0^3 + x_0^2x_1 + x_0x_1^2, x_0^3 + x_0^2x_1 + x_0x_1^2 + x_1^3]$

```
for f in l:
    S = []
    for x in F2:
        for y in F2:
            if [x,y] != [0,0] and f.subs(x0=x,x1=y) == 0:
                S.append([x,y])
    print f,  ' : ', S

x1^3   :  [[1, 0]]
x0*x1^2   :  [[0, 1], [1, 0]]
x0*x1^2 + x1^3   :  [[1, 0], [1, 1]]
x0^2*x1   :  [[0, 1], [1, 0]]
```

```
x0^2*x1 + x1^3   :  [[1, 0], [1, 1]]
x0^2*x1 + x0*x1^2   :  [[0, 1], [1, 0], [1, 1]]
x0^2*x1 + x0*x1^2 + x1^3   :  [[1, 0]]
x0^3   :  [[0, 1]]
x0^3 + x1^3   :  [[1, 1]]
x0^3 + x0*x1^2   :  [[0, 1], [1, 1]]
x0^3 + x0*x1^2 + x1^3   :  []
x0^3 + x0^2*x1   :  [[0, 1], [1, 1]]
x0^3 + x0^2*x1 + x1^3   :  []
x0^3 + x0^2*x1 + x0*x1^2   :  [[0, 1]]
x0^3 + x0^2*x1 + x0*x1^2 + x1^3   :  [[1, 1]]
```

This shows that two cubics forms have no non trivial solutions. We verify this for the form $x_0^3 + x_0x_1^2 + x_1^3$ :

| $x_0$ | $x_1$ | $x_0^3 + x_0x_1^2 + x_1^3$ |
|---|---|---|
| 0 | 1 | 1 |
| 1 | 0 | 1 |
| 1 | 1 | 1 |

So the sentence is false.

With three variables $x_0, x_1, x_2$, there are 1023 cubics forms. A similar program gives among them the form

$$f(x_0, x_1, x_2) = x_0^3 + x_0x_1^2 + x_1^3 + x_0x_1x_2 + x_0x_2^2 + x_1x_2^2 + x_2^2,$$

which has no non trivial zero:

| $x_0$ | $x_1$ | $x_2$ | $f(x_0, x_1, x_2)$ |
|---|---|---|---|
| 0 | 0 | 1 | 1 |
| 0 | 1 | 0 | 1 |
| 0 | 1 | 1 | 1 |
| 1 | 0 | 0 | 1 |
| 1 | 0 | 1 | 1 |
| 1 | 1 | 0 | 1 |
| 1 | 1 | 1 | 1 |

The Chevalley's Theorem shows that with 4 (or more) variables $x_0, x_1, x_2, x_3$, every cubic form has non trivial solutions. $\square$

**Ex. 10.17** *Show that for each $m > 0$ and finite field $F_q$ there is a form of degree $m$ in $m$ variables with no nontrivial zero. [Hint: Let $\omega_1, \omega_2, \ldots, \omega_m$ be a basis for $F_{q^m}$ over $F_q$ and show that $f(x_1, x_2, \ldots, x_m) = \prod_{i=0}^{m-1}(\omega_1^{q^i}x_1 + \cdots + \omega_m^{q^i}x_m)$ has the required properties.]*

*Proof.* Let $\omega_1, \omega_2, \ldots, \omega_m$ be a basis for $F_{q^m}$ over $F_q$.

Consider

$$f(x_1, \ldots, x_m) = \prod_{i=0}^{m-1}(\omega_1^{q^i}x_1 + \cdots + \omega_m^{q^i}x_m).$$

Then $f$ is a form of degree $m$ in $m$ variables.

By definition, $f \in \mathbb{F}_{q^m}(x_1, \dots, x_m)$. We show first that $f \in \mathbb{F}_q[x_1, \dots, x_m]$.

Let $f$ be the Frobenius automorphism on $\mathbb{F}_{q^m}$, defined by

$$F \left\{ \begin{array}{ccc} \mathbb{F}_{q^m} & \to & \mathbb{F}_{q^m} \\ \alpha & \mapsto & \alpha^q. \end{array} \right.$$

By Corollary 1 of Proposition 7.1.1, for every $\alpha \in \mathbb{F}_{q^m}$, $\alpha \in \mathbb{F}_q$ if and only if $F(\alpha) = \alpha$. If $p = \sum_{i=0}^d a_{i_1,\dots,i_m} x_1^{i_1} \cdots x_m^{i_m} \in \mathbb{F}_{q^m}[x_1, \dots, x_m]$, define $F \cdot p = \sum_{i=0}^d F(a_{i_1,\dots,i_m}) x_1^{i_1} \cdots x_m^{i_m}$. Then $F \cdot p \in \mathbb{F}_{q^m}[x] \iff F \cdot p = p$ and $F \cdot (pq) = (F \cdot p)(F \cdot q)$ for all $p, q \in \mathbb{F}_{q^m}[x_1, \dots, x_m]$.

Then, using this last property,

$$\begin{aligned}
F \cdot f &= \prod_{i=0}^{m-1} F \cdot (\omega_1^{q^i} x_1 + \cdots + \omega_m^{q^i} x_m) \\
&= \prod_{i=0}^{m-1} (\omega_1^{q^{i+1}} x_1 + \cdots + \omega_m^{q^{i+1}} x_m) \\
&= \prod_{j=1}^{m} (\omega_1^{q^j} x_1 + \cdots + \omega_m^{q^j} x_m) \qquad (j = i+1) \\
&= \prod_{j=0}^{m-1} (\omega_1^{q^j} x_1 + \cdots + \omega_m^{q^j} x_m) \qquad (\text{since } \omega_k^{q^m} = \omega_k = \omega_k^{q^0},\ k = 1, \dots, m) \\
&= f.
\end{aligned}$$

Therefore $f \in \mathbb{F}_q[x_1, \dots, x_m]$.

Now we prove that $f$ has no non trivial zero $\overline{a} = (\alpha_1, \dots, \alpha_m) \in \mathbb{F}_q^m \setminus \{(0, \dots, 0)\}$. If $f$ had such a zero $(\alpha_1, \dots, \alpha_m) \in \mathbb{F}_q^m$, then

$$\prod_{i=0}^{m-1} (\omega_1^{q^i} \alpha_1 + \cdots + \omega_m^{q^i} \alpha_m) = 0, \qquad \alpha_1, \dots, \alpha_m \in \mathbb{F}_q.$$

Then for some $i \in [\![0, m-1]\!]$,

$$\omega_1^{q^i} \alpha_1 + \cdots + \omega_m^{q^i} \alpha_m = 0.$$

Applying $F^{m-i}$ to this equality, and using $F(\alpha_i) = \alpha_i$, we obtain

$$\omega_1^{q^m} \alpha_1 + \cdots + \omega_m^{q^m} \alpha_m = 0.$$

Since $\omega_i^{q^m} = \omega_i,\ i = 1, \dots, m$, this gives

$$\omega_1 \alpha_1 + \cdots + \omega_m \alpha_m = 0.$$

Since $\omega_1, \omega_2, \dots, \omega_m$ is a basis for $F_{q^m}$ over $F_q$, this proves

$$(\alpha_1, \dots, \alpha_m) = (0, \dots, 0).$$

So $f$ has no non trivial zero.

Note : this proves that we cannot extend the Chevalley's Theorem to the forms of degree $m$ in $m$ varibles. $\square$

**Ex. 10.18** *Let $g_1, g_2, \dots, g_m \in \mathbb{F}_q[x_1, x_2, \dots, x_n]$ be homogeneous polynomials of degree $d$ and assume that $n > md$. Prove that there is nontrivial common zero. [Hint: Let $f$ be as in Exercise 17 and consider the polynomial $f(g_1(x_1, \dots, x_n), \dots, g_m(x_1, \dots, x_m))$.]*

*Proof.* Consider the polynomial $h = f(g_1(x_1, \dots, x_n), \dots, g_m(x_1, \dots, x_m)) \in \mathbb{F}_q[x_1, \dots, x_m]$. Then $h$ is homogeneous of degree $md$. Since $n > md$, the Chevalley's Theorem (Corollary of Theorem 1) shows that there is a non trivial zero $\overline{a} = (\alpha_1, \dots, \alpha_m) \in \mathbb{F}_q^m \setminus \{(0, \dots, 0)\}$ of $h$, so that

$$f(g_1(\alpha_1, \dots, \alpha_n), \dots, g_m(\alpha_1, \dots, \alpha_m)) = 0, \qquad (\alpha_1, \dots, \alpha_m) \in \mathbb{F}_q^m \setminus \{(0, \dots, 0)\}.$$

Then

$$f(\beta_1, \dots, \beta_m) = 0, \qquad \text{where } \beta_i = g_1(\alpha_1, \dots, \alpha_n) \in \mathbb{F}_q.$$

Since $f$ has no trivial zero by Exercise 17, we obtain $\beta_1 = \cdots = \beta_m = 0$, that is

$$g_1(\alpha_1, \dots, \alpha_n) = \ldots = g_m(\alpha_1, \dots, \alpha_m) = 0, \qquad (\alpha_1, \dots, \alpha_m) \in \mathbb{F}_q^m \setminus \{(0, \dots, 0)\}.$$

This proves that here is nontrivial common zero for $g_1, \dots g_m$, if $n > md$. □

**Ex. 10.19** *Characterize those extensions $\mathbb{F}_{p^n}$ of $\mathbb{F}_p$ that are such that the trace is identically zero on $\mathbb{F}_p$.*

*Proof.* If $\alpha \in \mathbb{F}^p$, then $\alpha^p = \alpha$, thus $\alpha^{p^k} = \alpha$ for all exponents $k \geq 0$.

In the extension $\mathbb{F}_{p^n}$ of $\mathbb{F}_p$, for all $\alpha \in \mathbb{F}_p$,

$$\begin{aligned} \operatorname{tr}(\alpha) &= \alpha + \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{n-1}} \\ &= n\alpha. \end{aligned}$$

If the characteristic $p$ divides $n$, then $n = 0$ in $\mathbb{F}_{p^n}$, thus $\operatorname{tr}(\alpha) = 0$ for all $\alpha \in \mathbb{F}_p$.

Conversely, if $\operatorname{tr}(\alpha) = 0$ for all $\alpha \in \mathbb{F}_p$, then $\operatorname{tr}(1) = n \cdot 1 = 0$, thus the characteristic $p$ divides $n$.

The extensions $\mathbb{F}_{p^n}$ of $\mathbb{F}_p$ that are such that the trace is identically zero on $\mathbb{F}_p$ are those which satisfy $p \mid n$.

□

**Ex. 10.20** *Show that if $\alpha \in \mathbb{F}_q$ has trace zero, then $\alpha = \beta - \beta^p$ for some $\beta \in \mathbb{F}_q$.*

*Proof.* Here $q = p^n$. Consider first the map

$$\operatorname{tr} \left\{ \begin{array}{lll} \mathbb{F}_{p^n} & \to & \mathbb{F}_p \\ \alpha & \mapsto & \operatorname{tr}(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{n-1}} \end{array} \right.$$

This makes sense, since by Proposition 10.3.1(a), $\operatorname{tr}(\alpha) \in \mathbb{F}_p$ for all $\alpha \in \mathbb{F}_{p^n}$. Moreover, parts (b),(c) of this proposition show that tr is $\mathbb{F}_p$-linear, and by part (d) that tr is surjective (onto): $\operatorname{Im}(\operatorname{tr}) = \mathbb{F}_p$.

The rank theorem gives

$$\dim_{\mathbb{F}_p} \operatorname{Im}(\operatorname{tr}) = \dim_{\mathbb{F}_p} \mathbb{F}_{p^n} - \dim_{\mathbb{F}_p} \ker(\operatorname{tr}),$$

thus

$$\dim_{\mathbb{F}_p} \ker(\operatorname{tr}) = n - 1.$$

Consider now

$$T \left\{ \begin{array}{ccc} \mathbb{F}_{p^n} & \to & \mathbb{F}_{p^n} \\ \beta & \mapsto & \beta - \beta^p \end{array} \right.$$

$T$ is a $\mathbb{F}_p$-linear map: for $a, b \in \mathbb{F}^p$, and $\alpha, \beta \in \mathbb{F}_{p^n}$, using $a^p = a, b^p = b$,

$$T(a\alpha + b\gamma) = a\alpha + b\gamma - (a^p\alpha^p + b^p\beta^p) = a(\alpha - \alpha^p) + b(\beta - \beta^p) = aT(\alpha) + bT(\beta).$$

If $\gamma = T(\beta) = \beta - \beta^p$ is in $\mathrm{Im}(T)$, then

$$\begin{aligned} \mathrm{tr}(\gamma) &= \mathrm{tr}(\beta) - \mathrm{tr}(\beta^p) \\ &= \left(\beta + \beta^p + \beta^{p^2} + \cdots + \beta^{p^{n-1}}\right) - \left(\beta^p + \beta^{p^2} + \beta^{p^3} + \cdots + \beta^{p^n}\right) \\ &= \beta - \beta^{p^n} \\ &= 0. \end{aligned}$$

This proves that

$$\mathrm{Im}(T) \subset \ker(\mathrm{tr}).$$

Moreover,

$$\beta \in \ker(T) \iff \beta = \beta^p \iff \beta \in \mathbb{F}_p,$$

so that $\ker(T) = \mathbb{F}_p$.

Using newly the rank theorem on $T$, we obtain

$$\begin{aligned} \dim_{\mathbb{F}_p} \mathrm{Im}(T) &= \dim_{\mathbb{F}_p} \mathbb{F}_{p^n} - \dim_{\mathbb{F}_p} \ker(T) \\ &= n - 1. \end{aligned}$$

From $\mathrm{Im}(T) \subset \ker(\mathrm{tr})$, where $\dim_{\mathbb{F}_p} \mathrm{Im}(T) = \dim_{\mathbb{F}_p} \ker(\mathrm{tr}) = n-1$, we deduce

$$\mathrm{Im}(T) = \ker(\mathrm{tr}).$$

To conclude, if $\alpha \in \mathbb{F}_q$ has trace zero, then $\alpha \in \mathrm{Im}(T)$, i.e. $\alpha = \beta - \beta^p$ for some $\beta \in \mathbb{F}_q$. $\square$

**Ex. 10.21** *Let $\psi$ be a map from $\mathbb{F}_q$ to $\mathbb{C}^*$ such that $\psi(\alpha + \beta) = \psi(\alpha)\psi(\beta)$ for all $\alpha, \beta \in \mathbb{F}_q$. Show that there is a $\gamma \in \mathbb{F}_q$ such that $\psi(x) = \zeta^{\mathrm{tr}(\gamma x)}$ for all $x \in \mathbb{F}_q$, where $\zeta = 2i\pi/p$.*

*Proof.* Here $q = p^n$.

The map $\psi$ is a group homomorphism, from $(\mathbb{F}_q, +)$ to $(\mathbb{C}^*, \times)$, thus $\psi(0) = 1$, and $\psi(a\alpha) = \psi(\alpha)^a$, where $\alpha \in \mathbb{F}_q$ and $a \in \mathbb{Z}$.

Let $(\omega_1, \ldots, \omega_n)$ be a basis for $\mathbb{F}_{p^n}$ over $\mathbb{F}_p$. For each $k \in [\![1, n]\!]$, since the characteristic of $\mathbb{F}_q$ is $p$,

$$\psi(\omega_k)^p = \psi(p\omega_i) = \psi(0) = 1.$$

Thus $\psi(\omega_k)$ is a $p$-th root of unity, of the form

$$\psi(\omega_k) = \zeta^{c_k}, \quad c_k \in \{0, \ldots, p-1\}.$$

Since $\zeta^{c_k} = \zeta^{c_k + lp}$ $(l \in \mathbb{Z})$, we can give a sense to $\psi(\omega_k) = \zeta^{c_k} = \zeta^{[c_k]}$, where $[c_k] \in \mathbb{F}_p$ is the class of $c_k$ modulo $p$.

Consider the map

$$\varphi \left\{ \begin{array}{ccl} \mathbb{F}_q & \to & (\mathbb{F}_p)^n \\ \gamma & \mapsto & (\mathrm{tr}(\gamma\omega_1), \ldots, \mathrm{tr}(\gamma\omega_n)). \end{array} \right.$$

We will show that the linear map $\varphi$ is bijective.

If $\gamma \in \ker(\varphi)$, then $\mathrm{tr}(\gamma\omega_1) = \ldots, \mathrm{tr}(\gamma\omega_n) = 0$. If $y$ is any element in $\mathbb{F}_q$, then $y = b_1\omega_1 + \cdots + b_n\omega_n$, where $b_1, \ldots, b_n \in \mathbb{F}_p$. Then $\mathrm{tr}(\gamma y) = b_1\mathrm{tr}(\gamma\omega_1) + b_n\mathrm{tr}(\gamma\omega_n) = 0$, which gives

$$\forall y \in \mathbb{F}_q,\ \mathrm{tr}(\gamma y) = 0.$$

Reasoning by contradiction suppose that $\gamma \neq 0$. Since tr maps $\mathbb{F}_q$ onto $\mathbb{F}_p$( Proposition 10.3.1.(d)), there is some $\delta \in \mathbb{F}_q$ such that $\mathrm{tr}(\delta) = 1$. If $y = \delta\gamma^{-1}$, then $0 = \mathrm{tr}(\gamma y) = \mathrm{tr}(\delta) = 1$. This is a contradiction, so $\gamma = 0$, and this proves $\ker(\varphi) = \{0\}$.

Moreover $\dim_{\mathbb{F}_p}(\mathbb{F}_q) = \dim_{\mathbb{F}_p}(\mathbb{F}_p)^n = n$, thus $\varphi$ is a bijection.

Thus there exists $\gamma \in \mathbb{F}_q$ such that

$$\mathrm{tr}(\gamma\omega_k) = [c_k], \qquad k = 1, \ldots, n.$$

Then, if $x$ is any element in $\mathbb{F}_q$, we can write $x = a_1\omega_1 + \cdots + a_n\omega_n$, where $a_1, \ldots, a_k \in \mathbb{F}_p$. Since $\psi(\omega_k)$ is a $p$-th root of unity,

$$\begin{aligned} \psi(x) &= \psi(a_1\omega_1 + \cdots + a_n\omega_n) \\ &= \psi(\omega_1)^{a_1} \cdots \psi(\omega_n)^{a_n} \\ &= \zeta^{a_1\mathrm{tr}(\gamma\omega_1) + \cdots + a_n\mathrm{tr}(\gamma\omega_n)} \\ &= \zeta^{\mathrm{tr}(\gamma x)}. \end{aligned}$$

If $\psi$ is a group homomorphism from $\mathbb{F}_q$ to $\mathbb{C}^*$, then there is a $\gamma \in \mathbb{F}_q$ such that $\psi(x) = \zeta^{\mathrm{tr}(\gamma x)}$ for all $x \in \mathbb{F}_q$. □

**Ex. 10.22** *If $g_\alpha(\chi)$ is a Gauss sum on $F$, defined in section 3, show that*

*(a)* $g_\alpha(\chi) = \overline{\chi(\alpha)}g(\chi)$.

*(b)* $g(\chi^{-1}) = g(\overline{\chi}) = \chi(-1)\overline{g(\chi)}$.

*(c)* $|g_\alpha(\chi)| = q^{1/2}$.

*(d)* $g(\chi)g(\chi^{-1}) = \chi(-1)q$.

*Proof.* Here $\psi : \mathbb{F}_q \to \mathbb{C}$ is defined by $\psi(\alpha) = \zeta_p^{\mathrm{tr}(\alpha)}$, and the Gauss sum for a character $\chi$ of $\mathbb{F}_q$ by

$$g_\alpha(\chi) = \sum_{t \in \mathbb{F}_q} \chi(t)\psi(\alpha t) = \sum_{t \in \mathbb{F}_q} \chi(t)\zeta_p^{\mathrm{tr}(\alpha t)}.$$

First we generalize Proposition 8.1.2, with the same proof. If $\chi \neq \varepsilon$, there is an $a \in \mathbb{F}_q^*$ such that $\chi(a) \neq 1$. Then, if $T = \sum_{t \in \mathbb{F}_q} \chi(t)$, then

$$\chi(a)T = \sum_{t \in \mathbb{F}_q} \chi(a)\chi(t) = \sum_{t \in \mathbb{F}_q} \chi(at) = \sum_{s \in \mathbb{F}_q} \chi(s) = T.$$

Since $\chi(a)T = T$ and $\chi(a) \neq 1$, it follows that $T = 0$. This proves, for a non trivial character $\chi$,

$$g_0(\chi) = \sum_{t \in \mathbb{F}_q} \chi(t) = 0.$$

(a) If $\alpha \in \mathbb{F}_q^*$,

$$\begin{aligned}
\chi(\alpha) g_\alpha(\chi) &= \sum_{t\in\mathbb{F}_q} \chi(\alpha)\chi(t)\psi(\alpha t)\\
&= \sum_{t\in\mathbb{F}_q} \chi(\alpha t)\psi(\alpha t)\\
&= \sum_{s\in\mathbb{F}_q} \chi(s)\psi(s) \qquad (s=\alpha t)\\
&= g(\chi).
\end{aligned}$$

Since $|\chi(\alpha)|=1$, $\chi(\alpha)^{-1} = \overline{\chi(\alpha)}$, thus

$$g_\alpha(\chi) = \overline{\chi(\alpha)} g(\chi).$$

(b) Since $(-1)^2=1$, $(\chi(-1))^2=1$, thus $\chi(-1)=\pm 1$ is real, therefore $\overline{\chi(-1)} = \chi(-1)$. This gives

$$\begin{aligned}
\overline{g(\chi)} &= \sum_{t\in\mathbb{F}_q} \overline{\chi(t)}\zeta_p^{-\mathrm{tr}(t)}\\
&= \sum_{t\in\mathbb{F}_q} \overline{\chi(-1)\chi(-t)}\zeta_p^{-\mathrm{tr}(t)}\\
&= \chi(-1)\sum_{t\in\mathbb{F}_q} \overline{\chi(-t)}\zeta_p^{\mathrm{tr}(-t)}\\
&= \chi(-1)\sum_{s\in\mathbb{F}_q} \overline{\chi(s)}\zeta_p^{\mathrm{tr}(s)} \qquad (s=-t)\\
&= \chi(-1) g(\overline{\chi})
\end{aligned}$$

We have seen in part (a) that $\chi^{-1} = \overline{\chi}$. This gives

$$g(\chi^{-1}) = g(\overline{\chi}) = \chi(-1)\overline{g(\chi)}.$$

(c) Here we assume that $\chi \neq \varepsilon$. By part (a), $|g_\alpha(\chi)| = |g(\chi)|$, so it it sufficient to verify $|g(\chi)| = q^{1/2}$.

We evaluate the sum $S = \sum_{\alpha\in\mathbb{F}_q} g_a(\chi)\overline{g_a(\chi)}$ in two ways.

- We have proved in the introduction that $g_0(\chi)=0$. If $a\in\mathbb{F}_q^*$, then $g_a(\chi) = \chi(a^{-1})g(\chi)$, and $\overline{g_a(\chi)} = \overline{\chi(a^{-1})g(\chi)} = \chi(a)\overline{g(\chi)}$. It follows that

$$\begin{aligned}
S &= \sum_{a\in\mathbb{F}_q^*} \chi(a^{-1})g(\chi)\chi(a)\overline{g(\chi)}\\
&= \sum_{a\in\mathbb{F}_q^*} |g(\chi)|^2\\
&= (q-1)|g(\chi)|^2
\end{aligned}$$

- Furthermore

$$g_a(\chi)\overline{g_a(\chi)} = \sum_{x\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_q} \chi(x)\overline{\chi(y)}\psi(a(x-y)).$$

Therefore,

$$\begin{aligned} S &= \sum_{a\in\mathbb{F}_q}\sum_{x\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_q} \chi(x)\overline{\chi(y)}\psi(a(x-y)) \\ &= \sum_{x\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_q} \chi(x)\overline{\chi(y)} \left(\sum_{a\in\mathbb{F}_q} \psi(a(x-y))\right) \end{aligned}$$

By Proposition 10.3.3,

$$\sum_{a\in\mathbb{F}_q} \psi(a(x-y)) = q\delta(x,y)$$

Therefore,

$$\begin{aligned} S &= q\sum_{x\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_q} \chi(x)\overline{\chi(y)}\delta(x,y) \\ &= q\sum_{x\in\mathbb{F}_q} \chi(x)\overline{\chi(x)} \end{aligned}$$

Since $\chi(x)\overline{\chi(x)} = 1$ if $x \neq 0$, and $\chi(x)\overline{\chi(x)} = 0$ if $x = 0$, we obtain

$$S = q(q-1).$$

The comparison of these two results gives

$$(q-1)|g(\chi)|^2 = (q-1)q,$$

thus

$$|g_\alpha(\chi)| = |g(\chi)| = \sqrt{q}.$$

(d) Here $\chi \neq \varepsilon$. Then, by parts (b) and (c),

$$\begin{aligned} g(\chi)g(\chi^{-1}) &= \chi(-1)g(\chi)\overline{g(\chi)} \\ &= \chi(-1)|g(\chi)|^2 \\ &= \chi(-1)q. \end{aligned}$$

□

**Ex. 10.23** *Suppose that $f$ is a function mapping $F$ to $\mathbb{C}$. Define $\hat{f}(s) = (1/q)\sum_t f(t)\overline{\psi(st)}$ and prove that $f(t) = \sum_s \hat{f}(s)\psi(st)$. The last sum is called the finite Fourier series expansion of $f$.*

*Proof.* Using the proposition 10.3.3, we obtain, for all $t \in \mathbb{F}_q$,

$$\begin{aligned}
\sum_{s\in\mathbb{F}_q} \hat{f}(s)\psi(st) &= \frac{1}{q}\sum_{s\in\mathbb{F}_q}\left(\sum_{u\in\mathbb{F}_q} f(u)\overline{\psi(su)}\right)\psi(st)\\
&= \frac{1}{q}\sum_{u\in\mathbb{F}_q} f(u)\sum_{s\in\mathbb{F}_q}\psi(s(t-u))\\
&= \frac{1}{q}\sum_{u\in\mathbb{F}_q} f(u)q\delta(t,u)\\
&= f(t).
\end{aligned}$$

□

**Ex. 10.24** *In Exercise 23 take $f$ to be a non trivial character $\chi$ and show that $\hat{\chi}(s) = (1/q)g_{-s}(\chi)$.*

*Proof.* By definition,

$$\begin{aligned}
\hat{\chi}(s) &= \frac{1}{q}\sum_{t\in\mathbb{F}_q}\chi(t)\overline{\psi(st)}\\
&= \frac{1}{q}\sum_{t\in\mathbb{F}_q}\chi(t)\zeta_p(-\mathrm{tr}(st))\\
&= \frac{1}{q}\sum_{t\in\mathbb{F}_q}\chi(t)\zeta_p(\mathrm{tr}((-s)t))\\
&= \frac{1}{q}\,g_{-s}(\chi).
\end{aligned}$$

□