

Chapter 10

Ex. 10.1 If K is an infinite field and $f(x_1, x_2, \dots, x_n)$ 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 has 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

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

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

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

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

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

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

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

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

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

Consider

$$\psi \left\{ \begin{array}{ll} \bar{H} & \rightarrow P_{n-1}(F) \\ [0, x_1, \dots, x_n] & \mapsto [x_1, \dots, x_n] \end{array} \right.$$

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

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

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

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

where $(a_0, \dots, a_n) \neq (0, \dots, 0)$ (if $(a_0, \dots, a_n) = (0, \dots, 0)$, then $\overline{K} = P_n(F)$ is not a hyperplane). Note that, if $(x_0, \dots, x_n) \sim (y_0, \dots, y_n)$, there is $\lambda \in F^*$ such that $y_i = \lambda x_i$, $i = 0, \dots, n$, 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 of the choice of the representative of the projective point.

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

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

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

If $\chi([x_0, \dots, x_n]) = \chi([y_0, \dots, y_n])$, where $[x_0, \dots, x_n]$ and $[y_0, \dots, y_n]$ are in \overline{K} , then $[x_1, \dots, x_n] = [y_1, \dots, y_n]$, thus there is $\lambda \in F^*$ such that $(y_1, \dots, y_n) = \lambda(x_1, \dots, x_n)$. 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 $[x_0, \dots, x_n] = [y_0, \dots, y_n]$. So φ is injective.

At last, let $[x_1, \dots, x_n]$ 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 $[x_0, \dots, x_n] \in \overline{K}$, and $\chi([x_0, \dots, x_n]) = [x_1, \dots, x_n]$. 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 \mathcal{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

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

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

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 $p = [\beta, 0, 1] \in \mathcal{C} \cap l$.

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

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

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

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

Similarly, by exchanging the roles of u_1, u_2 , if $|\mathcal{C} \cap l| > n$, 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 $l \subset \mathcal{C}$.

To conclude, if $l \not\subset \mathcal{C}$, then $|l \cap \mathcal{C}| \leq n$: 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 $\text{SL}_n(F)$ be the subset of those matrices with determinant equal to one. Show that $\text{SL}_n(F)$ 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 $M = (a_{i,j})_{1 \leq i \leq n, 1 \leq j \leq n} \in M_n(F)$,

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

if $f(x_{1,1}, \dots, x_{n,n}) = \sum_{\sigma \in S_n} \text{sgn}(\sigma) x_{\sigma(1)1} \cdots x_{\sigma(n)n}$, then $M \in \text{SL}_n(F)$ if and only if $f(a_{1,1}, \dots, a_{n,n}) = 0$,

where f is a non zero polynomial, since it contains the non zero term $x_{1,1} \cdots x_{n,n}$. Therefore $\text{SL}_n(F)$ is an hypersurface of $M_n(F)$.

Since a matrix $M \in M_n(F)$ is invertible if and only if its columns (C_1, \dots, C_n) is a basis of F^n , the number of matrices in $\text{GL}_n(F)$ 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, \dots, C_k are chosen, we take C_{k+1} between the $q^n - q^k$ vectors $v \notin \langle C_1, \dots, C_k \rangle$. At last, we choose $C_n \notin \langle C_1, \dots, C_{n-1} \rangle$. This gives

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

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

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

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

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

□

Ex. 10.7 Let $f \in F[x_0, \dots, x_n]$. 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 $a_1 + \dots + a_n = m = \deg(f)$, then

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

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

Ex. 10.9 If m is prime to the characteristic of F , show that the hypersurface defined by $a_0 x_0^m + a_1 x_1^m + \dots + a_n x_n^m$ 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 $f(x_0, \dots, x_n) = a_0 x_0^m + a_1 x_1^m + \dots + a_n x_n^m$.

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,

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

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 $\bar{a} = [1, u_1, \dots, u_n] \in \bar{F}$ is singular, and let

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

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

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

Since \bar{a} is singular,

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

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

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

which proves that \bar{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

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

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

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

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

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

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

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

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

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

Therefore

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

and

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

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

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

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

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 \mathcal{C} has two points at infinity.
- If $b^2 - 4ac = 0$ (parabolic case), then $\alpha = \beta$, and \mathcal{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

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

then

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

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

□

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

$$\bar{f}(t, x, y) = y^2t - x^3 - ax t^2 - b t^3.$$

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

$$\frac{\partial \bar{f}}{\partial t}(t, x, y) = y^2 - 2ax t - 3b t^2, \quad \frac{\partial \bar{f}}{\partial x}(t, x, y) = -3x^2 - a t^2, \quad \frac{\partial \bar{f}}{\partial y}(t, x, y) = 2y t,$$

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

For some other points $a = (u, v)$ on \bar{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

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

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 $4a^3 + 27b^2 \neq 0$, 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 $x_0^{n+1} + px_1^{n+1} + p^2x_2^{n+1} + \dots + p^nx_n^{n+1}$ has no zeros in $P^n(\mathbb{Q})$. (Hint: If \bar{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 $f(x_0, \dots, x_n) = x_0^{n+1} + px_1^{n+1} + p^2x_2^{n+1} + \dots + p^nx_n^{n+1}$.

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

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

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

Then

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

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 .

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

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

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

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

The induction is done. This proves that $p \mid a_0, \dots, p \mid a_n$. This is a contradiction, since the a_i are not all divisible by p . So the form $x_0^{n+1} + px_1^{n+1} + p^2x_2^{n+1} + \dots + p^nx_n^{n+1}$ 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

$$f(x_0, x_1) = ax_0^3 + bx_0^2x_1 + cx_0x_1^2 + dx_1^3, \quad a, b, c, d \in \mathbb{F}_2.$$

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]]
1
```

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

```

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 $\omega_1, \omega_2, \dots, \omega_m$ be a basis for F_{q^m} over F_q and show that $f(x_1, x_2, \dots, x_m) = \prod_{i=0}^{m-1} (\omega_1^{q^i} x_1 + \dots + \omega_m^{q^i} x_m)$ has the required properties.]

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

Consider

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

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

$$F \begin{cases} \mathbb{F}_{q^m} & \rightarrow \mathbb{F}_{q^m} \\ \alpha & \mapsto \alpha^q. \end{cases}$$

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 $p = \sum_{i=0}^d a_{i_1, \dots, i_m} x_1^{i_1} \dots x_m^{i_m} \in \mathbb{F}_{q^m}[x_1, \dots, x_m]$, define $F \cdot p = \sum_{i=0}^d F(a_{i_1, \dots, i_m}) x_1^{i_1} \dots x_m^{i_m}$. 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,

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

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

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

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

Then for some $i \in \llbracket 0, m-1 \rrbracket$,

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

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

$$\omega_1^{q^m} \alpha_1 + \dots + \omega_m^{q^m} \alpha_m.$$

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

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

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 variables. \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 $f(g_1(x_1, \dots, x_n), \dots, g_m(x_1, \dots, x_n))$.]

Proof. Consider the polynomial $h = f(g_1(x_1, \dots, x_n), \dots, g_m(x_1, \dots, x_n)) \in \mathbb{F}_q[x_1, \dots, x_n]$. 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 $\bar{a} = (\alpha_1, \dots, \alpha_m) \in \mathbb{F}_q^m \setminus \{(0, \dots, 0)\}$ of h , so that

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

Then

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

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

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

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

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 $\alpha \in \mathbb{F}_p$,

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

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

Conversely, if $\text{tr}(\alpha) = 0$ for all $\alpha \in \mathbb{F}_p$, then $\text{tr}(1) = n \cdot 1 = 0$, 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 $p \mid n$. \square

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

$$\text{tr} \begin{cases} \mathbb{F}_{p^n} & \rightarrow \mathbb{F}_p \\ \alpha & \mapsto \text{tr}(\alpha) = \alpha + \alpha^p + \alpha^{p^2} + \cdots + \alpha^{p^{n-1}} \end{cases}$$

This makes sense, since by Proposition 10.3.1(a), $\text{tr}(\alpha) \in \mathbb{F}_p$ 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): $\text{Im}(\text{tr}) = \mathbb{F}_p$.

The rank theorem gives

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

thus

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

Consider now

$$T \begin{cases} \mathbb{F}_{p^n} & \rightarrow \mathbb{F}_{p^n} \\ \beta & \mapsto \beta - \beta^p \end{cases}$$

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

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

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

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

This proves that

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

Moreover,

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

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

Using anew the rank theorem on T , we obtain

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

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

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

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

Ex. 10.21 Let ψ 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 $\psi(x) = \zeta^{\text{tr}(\gamma x)}$ for all $x \in \mathbb{F}_q$, where $\zeta = 2i\pi/p$.

Proof. Here $q = p^n$.

The map ψ 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 $(\omega_1, \dots, \omega_n)$ be a basis for \mathbb{F}_{p^n} over \mathbb{F}_p . For each $k \in \llbracket 1, n \rrbracket$, since the characteristic of \mathbb{F}_q is p ,

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

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

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

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

$$\varphi \begin{cases} \mathbb{F}_q & \rightarrow (\mathbb{F}_p)^n \\ \gamma & \mapsto (\text{tr}(\gamma\omega_1), \dots, \text{tr}(\gamma\omega_n)). \end{cases}$$

We will show that the linear map φ is bijective.

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

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

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 $\text{tr}(\delta) = 1$. If $y = \delta\gamma^{-1}$, then $0 = \text{tr}(\gamma y) = \text{tr}(\delta) = 1$. This is a contradiction, so $y = 0$, and this proves $\ker(\varphi) = \{0\}$.

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

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

$$\text{tr}(\gamma\omega_k) = [c_k], \quad k = 1, \dots, n.$$

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

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

□

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

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

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

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

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

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

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

First we generalize Proposition 8.1.2, with the same proof. If $\chi \neq \varepsilon$, there 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 χ ,

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

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

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

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

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

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

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

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

We evaluate the sum $S = \sum_{\alpha \in \mathbb{F}_q} g_\alpha(\chi) \overline{g_\alpha(\chi)}$ 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),

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

□