

Chapter 11

Ex. 11.1 Suppose that we may write the power series $1 + a_1u + a_2u^2 + \cdots$ as the quotient of two polynomials $P(u)/Q(u)$. Show that we may assume that $P(0) = Q(0) = 1$.

Proof. Here $f(u) = 1 + a_1u + a_2u^2 + \cdots \in \mathbb{C}[[u]]$ is a formal series in the variable u .

We suppose that $f(u) = P(u)/Q(u)$, where we may assume, after simplification, that the two polynomials are relatively prime. Then $P(1)/Q(1) = 1$. Write $c = P(1) = Q(1) \in F$.

If $c = 0$, then $u \mid P(u)$ and $u \mid Q(u)$. This is impossible since $P \wedge Q = 1$. So $c \neq 0$.

Define $P_1(u) = (1/c)P(u)$, $Q_1(u) = (1/c)Q(u)$. Then $f(u) = P_1(u)/Q_1(u)$ and $P_1(0) = Q_1(0) = 1$. If we replace P, Q by P_1, Q_1 , then the pair (P_1, Q_1) has the required properties. \square

Ex. 11.2 Prove the converse to Proposition 11.1.1.

Proof. If $N_s = \sum_{j=1}^e \beta_j^s - \sum_{i=1}^d \alpha_i^s$, where α_i, β_j are complex numbers, then

$$\begin{aligned} \sum_{s=1}^{\infty} \frac{N_s u^s}{s} &= \sum_{j=1}^e \left(\sum_{s=1}^{\infty} \frac{(\beta_j u)^s}{s} \right) - \sum_{i=1}^d \left(\sum_{s=1}^{\infty} \frac{(\alpha_i u)^s}{s} \right) \\ &= - \sum_{j=1}^e \ln(1 - \beta_j u) + \sum_{i=1}^d \ln(1 - \alpha_i u). \end{aligned}$$

Here u is a variable, and both members are formal polynomials in $\mathbb{C}[[u]]$, so we don't study convergence. Nevertheless, the left member has a radius of convergence at least q^{-n} , and the right member $\min_{i,j} (1/|\beta_j|, 1/|\alpha_i|)$.

Therefore,

$$Z_f(u) = \exp \left(\sum_{s=1}^{\infty} \frac{N_s u^s}{s} \right) = \prod_{j=1}^e (1 - \beta_j u)^{-1} \prod_{i=1}^d (1 - \alpha_i u) = \frac{\prod_{i=1}^d (1 - \alpha_i u)}{\prod_{j=1}^e (1 - \beta_j u)}$$

is a rational fraction. \square

Ex. 11.3 Give the details of the proof that N_s is independent of the field F_s (see the concluding paragraph to section 1).

Proof. Suppose that E and E' are two fields containing F both with q^s elements. We first show that there is a isomorphism $\sigma : E \rightarrow E'$ which fixes the elements of F , by showing that both E and E' are isomorphic over F to $F[x]/(f(x))$ for some irreducible polynomial $f(x) \in F(x)$.

There is a primitive element $\alpha' \in E'$, i.e. such that $E' = F(\alpha')$. For example, take α' to be a primitive $q^s - 1$ root of unity : since α is a generator of E'^* , every element $\gamma \in E'^*$ is equal to α'^k for some integer k , thus $\gamma \in F(\alpha')$ (and $0 \in F(\alpha')$). This proves $E' \subset F(\alpha')$, and since $\alpha' \in E'$ and $F \subset E'$, $F(\alpha') \subset E'$, so $E' = F(\alpha')$.

Let $f(x) \in F[x]$ be the minimal polynomial of α' over F . Then

$$E' = F(\alpha') \simeq F(x)/(f(x)),$$

where the isomorphism $\sigma_1 : F(\alpha') \rightarrow F(x)/(f(x))$ maps α' to $\bar{x} = x + (f(x))$, and maps $a \in F$ on $\bar{a} = a + (f(x))$. Since α' is a root of $x^{q^s} - x$, $f(x) \mid x^{q^s} - x$.

E is a field with q^s elements, so we have $x^{q^s} - x = \prod_{\alpha \in E} (x - \alpha)$. Thus $f(x) \mid \prod_{\alpha \in E} (x - \alpha)$, where $\deg(f(x)) = s \geq 1$, so $f(\alpha) = 0$ for some $\alpha \in E$. The polynomial f being irreducible over F , f is the minimal polynomial of α over F , thus $F(\alpha) \simeq F[x]/(f(x))$ is a field with q^s elements. Since $F(\alpha) \subset E$, and $|F(\alpha)| = |E|$, we conclude $E = F(\alpha)$, therefore

$$E = F(\alpha) \simeq F(x)/(f(x)),$$

where the isomorphism $\sigma_2 : F(\alpha) \rightarrow F(x)/(f(x))$ maps α to $\bar{x} = x + (f(x))$, and maps $a \in F$ on $\bar{a} = a + (f(x))$.

Then $\sigma = \sigma_1^{-1} \circ \sigma_2 : E \rightarrow E'$ is an isomorphism, and $\sigma(a) = a$ for all $a \in F$.

We can now use the isomorphism σ to induce a map

$$\bar{\sigma} \begin{cases} P^n(E) & \rightarrow P^n(E') \\ [\alpha_0, \dots, \alpha_n] & \mapsto [\sigma(\alpha_0), \dots, \sigma(\alpha_n)]. \end{cases}$$

Then $\bar{\sigma}$ is injective: if $[\sigma(\alpha_0), \dots, \sigma(\alpha_n)] = [\sigma(\beta_0), \dots, \sigma(\beta_n)]$, then there is $\lambda \in F^*$ such that $\beta_i = \lambda \sigma(\alpha_i) = \sigma(\lambda) \sigma(\alpha_i) = \sigma(\lambda \alpha_i)$, $i = 0, \dots, n$, thus $\beta_i = \lambda \alpha_i$, which proves $[\alpha_0, \dots, \alpha_n] = [\beta_0, \dots, \beta_n]$.

If $[\gamma_0, \dots, \gamma_n]$ is any projective point of $P^n(E')$, then

$$[\gamma_0, \dots, \gamma_n] = \bar{\sigma}([\sigma^{-1}(\gamma_0), \dots, \sigma^{-1}(\gamma_n)]).$$

This proves that $\bar{\sigma}$ is surjective. So $\bar{\sigma}$ is a bijection.

Now take $f(y_0, \dots, y_n) \in F[y_0, \dots, y_n]$ an homogeneous polynomial, $\bar{H}_f(E)$ the corresponding projective hypersurface in $P^n(E)$, and $\bar{H}_f(E')$ the corresponding projective hypersurface in $P^n(E')$. We show that $\bar{\sigma}(\bar{H}_f(E)) = \bar{H}_f(E')$.

Since σ is a F -isomorphism, $\sigma(f(\alpha_0, \dots, \alpha_n)) = f(\sigma(\alpha_0), \dots, \sigma(\alpha_n))$ ($\alpha_i \in E$), and similarly $\sigma^{-1}(f(\beta_0, \dots, \beta_n)) = f(\sigma^{-1}(\beta_0), \dots, \sigma^{-1}(\beta_n))$ ($\beta_i \in E'$), thus

$$\begin{aligned} [\alpha_0, \dots, \alpha_n] \in \bar{H}_f(E) &\Rightarrow f(\alpha_0, \dots, \alpha_n) = 0 \\ &\Rightarrow \sigma(f(\alpha_0, \dots, \alpha_n)) = \sigma(0) = 0 \\ &\Rightarrow f(\sigma(\alpha_0), \dots, \sigma(\alpha_n)) = 0 \\ &\Rightarrow \bar{\sigma}([\alpha_0, \dots, \alpha_n]) = [\sigma(\alpha_0), \dots, \sigma(\alpha_n)] \in \bar{H}_f(E'). \end{aligned}$$

This shows $\bar{\sigma}(\bar{H}_f(E)) \subset \bar{H}_f(E')$.

Conversely,

$$\begin{aligned} [\beta_0, \dots, \beta_n] \in \bar{H}_f(E') &\Rightarrow f(\beta_0, \dots, \beta_n) = 0 \\ &\Rightarrow \sigma^{-1}(f(\beta_0, \dots, \beta_n)) = \sigma^{-1}(0) = 0 \\ &\Rightarrow f(\sigma^{-1}(\beta_0), \dots, \sigma^{-1}(\beta_n)) = 0 \\ &\Rightarrow \bar{\sigma}^{-1}([\beta_0, \dots, \beta_n]) = [\sigma^{-1}(\beta_0), \dots, \sigma^{-1}(\beta_n)] \in \bar{H}_f(E). \end{aligned}$$

If we define $\alpha_i = \sigma^{-1}(\beta_i)$, $i = 0, \dots, n$, then $[\alpha_0, \dots, \alpha_n] \in \bar{H}_f(E)$, and $[\beta_0, \dots, \beta_n] = \bar{\sigma}([\alpha_0, \dots, \alpha_n]) \in \bar{\sigma}(\bar{H}_f(E))$. This shows $\bar{H}_f(E') \subset \bar{\sigma}(\bar{H}_f(E))$, and so

$$\bar{\sigma}(\bar{H}_f(E)) = \bar{H}_f(E').$$

Since $\bar{\sigma}$ is a bijection,

$$N_s = |\bar{H}_f(E)| = |\bar{H}_f(E')| = N'_s.$$

So N_s is independent of the choice of the extension $F_s = \mathbb{F}_{q^s}$ of $F = \mathbb{F}_q$. □

Ex. 11.4 Calculate the zeta function of $x_0x_1 - x_2x_3 = 0$ over \mathbb{F}_p .

Proof. Here $F = \mathbb{F}_p$, and $F_s = \mathbb{F}_{p^s}$.

To calculate N_s , we calculate the number of points at infinity (such that $x_0 = 0$), and the numbers of affine points of the curve $\overline{H}_f(\mathbb{F}_{p^s})$ associate to

$$f(x_0, x_1, x_2, x_3) = x_0x_1 - x_2x_3.$$

- To estimate the number of points at infinity, we calculate first the cardinality of the set

$$U = \{(\alpha_0, \alpha_1, \alpha_2, \alpha_3) \in F_s^4 \mid \alpha_0\alpha_1 - \alpha_2\alpha_3 = 0, \alpha_0 = 0\}.$$

Then α_1 takes an arbitrary value $a \in F_s$. Write

$$U_a = \{(\alpha_0, \alpha_1, \alpha_2, \alpha_3) \in U \mid \alpha_1 = a\}.$$

Then $U_a = \{(\alpha_0, \alpha_1, \alpha_2, \alpha_3) \in F_s^4 \mid \alpha_0 = 0, \alpha_1 = a, \alpha_2\alpha_3 = 0\}$, thus $U_a = A \cup B$, where

$$A = \{(\alpha_0, \alpha_1, \alpha_2, \alpha_3) \in U_a \mid \alpha_2 = 0\},$$

$$B = \{(\alpha_0, \alpha_1, \alpha_2, \alpha_3) \in U_a \mid \alpha_3 = 0\}.$$

Since $\alpha_0, \alpha_1, \alpha_3$ are fixed in A , the map $A \rightarrow F_s$ defined by $(\alpha_0, \alpha_1, \alpha_2, \alpha_3) \mapsto \alpha_3$ is a bijection, therefore $|A| = p^s$, and similarly $|B| = p^s$. But $A \cap B = \{(0, 0, 0, 0)\}$, thus

$$|U_a| = |A| + |B| - |A \cap B| = 2p^s - 1.$$

Since U is the disjoint union of the U_a , thus

$$|U| = \sum_{a \in F_s} |U_a| = \sum_{a \in F_s} (2p^s - 1) = 2p^{2s} - p^s.$$

Therefore the number of projective points $[\alpha_0, \alpha_1, \alpha_2, \alpha_3] \in P^3(F_s)$ at infinity (such that $\alpha_0 = 0$) is

$$N_\infty = \frac{|U| - 1}{p^s - 1} = \frac{2p^{2s} - p^s - 1}{p^s - 1} = 2p^s + 1.$$

- Now we calculate the number of points of the affine surface $H_f(\mathbb{F}_s)$ associate to the equation $y_1 = y_2y_3$ (where $y_i = x_i/x_0$).

The maps

$$u \left\{ \begin{array}{ccc} F_s^2 & \rightarrow & H_f(F_s) \\ (\beta, \gamma) & \mapsto & (\beta\gamma, \beta, \gamma) \end{array} \right. \quad \left\{ \begin{array}{ccc} H_f(F_s) & \rightarrow & F_s^2 \\ (\alpha, \beta, \gamma) & \mapsto & (\beta, \gamma) \end{array} \right.$$

satisfy $u \circ v = \text{id}, v \circ u = \text{id}$, so u is a bijection. With more informal words, the arbitrary choice of $\beta, \gamma \in F_s$ gives the affine point (α, β, γ) , where $\alpha = \beta\gamma$.

This gives $|H_f(F_s)| = p^{2s}$.

Therefore

$$N_s = |\overline{H}_f(F_s)| = p^{2s} + 2p^s + 1.$$

We obtain in $\mathbb{C}[[u]]$

$$\begin{aligned}\sum_{s=1}^{\infty} \frac{N_s u^s}{s} &= \sum_{s=1}^{\infty} \frac{(p^2 u)^s}{s} + 2 \sum_{s=1}^{\infty} \frac{(pu)^s}{s} + \sum_{s=1}^{\infty} \frac{u^s}{s} \\ &= -\ln(1 - p^2 u) - 2 \ln(1 - pu) - \ln(1 - u).\end{aligned}$$

This gives

$$Z_f(u) = (1 - p^2 u)^{-1} (1 - pu)^{-2} (1 - u)^{-1}.$$

Note: The result for N_s is verified with the naive and very slow following code in Sage:

```
def N(p,s):
    Fs = GF(p^s)
    counter = 0
    for x in Fs:
        for y in Fs:
            for z in Fs:
                for t in Fs:
                    if x*y == z*t:
                        counter += 1
    return (counter - 1)/(p^s - 1)

p, s = 5, 3
print N(p,s), p^(2*s) + 2*p^s + 1
```

15876 15876

There is a misprint in the “Selected Hints for the Exercises” in Ireland-Rosen p.371. \square

Ex. 11.5 Calculate as explicitly as possible the zeta function of $a_0 x_0^2 + a_1 x_1^2 + \cdots + a_n x_n^2$ over \mathbb{F}_q , where q is odd. The answer will depend on whether n is odd or even and whether $q \equiv 1 \pmod{4}$ or $q \equiv 3 \pmod{4}$.

Proof. Since q is odd, there is a unique character χ of order 2 over $F = \mathbb{F}_q$, and a unique character of order 2 over $F_s = \mathbb{F}_{q^s}$. We first compute the number in \mathbb{F}_q^{n+1} of solutions of the equation $f(x_0, \dots, x_n) = 0$, where $f(x_0, \dots, x_n) = a_0 x_0^2 + \cdots + a_n x_n^2 \in F[x_0, \dots, x_n]$.

$$\begin{aligned}N(a_0 x_0^2 + \cdots + a_n x_n^2 = 0) &= \sum_{a_0 u_0 + \cdots + a_n u_n = 0} N(x_0^2 = u_0) \cdots N(x_n^2 = u_n) \\ &= \sum_{a_0 u_0 + \cdots + a_n u_n = 0} (1 + \chi(u_0)) \cdots (1 + \chi(u_n)) \\ &= \sum_{v_0 + \cdots + v_n = 0} (1 + \chi(a_0)^{-1} \chi(v_0)) \cdots (1 + \chi(a_n^{-1}) \chi(v_n)) \quad (v_i = a_i u_i) \\ &= q^n + \chi(a_0^{-1}) \cdots \chi(a_n^{-1}) J_0(\chi, \chi, \dots, \chi),\end{aligned}$$

Indeed $J_0(\varepsilon, \dots, \varepsilon) = q^{l-1}$, and $J_0(\chi_0, \dots, \chi_n) = 0$ if some but not all of the χ_i are trivial (generalization of Proposition 8.5.1).

We estimate $J_0(\chi, \dots, \chi)$, where there are $n + 1$ entries of χ .

- If n is even, then $\chi^{n+1} = \chi \neq \varepsilon$, thus $J_0(\chi, \dots, \chi) = 0$ (Proposition 8.5.1(d)), and so

$$N(a_0x_0^2 + \dots + a_nx_n^2 = 0) = q^n,$$

and the number of projective points on the hypersurface is given by

$$N_1 = \frac{q^n - 1}{q - 1} = q^{n-1} + \dots + q + 1.$$

- If n is odd, then $\chi^{n+1} = \varepsilon$, thus $J_0(\chi, \dots, \chi) = \chi(-1)(q-1)J(\chi, \dots, \chi)$, with n entries of χ (same Proposition).

By Theorem 3 of chapter 8,

$$J(\chi, \dots, \chi) = \frac{g(\chi)^n}{g(\chi)} = g(\chi)^{n-1}.$$

Since $g(\chi)^2 = g(\chi)g(\chi)^{-1} = \chi(-1)q$ (Exercise 10.22),

$$\begin{aligned} \frac{1}{q-1} J_0(\chi, \dots, \chi) &= \chi(-1)g(\chi)^{n-1} \\ &= \chi(-1)g(\chi)^{n-1} \\ &= \frac{\chi(-1)g(\chi)^{n+1}}{g(\chi)^2} \\ &= \frac{1}{q} g(\chi)^{n+1}. \end{aligned}$$

Therefore

$$N(a_0x_0^2 + \dots + a_nx_n^2 = 0) = q^n + \chi(a_0)^{-1} \dots \chi(a_n)^{-1} \frac{q-1}{q} g(\chi)^{n_1},$$

and

$$N_1 = q^{n-1} + \dots + q + 1 + \frac{1}{q} \chi(a_0)^{-1} \dots \chi(a_n)^{-1} g(\chi)^{n+1}.$$

To conclude this first part,

$$\begin{aligned} N_1 &= q^{n-1} + \dots + q + 1 && \text{if } n \text{ is even,} \\ N_1 &= q^{n-1} + \dots + q + 1 + \frac{1}{q} \chi(a_0)^{-1} \dots \chi(a_n)^{-1} g(\chi)^{n+1} && \text{if } n \text{ is odd.} \end{aligned}$$

To compute N_s , we must replace q by q^s and χ by χ_s , the character of order 2 on F_s . Then

$$\begin{aligned} N_s &= q^{s(n-1)} + \dots + q^s + 1 && \text{if } n \text{ is even,} \\ N_s &= q^{s(n-1)} + \dots + q^s + 1 + \frac{1}{q^s} \chi_s(a_0)^{-1} \dots \chi_s(a_n)^{-1} g(\chi_s)^{n+1} && \text{if } n \text{ is odd.} \end{aligned}$$

(These two results can also be obtained by using the equations (1) and (2) in Theorem 2 of Chapter 10.)

It remains to study χ_s in the odd case.

Since $\chi_s^2 = \varepsilon$, for all $\alpha \in F_s$, $\chi_s(\alpha)^{-1} = \chi_s(\alpha)$, and $\chi_s(\alpha) = -1 \in \mathbb{C}$ if $\alpha^{\frac{q^s-1}{2}} = -1 \in F_s$, $\chi_s(\alpha) = 1$ otherwise.

If $a \in F$, $a^{\frac{q-1}{2}} = \pm 1 = \varepsilon$. Since q is odd, $1 + q + \cdots + q^{s-1} \equiv s \pmod{2}$, thus

$$a^{\frac{q^s-1}{2}} = a^{\frac{q-1}{2}(1+q+\cdots+q^{s-1})} = \varepsilon^{1+q+\cdots+q^{s-1}} = \varepsilon^s,$$

so

$$\chi_s(a) = \chi(a)^s \quad (a \in F).$$

We know that $g(\chi_s)^2 = \chi_s(-1)q^s$ (Ex. 10.22), thus, as n is odd,

$$\begin{aligned} g(\chi_s)^{n+1} &= [g(\chi_s)^2]^{\frac{n+1}{2}} \\ &= \chi_s(-1)^{\frac{n+1}{2}} q^{s\frac{n+1}{2}}. \end{aligned}$$

If $q \equiv 1 \pmod{4}$, then $(-1)^{\frac{q-1}{2}} = 1$, so -1 is a square in \mathbb{F}_q . In this case, -1 is a square in \mathbb{F}_{q^s} , and $\chi_s(-1) = 1$ for all $s \geq 1$. In this case, using $a_i \in F$,

$$\begin{aligned} N_s &= q^{s(n-1)} + \cdots + q^s + 1 + \chi_s(a_0) \cdots \chi_s(a_n) q^{s\frac{n-1}{2}} \\ &= q^{s(n-1)} + \cdots + q^s + 1 + [\chi(a_0) \cdots \chi(a_n)]^s q^{s\frac{n-1}{2}} \end{aligned}$$

If $q \equiv -1 \pmod{4}$, then $\chi(-1) = (-1)^{\frac{q-1}{2}} = -1$, and

$$\chi_s(-1) = \chi(-1)^s = (-1)^s,$$

thus

$$\frac{1}{q^s} g(\chi_s)^{n+1} = (-1)^{s\frac{n+1}{2}} q^{s\frac{n-1}{2}}.$$

This gives for odd integers n , and $q \equiv -1 \pmod{4}$,

$$\begin{aligned} N_s &= q^{s(n-1)} + \cdots + q^s + 1 + (-1)^{s\frac{n+1}{2}} \chi_s(a_0) \cdots \chi_s(a_n) q^{s\frac{n-1}{2}} \\ &= q^{s(n-1)} + \cdots + q^s + 1 + [(-1)^{\frac{n+1}{2}} \chi(a_0) \cdots \chi(a_n)]^s q^{s\frac{n-1}{2}}. \end{aligned}$$

To collect all these cases, we have proved

$$\begin{aligned} N_s &= q^{s(n-1)} + \cdots + q^s + 1 && \text{if } n \equiv 0 \pmod{2}, \\ N_s &= q^{s(n-1)} + \cdots + q^s + 1 + [\chi(a_0) \cdots \chi(a_n)]^s q^{s\frac{n-1}{2}} && \text{if } n \equiv 1 \pmod{2}, q \equiv +1 \pmod{4}, \\ N_s &= q^{s(n-1)} + \cdots + q^s + 1 + [(-1)^{\frac{n+1}{2}} \chi(a_0) \cdots \chi(a_n)]^s q^{s\frac{n-1}{2}} && \text{if } n \equiv 1 \pmod{2}, q \equiv -1 \pmod{4}. \end{aligned} \quad (4)$$

If n is even this gives, as in paragraph 1,

$$Z_f(u) = (1 - q^{n-1}u)^{-1} \cdots (1 - qu)^{-1} (1 - u)^{-1}.$$

In the case $n \equiv 1 \pmod{2}, q \equiv +1 \pmod{4}$, we write for simplicity $\varepsilon = \chi(a_0) \cdots \chi(a_n) = \pm 1$. Then

$$\begin{aligned} \sum_{s=1}^{\infty} \frac{N_s u^s}{s} &= \sum_{m=0}^{n-1} \left(\sum_{s=1}^{\infty} \frac{(q^m u)^s}{s} \right) + \sum_{s=1}^{\infty} \frac{(\varepsilon q^{\frac{n-1}{2}} u)^s}{s} \\ &= - \sum_{m=0}^{n-1} \ln(1 - q^m u) - \ln(1 - \varepsilon q^{\frac{n-1}{2}} u). \end{aligned}$$

Therefore

$$Z_f(u) = \left[\prod_{m=0}^{n-1} (1 - q^m u)^{-1} \right] (1 - \chi(a_0) \cdots \chi(a_n) q^{\frac{n-1}{2}} u)^{-1}.$$

(Same calculation in the last case, with $\varepsilon = (-1)^{\frac{n+1}{2}} \chi(a_0) \cdots \chi(a_n)$.)

We obtain

$$\begin{aligned} Z_f(u) &= P(u) && \text{if } n \equiv 0 \pmod{2}, \\ Z_f(u) &= P(u)(1 - \chi(a_0) \cdots \chi(a_n) q^{\frac{n-1}{2}} u)^{-1} && \text{if } n \equiv 1 \pmod{2}, q \equiv +1 \pmod{4}, \\ Z_f(u) &= P(u)(1 - (-1)^{\frac{n+1}{2}} \chi(a_0) \cdots \chi(a_n) q^{\frac{n-1}{2}} u)^{-1} && \text{if } n \equiv 1 \pmod{2}, q \equiv -1 \pmod{4}, \end{aligned}$$

where $P(u) = (1 - q^{n-1}u)^{-1} \cdots (1 - qu)^{-1}(1 - u)^{-1}$.

(These results are consistent with the example $N_s = q^{2s} + q^s + 1 + \chi_s(-1)q^s$ given in paragraph 1 for the surface defined by $-y_0^2 + y_1^2 + y_2^2 + y_3^2 = 0$, where $n = 3$ is odd.

$$\begin{aligned} Z_f(u) &= (1 - q^2u)^{-1}(1 - qu)^{-1}(1 - u)^{-1}(1 - \chi(-1)qu)^{-1} \\ &= \begin{cases} (1 - q^2u)^{-1}(1 - qu)^{-2}(1 - u)^{-1} & \text{if } q \equiv 1 \pmod{4}, \\ (1 - q^2u)^{-1}(1 - qu)^{-1}(1 - u)^{-1}(1 + qu)^{-1} & \text{if } q \equiv -1 \pmod{4}. \end{cases} \end{aligned}$$

□

Ex. 11.6 Consider $x_0^3 + x_1^3 + x_2^3 = 0$ as an equation over F_4 , the field with four elements. Show that there are nine points on the curve in $P^2(F_4)$. Calculate the zeta function. [Answer: $(1 + 2u)^2 / ((1 - u)(1 - 4u))$.]

Proof. Since $q = 4 \equiv 1 \pmod{3}$, we can apply Theorem 2 of Chapter 10. Let χ be a character of order 3 over $F = \mathbb{F}_4$. The only other character of order 3 is then χ^2 . Thus

$$N_1 = q + 1 + \frac{1}{q-1} \sum_{i,j,k} J_0(\chi^i, \chi^j, \chi^k),$$

where the sum is over all $(i, j, k) \in \{1, 2\}^3$ such that $i + j + k \equiv 0 \pmod{3}$, that is $(1, 1, 1)$ and $(2, 2, 2)$. Thus

$$N_1 = q + 1 + \frac{1}{q-1} (J_0(\chi, \chi, \chi) + J_0(\chi^2, \chi^2, \chi^2)).$$

Using $\frac{1}{q-1} J_0(\chi^k, \chi^k, \chi^k) = \frac{1}{q} g(\chi^k)^3$ for $k = 1, 2$, we obtain

$$N_1 = q + 1 + \frac{1}{q} (g(\chi)^3 + g(\chi^2)^3).$$

Consider $\mathbb{F}_4 = \mathbb{F}_2[x]/(x^2 + x + 1)$, where $a = \bar{x} = x + (x^2 + x + 1)$ is a generator of \mathbb{F}_4^* . Then $\mathbb{F}_4 = \{0, 1, a, a^2 = a + 1\}$. We compute $g(\chi)$ for the character χ of order 3 defined by

$$\frac{t}{\chi(t)} \mid \begin{array}{cccc} 0 & 1 & a & a^2 \\ 0 & 1 & \omega & \omega^2 \end{array}$$

where $\omega = e^{\frac{2i\pi}{3}}$.

for each $t \in \mathbb{F}_4$, $\text{tr}(a) = a + a^2 \in \mathbb{F}_2$, so the traces are $\text{tr}(1) = 1 + 1 = 0$, $\text{tr}(a) = a + a^2 = 1$, $\text{tr}(a^2) = a^2 + a^4 = a^2 + a = 1$. Therefore

$$\begin{aligned} g(\chi) &= \sum_{t \in \mathbb{F}_4} \chi(t) \zeta_2^{\text{tr}(t)} \\ &= \sum_{t \in \mathbb{F}_4} \chi(t) (-1)^{\text{tr}(t)} \\ &= 1 - \omega - \omega^2 \\ &= 2. \end{aligned}$$

(This is in accordance with $|g(\chi)| = q^{1/2} = 2$.) Then $g(\chi^2) = g(\chi^{-1}) = \chi(-1)\overline{g(\chi)} = g(\chi) = 2$. Therefore

$$\begin{aligned} N_1 &= q + 1 + \frac{1}{q}g(\chi)^3 + \frac{1}{q}g(\chi^2)^3 \\ &= 5 + \frac{1}{4}(8 + 8) \\ &= 9. \end{aligned}$$

There are nine points on the curve with equation $x_0^3 + x_1^3 + x_2^3 = 0$ in $P^2(F_4)$ (this is verified with a naive program in Sage).

Now we compute N_s . We must replace $q = 4$ by $q^s = 4^s$, and χ by χ_s , a character with order 3 on $F_s = \mathbb{F}_{4^s}$.

We obtain

$$N_s = q^s + 1 + \frac{1}{q^s} (g(\chi_s)^3 + g(\chi_s^2)^3).$$

Now we compute $g(\chi_s)^3$. By the generalization of Corollary of Proposition 8.3.3.,

$$g(\chi_s)^3 = q^s J(\chi_s, \chi_s),$$

thus

$$N_s = q^s + 1 + J(\chi_s, \chi_s) + J(\chi_s^2, \chi_s^2).$$

We know that $|J(\chi_s, \chi_s)|^2 = q^s = 4^s$ (generalization of Corollary of Theorem 1). Writing $J(\chi_s, \chi_s) = a + b\omega$, $a, b \in \mathbb{Z}$, we search the solutions of

$$|a + b\omega|^2 = a^2 - ab + b^2 = 4^s.$$

Since $\mathbb{Z}[\omega]$ is a PID, the factorization in primes is unique. Here 2 is a prime element of $\mathbb{Z}[\omega]$, and $(a + b\omega)(a + b\omega^2) = 2^{2s}$, therefore $a + b\omega = \varepsilon 2^k$, $a + b\omega^2 = \zeta 2^l$, where $l, k \in \mathbb{N}$ and ε, ζ are units. Moreover $2^k = |a + b\omega| = |a + b\omega^2| = 2^l$, so $k = l = s$. This shows that every solution $a + b\omega$ of $|a + b\omega|^2 = 4^s$ is associated to 2^s :

$$|a + b\omega|^2 = 4^s \iff a + b\omega \in \{-2^s, -1 - 2^s\omega, -2^s\omega, 2^s, 1 + 2^s\omega, 2^s\omega\}.$$

Moreover, we know that $a \equiv -1 \pmod{3}$, $b \equiv 0 \pmod{3}$ (generalization of Proposition 8.3.4.). Therefore

$$J(\chi_s, \chi_s) = a + b\omega = -(-2)^s,$$

and similarly $J(\chi_s^2, \chi_s^2) = -(-2)^s$ (this proves particular cases of the Hasse-Davenport relation, which we have not used here). This gives

$$N_s = 4^s + 1 - 2(-2)^s.$$

For $s = 1$, we find anew $N_1 = 9$.

Then

$$\begin{aligned} \sum_{s=1}^{\infty} \frac{N_s u^s}{s} &= \sum_{s=1}^{\infty} \frac{(4u)^s}{s} + \sum_{s=1}^{\infty} \frac{u^s}{s} - 2 \sum_{s=1}^{\infty} \frac{(-2u)^s}{s} \\ &= -\ln(1 - 4u) - \ln(1 - u) + 2\ln(1 + 2u). \end{aligned}$$

This gives

$$Z_f(u) = \frac{(1 + 2u)^2}{(1 - 4u)(1 - u)}.$$

This is the first example where Z_f has a zero, which satisfies the Riemann hypothesis for curves. \square

Ex. 11.7 Try this exercise if you know a little projective geometry. Let N_s be the number of lines in $P_n(F_{p^s})$. Find N_s and calculate $\sum_{s=1}^{\infty} N_s u^s / s$. (The set of lines in projective space form an algebraic variety called a Grassmannian variety. So do the set of planes three-dimensional linear subspaces, etc.)

Proof. Write $q = p^s$. The set of lines in $P_n(F_q)$ is in bijective correspondence with the set of planes of the vector space F_q^{n+1} . To count these planes, consider the set A of linearly independent pairs (u, v) of the space F_q^{n+1} , and B the set of planes of F_q^{n+1} , and

$$f \left\{ \begin{array}{ll} A & \rightarrow B \\ (u, v) & \mapsto \langle u, v \rangle. \end{array} \right.$$

The set of pre-images of a fixed plane P in B is the set of basis of this plane P . Thus, to obtain N_s , we divide the number of linearly independent pairs (u, v) of the space by the number of basis of a fixed plane. To build such a pair, we choose first a nonzero vector u , and then a vector v not on the line generated by u . Therefore

$$\begin{aligned} N_s &= \frac{(q^{n+1} - 1)(q^{n+1} - q)}{(q^2 - 1)(q^2 - q)} \\ &= \frac{(q^{n+1} - 1)(q^n - 1)}{(q^2 - 1)(q - 1)}. \end{aligned}$$

□

• If $n = 2m + 1$ is odd, then

$$\begin{aligned} N_s &= \frac{q^{2m+2} - 1}{q^2 - 1} \cdot \frac{q^{2m+1} - 1}{q - 1} \\ &= \sum_{k=0}^m q^{2k} \sum_{l=0}^2 q^l \\ &= \sum_{k=0}^m \sum_{l=0}^{2m} q^{2k+l} \\ &= \sum_{r=0}^{4m} a_r q^r \quad (r = 2k + l), \end{aligned}$$

where a_r is the cardinality of the set

$$A_r = \{(k, l) \in \llbracket 0, m \rrbracket \times \llbracket 0, 2m \rrbracket \mid 2k + l = r\}.$$

We note that $0 \leq l = r - 2k \leq 2m$ gives

$$\left\{ \begin{array}{lll} \frac{r}{2} - m \leq k & \leq \frac{r}{2}, \\ 0 \leq k & \leq m, \end{array} \right.$$

that is

$$\max\left(0, \frac{r}{2} - m\right) \leq k \leq \min\left(\frac{r}{2}, m\right), \quad (1)$$

and each such k gives a unique pair $(k, l) = (k, r - 2k)$ in A_r .

– If $0 \leq r \leq 2m$, then (1) $\iff 0 \leq k \leq \frac{r}{2}$, thus $a_r = \lfloor \frac{r}{2} \rfloor + 1$.

- If $2m < r \leq 4m$, then (1) $\iff \frac{r}{2} - m \leq k \leq m$, thus $a_r = 2m - \left\lceil \frac{r}{2} \right\rceil + 1$.

If n is odd, we have proved that

$$\begin{aligned} N_s &= \sum_{r=0}^{2m} \left(\left\lfloor \frac{r}{2} \right\rfloor + 1 \right) q^r + \sum_{r=2m+1}^{4m} \left(2m + 1 - \left\lceil \frac{r}{2} \right\rceil \right) q^r \\ &= \sum_{r=0}^{n-1} \left(\left\lfloor \frac{r}{2} \right\rfloor + 1 \right) p^{sr} + \sum_{r=n}^{2n-2} \left(n - \left\lceil \frac{r}{2} \right\rceil \right) p^{sr}. \end{aligned}$$

- If $n = 2m$ is even, then

$$\begin{aligned} N_s &= \frac{q^{2m} - 1}{q^2 - 1} \cdot \frac{q^{2m+1} - 1}{q - 1} \\ &= \sum_{k=0}^{m-1} q^{2k} \sum_{l=0}^{2m} q^l \\ &= \sum_{k=0}^{m-1} \sum_{l=0}^{2m} q^{2k+l} \\ &= \sum_{r=0}^{4m-2} b_r q^r \quad (r = 2k + l), \end{aligned}$$

where b_r is the cardinality of the set

$$B_r = \{(k, l) \in \llbracket 0, m-1 \rrbracket \times \llbracket 0, 2m \rrbracket \mid 2k + l = r\}.$$

Here $0 \leq l = r - 2k \leq 2m$ gives

$$\begin{cases} \frac{r}{2} - m \leq k \leq \frac{r}{2}, \\ 0 \leq k \leq m-1, \end{cases}$$

that is

$$\max\left(0, \frac{r}{2} - m\right) \leq k \leq \min\left(\frac{r}{2}, m-1\right), \quad (2)$$

and each such k gives a unique pair $(k, l) = (k, r - 2k)$ in B_r .

- If $0 \leq r \leq 2m-1$, then (2) $\iff 0 \leq k \leq \frac{r}{2}$, thus $b_r = \left\lfloor \frac{r}{2} \right\rfloor + 1$.
- If $2m \leq r \leq 4m-2$, then (2) $\iff \frac{r}{2} - m \leq k \leq m-1$, thus $b_r = 2m - \left\lceil \frac{r}{2} \right\rceil$.

If n is odd, we have proved that

$$\begin{aligned} N_s &= \sum_{r=0}^{2m-1} \left(\left\lfloor \frac{r}{2} \right\rfloor + 1 \right) q^r + \sum_{r=2m}^{4m-2} \left(2m - \left\lceil \frac{r}{2} \right\rceil \right) q^r \\ &= \sum_{r=0}^{n-1} \left(\left\lfloor \frac{r}{2} \right\rfloor + 1 \right) p^{sr} + \sum_{r=n}^{2n-2} \left(n - \left\lceil \frac{r}{2} \right\rceil \right) p^{sr}. \end{aligned}$$

This is the same formula as in the odd case ! To conclude, for all dimension n ,

$$N_s = \sum_{r=0}^{n-1} \left(\left\lfloor \frac{r}{2} \right\rfloor + 1 \right) p^{sr} + \sum_{r=n}^{2n-2} \left(n - \left\lceil \frac{r}{2} \right\rceil \right) p^{sr},$$

therefore

$$\sum_{s=1}^{\infty} \frac{N_s u^s}{s} = - \sum_{r=0}^{n-1} \left(\left\lfloor \frac{r}{2} \right\rfloor + 1 \right) \ln(1 - p^r u) - \sum_{r=n}^{2n-2} \left(n - \left\lceil \frac{r}{2} \right\rceil \right) \ln(1 - p^r u)$$

This gives the order of the poles p^{-r} of $Z(u) = \exp \left(\sum_{s=1}^{\infty} \frac{N_s u^s}{s} \right)$.

To verify the equality between the two formulas giving N_s , we test this equality with a Sage program.

```
def N(n,p,s):
    q = p^s
    num = (q^(n+1) - 1)*(q^(n+1) - q)
    den = (q^2 - 1)*(q^2-q)
    return num // den

def M(n,p,s):
    q = p^s
    a = sum((floor(r/2) + 1)*q^r for r in range(n))
    b = sum((n - ceil(r/2))*q^r for r in range(n,2*n-1))
    return a+b
```

N(4,5,3),M(4,5,3)

(3845707062626, 3845707062626)

Ex. 11.8 If f is a nonhomogeneous polynomial, we can consider the zeta function of the projective closure of the hypersurface defined by f (see Chapter 10). One way to calculate this is to count the number of points on $H_f(F_q)$ and then add to it the number of points at infinity. For example, consider $y^2 = x^3$ over F_{p^s} . Show that there is one point at infinity. The origin $(0,0)$ is clearly on this curve. If $x \neq 0$, write $(y/x)^2 = x$ and show that there are p^s more points on this curve. Altogether we have p^s points and the zeta function over F_p is $(1 - pu)^{-1}$.

Proof. Consider the polynomial $f(x, y) = y^2 - x^3$ and $g(x, z) = y^2 - x$, and

$$\begin{aligned} \Gamma &= H_f(F_q) = \{(x, y) \in F_p^2 \mid y^2 = x^3\}, \\ \Gamma_1 &= H_g(F_q) = \{(x, y) \in F_q^2 \mid y^2 = x\}. \end{aligned}$$

Then

$$\varphi \begin{cases} \Gamma \setminus \{(0,0)\} & \rightarrow \Gamma_1 \setminus \{(0,0)\} \\ (x, y) & \mapsto (x, \frac{y}{x}) \end{cases}$$

is defined, since $(\frac{y}{x})^2 = x$ for $(x, y) \in \Gamma \setminus \{(0,0)\}$, thus $(x, \frac{y}{x}) \in \Gamma_1$. Moreover

$$\psi \begin{cases} \Gamma_1 \setminus \{(0,0)\} & \rightarrow \Gamma \setminus \{(0,0)\} \\ (x, y) & \mapsto (x, xy) \end{cases}$$

is correctly defined, since for each $(x, y) \in \Gamma_1 \setminus \{(0,0)\}$, $y^2 = x$, then $x \neq 0$, thus $(xy)^2 = x^3$, and $(x, xy) \in \Gamma$, where $(x, xy) \neq (0,0)$.

Moreover ψ satisfies $\psi \circ \varphi = \text{id}, \varphi \circ \psi = \text{id}$:

$$\begin{aligned}(\psi \circ \varphi)(x, y) &= \psi\left(x, \frac{y}{x}\right) = \left(x, x \frac{y}{x}\right) = (x, y) & ((x, y) \in \Gamma \setminus \{(0, 0)\}), \\(\varphi \circ \psi)(x, y) &= \varphi(x, xy) = \left(x, \frac{xy}{x}\right) = (x, y) & ((x, y) \in \Gamma_1 \setminus \{(0, 0)\}).\end{aligned}$$

So φ is a bijection. This shows that $|\Gamma \setminus \{(0, 0)\}| = |\Gamma_1 \setminus \{(0, 0)\}|$, where $(0, 0) \in \Gamma$ and $(0, 0) \in \Gamma_1$, thus

$$|\Gamma_1| = |\Gamma|.$$

To count the points on Γ_1 , we consider

$$\lambda \begin{cases} F_q & \rightarrow \Gamma_1 \\ y & \mapsto (y^2, y). \end{cases}$$

Then λ is bijective, with inverse $\mu : (x, y) \mapsto y$. This show that

$$|\Gamma| = |\Gamma_1| = q = p^s.$$

Therefore the zeta function of the affine curve $y^2 = x^3$ over F_p is

$$Z_f(u) = (1 - pu)^{-1}.$$

But the projective closure $H_{\bar{f}}(F_q)$ of this curve has $p^s + 1$ points, with only one point at infinity, since $ty^2 = x^3$ has only one point $[t, x, y]$ satisfying $t = 0$, the point $[0, 0, 1]$.

The zeta function of the curve with homogeneous equation $\bar{f}(t, x, y) = ty^2 - x^3$ over F_p is

$$Z_{\bar{f}}(u) = (1 - u)^{-1}(1 - pu)^{-1}.$$

□

Ex. 11.9 Calculate the zeta function of $y^2 = x^3 + x^2$ over F_p .

Proof. The curve Γ defined by the equation $y^2 = x^3 + x^2$ has a singularity at the origine, as in the previous exercise. The same method applies here: if we use $z = y/x$, then $z^2 = x + 1$.

Watch out! Here there are two points $(x, z) \in \Gamma_1$ such that $x = 0$, the points $(0, 1)$ and $(0, -1)$ (here we assume that $p \neq 2$). The curve Γ_1 defined by the equation $z^2 = x + 1$ is such that

$$\varphi \begin{cases} \Gamma \setminus \{(0, 0)\} & \rightarrow \Gamma_1 \setminus \{(0, 1), (0, -1)\} \\ (x, y) & \mapsto \left(x, \frac{y}{x}\right) \end{cases}$$

is bijective, thus $|\Gamma| = |\Gamma_1| - 1$. Since each point of Γ_1 is determined by its coordinate z , $|\Gamma_1| = q = p^s$, and $|\Gamma| = p^s - 1$.

Therefore the zeta function of the affine curve $y^2 = x^3 + x^2$ over F_p is

$$Z_f(u) = (1 - u)(1 - pu)^{-1},$$

There is only one point p at infinity, given by $y^2t = x^3 + x^2t, t = 0$, i.e. $p = [0, 0, 1]$. Thus $N_s = p^s$, and the zeta function of the projective closure of Γ is

$$Z_{\bar{f}}(u) = (1 - pu)^{-1}.$$

□

The results of Ex.8 and Ex. 9 concern only singular cubics.

Ex. 11.10 If $A \neq 0$ in F_q and $q \equiv 1 \pmod{3}$, show that the zeta function of $y^2 = x^3 + A$ over F_q has the form $Z(u) = (1+au+qu^2)/((1-u)(1-qu))$, where $a \in \mathbb{Z}$ and $|a| \leq 2q^{1/2}$.

Proof. Here we compute the zeta function of the projective closure $\overline{H}_f(F_q)$, with equation $f(x, y, t) = y^2t = x^3 + At^3$. If $t = 0$, then $x = 0$, thus there is only one point $[0, 1, 0]$ at infinity (over F_q or over F_{q^s}).

We assume that the characteristic is not 2. Then q is odd, and so $q \equiv 1 \pmod{6}$. Therefore, there are characters of order 2 and 3 on F_q . Write ρ the unique character of order 2, and write χ a character of order 3. As χ is a character of order 3, the characters whose order divides 3 are $\varepsilon, \chi, \chi^2$.

We compute first N_1 . We write $N(y^2 = x^3 + A)$ for the number of points of the affine cubic over F_q , and N_1 for the number of points of the projective cubic, so that $N_1 = N(y^2 = x^3 + A) + 1$. We recall the results obtained in Ex. 8.15.

The map $x \mapsto -x$ is a bijection between the set of roots of $x^3 = b$ and the set of roots of $(-x)^3 = b$, so $N(x^3 = b) = N((-x)^3 = b) = N(x^3 = -b)$.

Using Prop. 8.1.5, we obtain, since $A \neq 0$,

$$\begin{aligned} N(y^2 = x^3 + A) &= \sum_{a+b=A} N(y^2 = a)N(x^3 = -b) \\ &= \sum_{a+b=A} N(y^2 = a)N(x^3 = b) \\ &= \sum_{a+b=A} (1 + \rho(a))(1 + \chi(b) + \chi^2(b)) \\ &= \sum_{i=0}^1 \sum_{j=0}^2 \sum_{a+b=A} \rho^i(a) \chi^j(b) \\ &= \sum_{i=0}^1 \sum_{j=0}^2 \rho(A)^i \chi(A)^j \sum_{a'+b'=1} \rho^i(a') \chi^j(b') \quad (a = Aa', b = Ab') \\ &= \sum_{i=0}^1 \sum_{j=0}^2 \rho(A)^i \chi(A)^j J(\chi^j, \rho^i). \end{aligned}$$

We know (generalization of Theorem 1, Chapter 8) that $J(\chi, \varepsilon) = J(\chi^2, \varepsilon) = J(\varepsilon, \rho) = 0$, and $J(\varepsilon, \varepsilon) = q$, so

$$N(y^2 = x^3 + A) = q + \rho(A)\chi(A)J(\chi, \rho) + \rho(A)\chi^2(A)J(\chi^2, \rho).$$

As $\chi^2(A) = \chi^{-1}(A) = \overline{\chi(A)}$, and as $\overline{\rho(A)} = \rho(A)$, then $J(\chi^2, \rho) = J(\overline{\chi}, \overline{\rho}) = \overline{J(\chi, \rho)}$, and

$$N(y^2 = x^3 + A) = q + \pi + \bar{\pi}, \text{ where } \pi = \rho(A)\chi(A)J(\chi, \rho),$$

therefore

$$N_1 = q + 1 + \pi + \bar{\pi}, \text{ where } \pi = \rho(A)\chi(A)J(\chi, \rho).$$

Since the orders of χ, ρ , and $\chi\rho$ are 3, 2 and 6, $\chi \neq \varepsilon, \rho \neq \varepsilon, \chi\rho \neq \varepsilon$, thus Theorem 1 of Chapter 6 gives

$$J(\chi, \rho) = \frac{g(\chi)g(\rho)}{g(\chi\rho)}, \quad \pi = \rho(A)\chi(A) \frac{g(\chi)g(\rho)}{g(\chi\rho)}.$$

Write $\chi' = \chi \circ N_{F_{q^s}/F_q}$, $\rho' = \rho \circ N_{F_{q^s}/F_q}$. Then χ', ρ' are characters on F_{q^s} , and the orders of χ', ρ' are 3 and 2 (by properties (a), (b) of §3). The same reasoning in F_{q^s} gives

$$N_s = q^s + 1 + \pi' + \overline{\pi'}, \quad \pi' = \rho'(A)\chi'(A)\frac{g(\chi')g(\rho')}{g(\chi'\rho')}.$$

Since $A \in F_q$, the property (c) of §3 gives $\chi'(A) = \chi(A)^s$, $\rho'(A) = \rho(A)^s$. Using the Hasse-Davenport Relation, and $(\chi\rho)' = \chi'\rho'$, we obtain

$$\begin{aligned} \pi' &= \rho'(A)\chi'(A)\frac{g(\chi')g(\rho')}{g(\chi'\rho')} \\ &= -\rho(A)^s\chi(A)^s\frac{(-g(\chi))^s(-g(\rho))^s}{(-g(\chi\rho))^s} \\ &= (-1)^{s+1}\rho(A)^s\chi(A)^s\left[\frac{g(\chi)g(\rho)}{g(\chi\rho)}\right]^s \\ &= -\left[-\rho(A)\chi(A)\frac{g(\chi)g(\rho)}{g(\chi\rho)}\right]^s \\ &= -(-\pi)^s. \end{aligned}$$

This gives N_s in the appropriate form:

$$N_s = q^s + 1 - (-\pi)^s - (-\overline{\pi})^s, \quad \pi = \rho(A)\chi(A)J(\chi, \rho) = \rho(A)\chi(A)\frac{g(\chi)g(\rho)}{g(\chi\rho)}.$$

Using the converse to Proposition 11.1.1 given in Exercise 2, we obtain

$$Z_f(u) = \frac{(1 + \pi u)(1 + \overline{\pi} u)}{(1 - u)(1 - qu)}.$$

Note that $\pi\overline{\pi} = |\pi|^2 = q$ (by Exercise 10.22). Expanding the numerator, this gives

$$Z_f(u) = \frac{1 + au + qu^2}{(1 - u)(1 - qu)},$$

where $a = \pi + \overline{\pi}$.

For all $t \in F_q^*$, $\chi^3(t) = 1$, thus $\chi(t) \in \{1, \omega, \omega^2\} \subset \mathbb{Z}[\omega]$, and $\rho(t) = \pm 1$, therefore $\pi = \rho(A)\chi(A)\sum_{t \in F_q^*} \chi(t)\rho(t) \in \mathbb{Z}[\omega]$. Writing $\pi = u + v\omega$, $u, v \in \mathbb{Z}$, we obtain $a = \pi + \overline{\pi} = 2u - v \in \mathbb{Z}$.

Moreover,

$$|a| \leq |\pi| + |\overline{\pi}| = 2|\pi| = 2q^{1/2}.$$

To conclude,

$$Z_f(u) = \frac{1 + au + qu^2}{(1 - u)(1 - qu)}, \quad a \in \mathbb{Z}, |a| \leq 2q^{1/2}.$$

□

Ex. 11.11 Consider the curve $y^2 = x^3 - Dx$ over F_p , where $D \neq 0$. Call this curve C_1 . Show that the substitution $x = \frac{1}{2}(u + v^2)$ and $y = \frac{1}{2}v(u + v^2)$ transforms C_1 into the curve C_2 given by $u^2 - v^4 = 4D$. Show that in any given finite field the number of finite points on C_1 is one more than the number of finite points on C_2 .

Proof. Let F be a finite field such that the characteristic of F is not 2. Here

$$\begin{aligned} C_1 &= \{(x, y) \in F^2 \mid y^2 = x^3 - Dx\}, \\ C_2 &= \{(u, v) \in F^2 \mid u^2 - v^4 = 4D\}. \end{aligned}$$

Consider the maps

$$\varphi \begin{cases} C_1 \setminus \{(0, 0)\} & \rightarrow C_2 \\ (x, y) & \mapsto \left(2x - \left(\frac{y}{x}\right)^2, \frac{y}{x}\right), \end{cases} \quad \psi \begin{cases} C_2 & \rightarrow C_1 \setminus \{(0, 0)\} \\ (u, v) & \mapsto \left(\frac{1}{2}(u + v^2), \frac{1}{2}v(u + v^2)\right). \end{cases}$$

• The map φ is well defined: If $(x, y) \in C_1 \setminus \{(0, 0)\}$, then $y^2 = x^3 - Dx$, and $x \neq 0$, otherwise $y^2 = x^3 - Dx = 0$, and then $(x, y) = (0, 0)$.

Write $(u, v) = \left(2x - \left(\frac{y}{x}\right)^2, \frac{y}{x}\right)$, then $x = \frac{1}{2}(u + v^2)$ and $y = \frac{1}{2}v(u + v^2)$. The equality $y^2 = x^3 - Dx$ gives

$$\begin{aligned} \frac{1}{2}v^2(u + v^2) &= \frac{1}{4}(u + v^2)^2 - D, \\ 4D &= (u + v^2)^2 - 2v^2(u + v^2), \\ 4D &= u^2 - v^4, \end{aligned}$$

so that $(u, v) = \left(2x - \left(\frac{y}{x}\right)^2, \frac{y}{x}\right) \in C_2$.

• The map ψ is well defined: if $(u, v) \in C_2$, then $u^2 - v^4 = 4D$. Then $u + v^2 \neq 0$, otherwise $4D = u^2 - v^4 = (u - v^2)(u + v^2) = 0$, where $4D \neq 0$ ($D \neq 0$), and the characteristic is not 2 by hypothesis).

Write $(x, y) = \left(\frac{1}{2}(u + v^2), \frac{1}{2}v(u + v^2)\right)$. Then $x = \frac{1}{2}(u + v^2) \neq 0$, and $(u, v) = \left(2x - \left(\frac{y}{x}\right)^2, \frac{y}{x}\right)$. The equality $u^2 - v^4 = 4D$ gives

$$\begin{aligned} \left(2x - \left(\frac{y}{x}\right)^2\right)^2 - \left(\frac{y}{x}\right)^4 &= 4D, \\ 4x^2 - 4\frac{y^2}{x} &= 4D, \\ x^3 - Dx &= y^2, \end{aligned}$$

so that $(x, y) = \left(\frac{1}{2}(u + v^2), \frac{1}{2}v(u + v^2)\right) \in C_1$, and $(x, y) \neq (0, 0)$.

Take any point $(x, y) \in C_1 \setminus \{(0, 0)\}$, then $x \neq 0$. Write $(u, v) = \varphi(x, y) = \left(2x - \left(\frac{y}{x}\right)^2, \frac{y}{x}\right)$. Then $(x, y) = \left(\frac{1}{2}(u + v^2), \frac{1}{2}v(u + v^2)\right) = \psi(u, v) = (\psi \circ \varphi)(x, y)$. Thus $\psi \circ \varphi = 1_{C_1 \setminus \{(0, 0)\}}$. Similarly, take any point $(u, v) \in C_2$. Write $(x, y) = \psi(u, v) = \left(\frac{1}{2}(u + v^2), \frac{1}{2}v(u + v^2)\right)$. Then $(u, v) = \left(2x - \left(\frac{y}{x}\right)^2, \frac{y}{x}\right) = \varphi(x, y) = (\varphi \circ \psi)(u, v)$. Thus $\varphi \circ \psi = 1_{C_2}$.

This proves that φ and ψ are bijections.

Therefore $|C_2| = |C_1 \setminus \{(0, 0)\}| = |C_1| - 1$, and $|C_1| = |C_2| + 1$.

To conclude, in any given finite field whose characteristic is not 2, the number of finite points on C_1 is one more than the number of finite points on C_2 . \square

Ex. 11.12 (*continuation*)

If $p \equiv 3 \pmod{4}$, show that the number of projective points on C_1 is just $p + 1$.

If $p \equiv 1 \pmod{4}$, show that the answer is $p + 1 + \overline{\chi(D)}J(\chi, \chi^2) + \chi(D)J(\chi, \chi^2)$, where χ is a character of order 4 on F_p .

Note: There is an obvious misprint. We must read $p + 1 + \overline{\chi(D)}J(\chi, \chi^2) + \chi(D)\overline{J(\chi, \chi^2)}$

Proof. • Assume first that $p \equiv 3 \pmod{4}$. First, we count the number of affine points on C_2 .

In this case, there is no character of order 4, and the only characters whose order divides 4 are ε and ρ , where ρ is the Legendre's character. Then Exercises 8.1, 8.2, with $d = 4 \wedge (p - 1) = 2$, and Proposition 8.1.5 show that $N(x^4 = a) = N(y^2 = a) = 1 + \rho(a)$. Therefore

$$\begin{aligned}
N(u^2 - v^4 = 4D) &= \sum_{a-b=4D} N(u^2 = a)N(v^4 = b) \\
&= \sum_{a-b=4D} (1 + \rho(a))(1 + \rho(b)) \\
&= \sum_{a \in F} (1 + \rho(a))(1 + \rho(a - 4D)) \\
&= \sum_{a \in F} 1 + \sum_{a \in F} \rho(a) + \sum_{a \in F} \rho(a - 4D) + \sum_{a \in F} \rho(a)\rho(a - 4D) \\
&= p + \sum_{a \in F} \rho(a)\rho(a - 4D).
\end{aligned}$$

We compute this last sum.

$$\begin{aligned}
\sum_{a \in F} \rho(a)\rho(a - 4D) &= \rho(-1) \sum_{a \in F} \rho(a)\rho(c) \\
&= \rho(-1) \sum_{a+c=4D} \rho(a)\rho(c) \\
&= \rho(-1) \sum_{a'+c'=1} \rho(4D)^2 \rho(a')\rho(b') \quad (a = 4Da', c = 4Db') \\
&= \rho(-1)J(\rho, \rho).
\end{aligned}$$

Moreover, by Theorem 1(c), Chapter 8, since $\rho^2 = \varepsilon$,

$$J(\rho, \rho) = J(\rho, \rho^{-1}) = -\rho(-1).$$

Putting all together, we obtain

$$N(u^2 - v^4 = 4D) = p - 1.$$

Then Exercise 11 gives

$$N(y^2 = x^3 - Dx) = p.$$

The projective closure of C_1 has equation $y^2t = x^3 - Dxt^2$. For $t = 0$, $x = 0$, thus $[0, 1, 0]$ is the only point at infinity. The number of projective points on C_1 is

$$N_1 = p + 1.$$

- Now we assume that $p \equiv 1 \pmod{4}$. Then there is a character χ of order 4 on F_p .

$$\begin{aligned}
N(u^2 - v^4 = 4D) &= \sum_{a-b=4D} N(u^2 = a)N(v^4 = b) \\
&= \sum_{a-b=4D} (1 + \rho(a))(1 + \chi(b) + \chi^2(b) + \chi^3(b)) \\
&= \sum_{i=0}^1 \sum_{j=0}^3 \sum_{a-b=4D} \rho^i(a) \chi^j(b).
\end{aligned}$$

The inner sum for each fixed pair (i, j) is

$$\begin{aligned}
\sum_{a-b=4D} \rho^i(a) \chi^j(b) &= \sum_{a \in F_p} \rho^i(a) \chi^j(a - 4D) \\
&= \chi^j(-1) \sum_{a \in F_p} \rho^i(a) \chi^j(4D - a) \\
&= \chi^j(-1) \sum_{a+c=4D} \rho^i(a) \chi^j(c) \\
&= \chi^j(-1) \sum_{a'+c'=1} \rho^i(a') \chi^j(c') \quad (a = 4Da', c = 4Db') \\
&= \chi^j(-1) \rho^i(4D) \chi^j(4D) J(\rho^i, \chi^j).
\end{aligned}$$

Since χ^2 is of order 2, $\rho = \chi^2$, thus

$$\sum_{a-b=4D} \rho^i(a) \chi^j(b) = \chi^j(-1) \chi^{2i+j}(4D) J(\chi^{2i}, \chi^j),$$

and, using $J(\varepsilon, \varepsilon) = p$, $J(\varepsilon, \chi^j) = 0$ if $j \neq 0$,

$$\begin{aligned}
N(u^2 - v^4 = 4D) &= \sum_{i=0}^1 \sum_{j=0}^3 \chi^j(-1) \chi^{2i+j}(4D) J(\chi^{2i}, \chi^j) \\
&= p + \chi(-1) \chi^3(4D) J(\chi^2, \chi) \\
&\quad + \chi^2(-1) \chi^4(4D) J(\chi^2, \chi^2) \\
&\quad + \chi^3(-1) \chi^5(4D) J(\chi^2, \chi^3).
\end{aligned}$$

Since $J(\chi^2, \chi^2) = J(\chi^2, \chi^{-2}) = -\chi^2(-1) = -1$, and $\chi^3 = \bar{\chi}$, we obtain

$$N(u^2 - v^4 = 4D) = p - 1 + \chi(-1) [\overline{\chi(4D)} J(\chi, \chi^2) + \chi(4D) \overline{J(\chi, \chi^2)}].$$

Comme $\chi(4)^2 = \chi(2^4) = \chi^4(2) = 1$, $\chi(4) = \pm 1$ is real. Therefore

$$N(u^2 - v^4 = 4D) = p - 1 + \chi(-4) \left[\overline{\chi(D)} J(\chi, \chi^2) + \chi(D) \overline{J(\chi, \chi^2)} \right].$$

We must add one to obtain the number of affine points of C_1 , and one more to the point at infinity. Thus the number of projective points on C_1 is

$$N_1 = p + 1 + \chi(-4) [\overline{\chi(D)} J(\chi, \chi^2) + \chi(D) \overline{J(\chi, \chi^2)}].$$

But $\chi(-1) = (-1)^{\frac{p-1}{4}}$. To prove this equality, take g a generator of F_p^* such that $\chi(g) = i$ (such a generator exists, since $\chi(g) = \pm i$: if $\chi(g) = -i$, replace g by g^{-1}). Since $g^{p-1} = 1$, and $g^{(p-1)/2} \neq 1$, we obtain $g^{(p-1)/2} = -1$, thus $\chi(-1) = \chi(g)^{(p-1)/2} = i^{(p-1)/2} = (-1)^{(p-1)/4}$. Moreover $\chi(4) = \chi^2(2) = \rho(2) = (-1)^{(p^2-1)/8}$. Thus, for $p = 4k + 1$,

$$\chi(-4) = \chi(-1)\chi(4) = (-1)^{\frac{p-1}{4}}(-1)^{\frac{p^2-1}{8}} = (-1)^k(-1)^{2k^2+k} = 1.$$

Alleluia! We conclude

$$N_1 = p + 1 + \overline{\chi(D)}J(\chi, \chi^2) + \chi(D)\overline{J(\chi, \chi^2)}.$$

□

Ex. 11.13 (continuation) If $p \equiv 1 \pmod{4}$, calculate the zeta function of $y^2 = x^3 - Dx$ over F in terms of π and $\chi(D)$, where $\pi = -J(\chi, \chi^2)$. This calculation in somewhat sharpened form is contained in [23]. The result has played a key role in recent empirical work of B.J.Birch and H.P.F. Swinnerton-Dyer on elliptic curves.

Proof. Here $p \equiv 1 \pmod{4}$, thus $p^s \equiv 1 \pmod{4}$. We consider here the two fields $F = \mathbb{F}_p$ and $F_s = \mathbb{F}_{p^s}$, where $|F| = p$ and $F_s = p^s$.

Let $\rho' = \rho \circ N_{F_s/F}$, and $\chi' = \chi \circ N_{F_s/F}$. The results of §3 show that the map $\xi \mapsto \xi' = \xi \circ N_{F_s/F}$ induces a group isomorphism between the group cyclic C_n of characters on F whose order divides n on the group cyclic C'_n of characters on F_s whose order divides n (see Exercise 16). Thus the order of ρ' is 2 and the order of χ' is 4, and $\chi'^2 = \rho'$.

Replacing χ, rho by χ', ρ' , and p by p^s , we obtain by the same reasoning that the number of projective point of C_1 in $\overline{H}_f(F_s)$ is

$$N_s = p^s + 1 + \chi'(-4) \left[\overline{\chi'(D)}J(\chi', \chi'^2) + \chi'(D)\overline{J(\chi', \chi'^2)} \right].$$

To compute $\chi'(-4)$ and $\chi'(D)$ we use the property (c) of §3. Since -4 and D are in F ,

$$\chi'(-4) = \chi(-4)^s = 1, \quad \chi'(D) = \chi(D)^s.$$

Therefore

$$N_s = p^s + 1 + \overline{\chi(D)}^s J(\chi', \chi'^2) + \chi(D)^s \overline{J(\chi', \chi'^2)}.$$

It remains to compute $J(\chi', \chi'^2)$. Since $\chi' \neq \varepsilon, \chi'^2 \neq \varepsilon, \chi'^3 \neq \varepsilon$,

$$J(\chi', \chi'^2) = \frac{g(\chi')g(\chi'^2)}{g(\chi'^3)}.$$

The Hasse-Davenport relation gives $g(\chi'^k) = -(-g(\chi^k))^s$, thus

$$\begin{aligned} J(\chi', \chi'^2) &= - \left[-\frac{g(\chi)g(\chi^2)}{g(\chi^3)} \right]^s \\ &= -(-J(\chi, \chi^2))^s \\ &= -\pi^s, \end{aligned}$$

where $\pi = -J(\chi, \chi^2) \in \mathbb{Z}[i]$. To conclude,

$$N_s = p^s + 1 - \overline{\chi(D)}^s \pi^s - \chi(D)^s \overline{\pi}^s, \quad \pi = -J(\chi, \chi^2).$$

Then Exercise 2 gives

$$Z_f(u) = \frac{(1 - \overline{\chi(D)}\pi u)(1 - \chi(D)\overline{\pi}u)}{(1 - u)(1 - pu)}, \quad \pi = -J(\chi, \chi^2).$$

Since $|\pi|^2 = |J(\chi, \chi^2)|^2 = p$ (corollary of Theorem 1, chapter 8), expanding the numerator, we obtain

$$Z_f(u) = \frac{1 + au + pu^2}{(1 - u)(1 - pu)}, \quad a = -\text{tr}(\overline{\chi(D)}\pi) \in \mathbb{Z}, \quad \pi = -J(\chi, \chi^2) \in \mathbb{Z}[i].$$

Note: Since $Z_f(u) = \exp(N_1u + \cdots) = 1 + N_1u + \cdots$, and

$$\begin{aligned} Z_f(u) &= (1 + au + pu^2)(1 + u + u^2 + \cdots)(1 + pu + p^2u^2 + \cdots) \\ &= 1 + (a + p + 1)u + \cdots, \end{aligned}$$

the comparison of the coefficient of u in the two power series gives

$$a = N_1 - p - 1, \quad \text{where } N_1 = p + 1 - \overline{\chi(D)}\pi - \chi(D)\overline{\pi}, \quad \pi = -J(\chi, \chi^2).$$

This gives anew $a = -\text{tr}(\overline{\chi(D)}\pi)$.

□

Ex. 11.14 Suppose that $p \equiv 1 \pmod{4}$ and consider the curve $x^4 + y^4 = 1$ over F_p . Let χ be a character of order 4 and $\pi = -J(\chi, \chi^2)$. Give a formula for the number of projective points over F_p and calculate the zeta function. Both answers should depend only on π . (Hint: See Exercises 7 and 16 of Chapter 8, but be careful since there were counting only finite points.)

Proof. We count the number of points at infinity of the curve $C : x^4 + y^4 = 1$ over a finite field F . The projective closure of C has equation $x^4 + y^4 = t^4$. The projective points $[t, x, y]$ such that $t = 0$ satisfy the equation $x^4 + y^4 = 0$. Note that $y = 0$ is impossible since $[0, 0, 0]$ is not a projective point. Thus the points at infinity of the curve C are the points $[0, x, y]$ such that $(0, x, y) = y(0, a, 1)$, where $a^4 = -1$, so that the points at infinity are

$$[0, a, 1], \quad \text{where } a^4 = -1.$$

Since $(0, a, 1) = \lambda(0, b, 1)$ for some $\lambda \in F$ implies $a = b$, their number is $N(a^4 = -1)$.

Write, as in Chapter 8 and Exercise 8.16, for $a \in F$,

$$\begin{cases} \delta_4(a) &= 1 \text{ if } a \text{ is a fourth power in } F, \\ &= 0 \text{ if not.} \end{cases}$$

If $\delta_4(-1) = 0$, then $N(a^4 = -1) = 0$, and if $\delta_4(-1) = 1$, then $N(a^4 = -1) = 4 \wedge (p-1) = 4$ because $p \equiv 1 \pmod{4}$. In both cases $N(a^4 = -1) = 4\delta_4(-1)$.

To conclude, the number of points at infinity of the curve $C : x^4 + y^4 = 1$ over a finite field F is $4\delta_4(-1)$.

In Exercise 8.16, we show that the number of affine points of C is

$$N(x^4 + y^4 = 1) = p + 1 - 4\delta_4(-1) + 2\text{Re}(J(\chi, \chi)) + 4\text{Re}(J(\chi, \chi^2)).$$

Therefore the number of points of the projective closure of C in $\overline{H}_f(F_p)$ is

$$N_1 = p + 1 + 2\operatorname{Re}(J(\chi, \chi)) + 4\operatorname{Re}(J(\chi, \chi^2)).$$

With the same calculation as in Exercise 16 and above, we obtain similarly in the field F_{p^s} ,

$$N_s = p^s + 1 + 2\operatorname{Re}(J(\chi', \chi')) + 4\operatorname{Re}(J(\chi', \chi'^2)),$$

where $\chi' = \chi \circ N_{F_{p^s}/F_p}$ is a character of order 4 on F_{p^s} .

The generalization of Exercise 8.7 gives

$$J(\chi', \chi') = \chi'(-1)J(\chi', \chi'^2),$$

where $\chi'(-1) = \chi(-1)^s = ((-1)^{\frac{p-1}{4}})^s$.

As in exercise 13, the Hasse-Davenport relation shows that

$$\begin{aligned} J(\chi', \chi'^2) &= \frac{g(\chi')g(\chi'^2)}{g(\chi'^3)} \\ &= - \left[-\frac{g(\chi)g(\chi^2)}{g(\chi^3)} \right]^s \\ &= -(-J(\chi, \chi^2))^s \\ &= -\pi^s. \end{aligned}$$

Putting all together, we obtain

$$N_s = p^s + 1 - (((-1)^{\frac{p-1}{4}})^s + 2)(\pi^s + \bar{\pi}^s), \quad \pi = -J(\chi, \chi^2),$$

that is

$$N_s = p^s + 1 - ((-1)^{\frac{p-1}{4}} \pi)^s - ((-1)^{\frac{p-1}{4}} \bar{\pi})^s - 2\pi^s - 2\bar{\pi}^s.$$

Then Exercise 2 gives

$$Z_f(u) = \frac{(1 - (-1)^{\frac{p-1}{4}} \pi u)(1 - (-1)^{\frac{p-1}{4}} \bar{\pi} u)(1 - \pi u)^2(1 - \bar{\pi} u)^2}{(1 - u)(1 - pu)}.$$

Using $|\pi|^2 = p$, we conclude

$$Z_f(u) = \frac{(1 - 2(-1)^{\frac{p-1}{4}} au + pu^2)(1 - 2au + pu^2)^2}{(1 - u)(1 - pu)}, \quad a = \operatorname{Re}(\pi) \in \mathbb{Z}, \quad \pi = -J(\chi, \chi^2) \in \mathbb{Z}[i].$$

Note: By §5 (or Ex. 8.18), we know that a is the unique integer such that $p = a^2 + b^2$ where $a + bi \equiv 1 \pmod{2 + 2i}$. With a simpler formulation $p = a^2 + b^2$, and $a \equiv 1 \pmod{4}$ if $4 \mid b$, $a \equiv -1 \pmod{4}$ if $4 \nmid b$. So we can verify these results for small primes p . \square

Ex. 11.15 Find the number of points on $x^2 + y^2 + x^2y^2 = 1$ for $p = 13$ and $p = 17$. Do it both by means of the formula in section 5 and by direct calculation.

Proof. • If $p = 13$, the only finite points on the curve are the 4 points $(0, 1)(0, -1), (1, 0), (-1, 0)$. We must add the 2 points at infinity to obtain the 6 points $[t, x, y]$

$$[0, 1, 0], [0, 0, 1], [1, 0, 1], [1, 0, -1], [1, 1, 0], [1, -1, 0].$$

Since $p = 13 = 3^2 + 2^2$, where $4 \nmid 2$ and $3 \equiv -1 \pmod{4}$, here $a = 3$, thus the formula of §5 gives

$$N_1 = p - 1 - 2a = 6.$$

• If $p = 17$, the finite points on the curve, given by the following naive program, are the 12 points

$$(0, 1), (0, 16), (1, 0), (2, 8), (2, 9), (8, 2), (8, 15), (9, 2), (9, 15), (15, 8), (15, 9), (16, 0).$$

With the two points at infinity, we obtain 14 projective points.

Here $p = 1^2 + 4^2$, and $p \nmid b = 4$, $a = 1 \equiv 1 \pmod{4}$, thus $a = 1$, and the formula of §5 gives

$$N_1 = p - 1 - 2a = 14.$$

The formula is verified in both cases.

Program Sage to obtain the finite points on the curve $x^2 + y^2 + x^2y^2 = 1$:

```
def N(p):
    Fp = GF(p)
    l = []
    for x in Fp:
        for y in Fp:
            if x^2 + y^2 + x^2*y^2 == 1:
                l.append((x,y))
    return l
```

□

Ex. 11.16 Let F be a field with q elements and F_s an extension of degree s . If χ is a character of F , let $\chi' = \chi \circ N_{F_s/F}$. Show that

- (a) χ' is a character of F_s .
- (b) $\chi \neq \rho$ implies that $\chi' \neq \rho'$.
- (c) $\chi^m = \varepsilon$ implies that $\chi'^m = \varepsilon$.
- (d) $\chi'(a) = \chi(a)^s$ for $a \in F$.
- (e) As χ varies over all characters of F with order dividing m , χ' varies over all characters of F_s with order dividing m . Here we are assuming that $q \equiv 1 \pmod{m}$.

Proof.

- (a) If $\alpha, \beta \in F_s$, we know that $N_{F_s/F}(\alpha\beta) = N_{F_s/F}(\alpha)N_{F_s/F}(\beta)$ (Proposition 11.2.2). Therefore

$$\chi'(\alpha\beta) = \chi(N_{F_s/F}(\alpha\beta)) = \chi(N_{F_s/F}(\alpha)N_{F_s/F}(\beta)) = \chi(N_{F_s/F}(\alpha))\chi(N_{F_s/F}(\beta)) = \chi'(\alpha)\chi'(\beta).$$

This shows that χ' is a character.

(b) Assume that $\chi' = \rho'$. Then for all $\alpha \in K^*$, $\chi(N_{F_s/F}(\alpha)) = \rho(N_{F_s/F}(\alpha))$. By Proposition 11.2.2 (d), the map

$$\varphi \begin{cases} K^* & \rightarrow F^* \\ \alpha & \mapsto N_{K/F}(\alpha) \end{cases}$$

is surjective. Let a be any element of F^* . Since φ is surjective, there is some $\alpha \in F_s^*$ such that $\alpha = a$. Then $\chi(a) = \chi(N_{F_s/F}(\alpha)) = \rho(N_{F_s/F}(\alpha)) = \rho(a)$. Since this is true for every $a \in F^*$, and $\chi(0) = 0 = \rho(0)$, this shows that $\chi = \rho$.

To conclude, $\chi' = \rho'$ implies $\chi = \rho$, thus $\chi \neq \rho$ implies $\chi' \neq \rho'$.

(c) If $\chi^m = \varepsilon$, then for all $\alpha \in K$, $(\chi')^m(\alpha) = \chi^m(N_{F_s/F}(\alpha)) = 1$, thus $\chi'^m = \varepsilon$.

(d) Si $a \in F$, by Proposition 11.2.2(c), $N_{F_s/F}(a) = a^s$, therefore

$$\chi'(a) = \chi(N_{K/F}(a)) = \chi(a^s) = \chi(a)^s.$$

(e) Assume that $q \equiv 1 \pmod{m}$. Write C the group of character on F , C' the group of characters on F_s , C_m the group of character on F with order dividing m , and C'_m the group of character on F_s with order dividing m . By the generalization of Proposition 8.1.3, C is a cyclic group of order $q - 1$, and C' a cyclic group of order $q^s - 1$.

We know that if $m \mid q - 1 = |C|$, the subgroup $C_m = \{\chi \in C \mid \chi^m = \varepsilon\}$ of the cyclic group C is cyclic of order m . Since $m \mid q - 1 \mid q^s - 1$, it is the same for C'_m :

$$|C_m| = |C'_m| = m.$$

Let ψ be the map

$$\psi \begin{cases} C_m & \rightarrow C'_m \\ \chi & \mapsto \chi' = \chi \circ N_{F_s/F}. \end{cases}$$

Part (b) shows that ψ is injective, and $|C_m| = |C'_m| = m$, therefore ψ is bijective. In other words, as χ varies over all characters of F with order dividing m , χ' varies over all characters of F_s with order dividing m . \square

Ex. 11.17 In Theorem 2 show that the order of the numerator of the zeta function, $P(u)$ has degree $m^{-1}((m-1)^{n+1} + (-1)^{n+1}(m-1))$.

Proof. In Theorem 2,

$$P(u) = \prod_{(\chi_0, \dots, \chi_n) \in A} \left(1 - (-1)^{n+1} \frac{1}{q} \chi_0(a_0)^{-1} \cdots \chi_n(a_n^{-1}) g(\chi_0) \cdots g(\chi_n) u \right),$$

where A is the set of $(n+1)$ -tuples (χ_0, \dots, χ_n) of characters on F such that $\chi_i^m = \varepsilon$, $\chi_i \neq \varepsilon$ ($i = 0, \dots, n$) and $\chi_0 \cdots \chi_n = \varepsilon$. In each factor, the coefficient of u is not zero, thus each factor has degree 1. Therefore the degree d of P is $d = \deg(P) = |A|$. Write C_m the subgroup of characters on F such that $\chi^m = \varepsilon$.

Since $q \equiv 1 \pmod{m}$ is an hypothesis of Theorem 2, C_m is a subgroup of order m : $|C_m| = m$ and $|C_m - \{\varepsilon\}| = m - 1$. We count the number d of $(n+1)$ -tuples $(\chi_0, \dots, \chi_n) \in (C_m - \{\varepsilon\})^{n+1}$ such that $\chi_0 \cdots \chi_n = \varepsilon$, that is $\chi_n = \chi_0^{-1} \cdots \chi_{n-1}^{-1}$, and $\chi_n \neq \varepsilon$. Let χ be a character of order m (such a character exists because C_m is cyclic). Write $\chi_i = \chi^{k_i}$, where $1 \leq k_i \leq m - 1$. Then d is the number of n -tuples $(k_0, \dots, k_{n-1}) \in \llbracket 1, m - 1 \rrbracket^n$ such that

$$k_0 + k_1 + \cdots + k_{n-1} \not\equiv 0 \pmod{m}.$$

In other words, d is the number of n -tuples $(a_0, \dots, a_{n-1}) \in ((\mathbb{Z}/m\mathbb{Z})^*)^n$ such that

$$a_0 + a_1 + \dots + a_{n-1} \neq 0.$$

To begin an induction, fix the integer $m \in \mathbb{N}^*$, and write

$$d_n = \text{Card}\{(a_0, \dots, a_{n-1}) \in ((\mathbb{Z}/m\mathbb{Z})^*)^n \mid a_0 + a_1 + \dots + a_{n-1} \neq 0\}.$$

For $n \geq 2$, if $(a_0, \dots, a_{n-2}) \in ((\mathbb{Z}/m\mathbb{Z})^*)^{n-1}$ is given, we count the number of $a_{n-1} \in (\mathbb{Z}/m\mathbb{Z})^*$ such that $a_{n-1} \neq -a_0 - a_1 - \dots - a_{n-2}$.

There are two cases.

If $a_0 + \dots + a_{n-2} \neq 0$, there are $m-2$ choices for $a_{n-1} \in \mathbb{Z}/m\mathbb{Z} \setminus \{0, -a_0 - \dots - a_{n-2}\}$, and if $a_0 + \dots + a_{n-2} = 0$, there are $m-1$ choices for $a_{n-1} \in \mathbb{Z}/m\mathbb{Z} \setminus \{0\}$. This gives the relation

$$\begin{aligned} d_n &= (m-2)d_{n-1} + (m-1)((m-1)^{n-1} - d_{n-1}), \\ &= (m-1)^n - d_{n-1}. \end{aligned}$$

Since $d_1 = \text{Card}\{a \in (\mathbb{Z}/m\mathbb{Z})^* \mid a \neq 0\} = m-1$, we obtain by immediate induction

$$d_n = (m-1)^n - (m-1)^{n-1} + \dots + (-1)^{n-1}(m-1) \quad (n \geq 1).$$

Then

$$\begin{aligned} d_n &= (m-1)^n - (m-1)^{n-1} + \dots + (-1)^{n-1}(m-1) \\ &= (-1)^{n-1}(m-1) \{[-(m-1)]^{n-1} + [-(m-1)]^{n-2} + \dots + 1\} \\ &= (-1)^{n-1}(m-1) \frac{[-(m-1)]^n - 1}{-(m-1) - 1} \\ &= \frac{(-1)^n(m-1) \{[-(m-1)]^n - 1\}}{m} \\ &= \frac{(m-1)^{n+1} + (-1)^{n+1}(m-1)}{m}. \end{aligned}$$

This is the waited answer,

$$\deg(P(u)) = \frac{(m-1)^{n+1} + (-1)^{n+1}(m-1)}{m}.$$

□

Ex. 11.18 Let the notation be as in Exercise 16. Use the Hasse-Davenport relation to show that $J(\chi'_1, \chi'_2, \dots, \chi'_n) = (-1)^{(s-1)(n-1)} J(\chi_1, \chi_2, \dots, \chi_n)^s$, where the χ_i are non trivial characters of F and $\chi_1 \chi_2 \dots \chi_n \neq \varepsilon$.

Proof. Note that $(\chi\rho)' = \chi'\rho'$, thus $(\chi_1 \dots \chi_n)' = \chi'_1 \chi'_2 \dots \chi'_n$.

The conditions on the characters, and Exercise 16, show that $\chi'_i \neq \varepsilon$ and $\chi'_1 \chi'_2 \dots \chi'_n \neq \varepsilon$. By Theorem 3 of Chapter 8,

$$J(\chi'_1, \dots, \chi'_n) = \frac{g(\chi'_1)g(\chi'_2) \dots g(\chi'_n)}{g(\chi'_1 \chi'_2 \dots \chi'_n)}.$$

Then the Hasse-Davenport relation gives

$$\begin{aligned}
J(\chi'_1, \dots, \chi'_n) &= \frac{[-(-g(\chi_1))^s][(-g(\chi_2))^s] \cdots [-(-g(\chi_n))^s]}{-(-g(\chi_1\chi_2 \cdots \chi_n))^s} \\
&= (-1)^{n-1}(-1)^{s(n-1)} \left(\frac{g(\chi_1)g(\chi_2) \cdots g(\chi_n)}{g(\chi_1\chi_2 \cdots \chi_n)} \right)^s \\
&= (-1)^{(s+1)(n-1)} J(\chi_1, \dots, \chi_n)^s \\
&= (-1)^{(s-1)(n-1)} J(\chi_1, \dots, \chi_n)^s.
\end{aligned}$$

□

Ex. 11.19 Prove the identity $\sum \lambda(f)t^{\deg(f)} = \prod (1 - \lambda(f)t^{\deg(f)})^{-1}$, where the sum is over all monic polynomials in $F[t]$ and the product is over all monic irreducible in $F[t]$. λ is defined in Section 4.

(The solution of this exercise requires external knowledge on formal power series. To learn more about formal power series, see [Niven, Formal power series], [Bourbaki, Algebra IV, §4], and [Wikipedia, Formal power series]. About summable families, see [Bourbaki, General Topology, III §5].)

Proof. For each monic polynomial $f(x) = x^n - c_1x^{n-1} + \cdots + (-1)^nc_n \in F[x]$, $\lambda(f)$ is defined by

$$\lambda(f) = \psi(c_1)\chi(c_n).$$

To complete this definition, we define $\lambda(1) = 1$. By Lemma 1, $\lambda(fg) = \lambda(f)\lambda(g)$ for all monic polynomials $f, g \in F[x]$.

We must prove the following equality in the ring of formal power series $\mathbb{C}[[t]]$:

$$\sum_{f \in M} \lambda(f)t^{\deg(f)} = \prod_{f \in I} \left(1 - \lambda(f)t^{\deg(f)}\right)^{-1}, \quad (3)$$

where M is the set of monic polynomials of $F[x]$, and I is the set of monic polynomials of $F[x]$ which are irreducible over F .

Since I and M are infinite sets, we must give a sense at this formula. This implies to introduce a topology on the algebra $\mathbb{C}[[t]]$, which is given by the distance d defined by

$$d(\alpha, \beta) = 2^{-\nu(\alpha - \beta)}, \quad \alpha, \beta \in \mathbb{C}[[t]],$$

where $\nu : \mathbb{C}[[t]] \rightarrow \mathbb{N} \cup \{\infty\}$ is the valuation on $\mathbb{C}[[t]]$: if $\alpha = \sum_{k=0}^{\infty} a_k t^k$, then $\nu(0) = \infty$, and $\nu(\alpha) = \min\{k \in \mathbb{N} \mid a_k \neq 0\}$. This distance is associated to the norm $\|\cdot\|$, given by $\|\gamma\| = 2^{-\nu(\gamma)}$, $\gamma \in \mathbb{C}[[t]]$, so that $E = \mathbb{C}[[t]]$ is a normed vector space.

As in Bourbaki, a family $(u_i)_{i \in I}$ of vectors of a normed vector space is summable, if there is some $S \in E$ such that

$$\forall \varepsilon, \exists J_\varepsilon \in \mathcal{F}(I), \forall J \in \mathcal{F}(I), J \supset J_\varepsilon \Rightarrow \left\| \sum_{i \in J} u_i - S \right\| < \varepsilon,$$

where $\mathcal{F}(I)$ is the set of finite subsets of I . Then we write $S = \sum_{i \in I} u_i$. There is a similar definition for multipliable families.

In the algebra $\mathbb{C}[[t]]$, this is equivalent to $\lim_k u_k = 0$ under the filter of the complementaries of finite sets: $\{A \in \mathcal{P}(I) \mid I \setminus A \in \mathcal{F}(I)\}$ (Bourbaki, IV, 4, Lemma 1), which means, for $(u_i)_{i \in I} \in \mathbb{C}[[t]]^I$,

$$\forall \varepsilon, \exists J_\varepsilon \in \mathcal{F}(I), \forall i \in I \setminus J, \|u_i\| < \varepsilon.$$

Moreover, if the family $(u_i)_{i \in I}$ is summable, then $(1+u_i)_{i \in I}$ is multipliable (Bourbaki, Algebra IV, 4, Proposition 2).

A summable family $(u_i)_{i \in I}$, where I is a countable set, can be summed in any order (Bourbaki, General Topology, III,7 Proposition 9). If $\varphi : \mathbb{N} \rightarrow I$ is a bijection, then

$$\sum_{i \in I} u_i = \sum_{j=0}^{\infty} u_{\varphi(j)}. \quad (4)$$

After these preliminaries, we can show that the family $(\lambda(f)t^{\deg(f)})_{f \in M}$ is summable.

If $\varepsilon > 0$, let N be an integer such that $2^{-N} < \varepsilon$, and consider the set J_ε of monic polynomials f such that $\deg(f) \leq N$. Then J_ε is a finite set, and for all $f \in I \setminus J$, $\deg(f) > N$, so that $\|\lambda(f)t^{\deg(f)}\| = 2^{-\deg(f)} \leq 2^{-N} < \varepsilon$.

This proves that the family $(\lambda(f)t^{\deg(f)})_{f \in M}$ is summable, and $\sum_{f \in M} \lambda(f)t^{\deg(f)}$ makes sense.

Then the sub-family $(\lambda(f)t^{\deg(f)})_{f \in I}$ is also summable. This proves that $(1 - \lambda(f)t^{\deg(f)})_{f \in I}$ is multiplicable, and $\prod_{f \in I} (1 - \lambda(f)t^{\deg(f)})^{-1}$ makes sense.

To prove (3), we use first geometric power series. For all $f \in I$,

$$(1 - \lambda(f)t^{\deg(f)})^{-1} = \sum_{k=0}^{\infty} \lambda(f)^k t^{k \deg(f)}.$$

The set I is a countable set (countable union of finite sets). We use an arbitrary numbering of I , $I = \{f_1, f_2, \dots, f_n, \dots\}$, obtained by a bijection $\varphi : \mathbb{N}^* \rightarrow I$, $\varphi(n) = f_n$. Write I_m the finite set $I_m = \{f_1, \dots, f_m\}$, et M_m the set of monic polynomials whose irreducible factors are in I_m , so that every $f \in M$ uniquely decomposes under the form

$$f = f_1^{a_1} \dots f_m^{a_m}, \quad a_1, \dots, a_m \in \mathbb{N}.$$

Write $d_i = \deg(f_i)$. Then (see Bourbaki, Algebra IV, 4, Proposition 2)

$$\begin{aligned} \sum_{f \in M_m} \lambda(f)t^{\deg(f)} &= \sum_{(a_1, \dots, a_m) \in \mathbb{N}^m} \lambda(f_1)^{a_1} \dots \lambda(f_m)^{a_m} t^{a_1 d_1 + \dots + a_m d_m} \\ &= \left(\sum_{a_1=0}^{\infty} \lambda(f_1)^{a_1} t^{a_1 d_1} \right) \dots \left(\sum_{a_m=0}^{\infty} \lambda(f_m)^{a_m} t^{a_m d_m} \right) \\ &= (1 - \lambda(f_1)t^{d_1})^{-1} \dots (1 - \lambda(f_m)t^{d_m})^{-1} \\ &= \prod_{i=1}^m (1 - \lambda(f_i)t^{\deg(f_i)})^{-1}. \end{aligned}$$

Then, using (4),

$$\begin{aligned} \lim_{m \rightarrow \infty} \prod_{i=1}^m (1 - \lambda(f_i)t^{\deg(f_i)})^{-1} &= \prod_{i=1}^{\infty} (1 - \lambda(f_i)t^{\deg(f_i)})^{-1} \\ &= \prod_{f \in I} (1 - \lambda(f)t^{\deg(f)})^{-1}, \end{aligned}$$

the limit being in the metric space $\mathbb{C}[[t]]$ with the distance d .

Since M is the increasing union of the M_m ,

$$\lim_{m \rightarrow \infty} \sum_{f \in M_m} \lambda(f) t^{\deg(f)} = \sum_{f \in M} \lambda(f) t^{\deg(f)}.$$

We justify this statement.

If $\varepsilon > 0$, let N be an integer such that $2^{-N} < \varepsilon$. The set of monic irreducible polynomials $f_i \in I$ such that $\deg(f) \leq N$ is finite, thus there is some integer M such that, for all integers i , $i \geq M$ implies $\deg(f_i) > N$.

For every $m \geq M$, if $f \in M \setminus M_m$, there is some irreducible monic factor f_i of f such that $i \geq m$, therefore $\deg(f) \geq \deg(f_i) > N$. Then

$$\nu \left(\sum_{f \in M \setminus M_m} \lambda(f) t^{\deg(f)} \right) \geq N,$$

so

$$\left\| \sum_{f \in M} \lambda(f) t^{\deg(f)} - \sum_{f \in M_m} \lambda(f) t^{\deg(f)} \right\| = \left\| \sum_{f \in M \setminus M_m} \lambda(f) t^{\deg(f)} \right\| \leq 2^{-N} < \varepsilon.$$

This shows the statement.

Since

$$\begin{cases} \lim_{m \rightarrow \infty} \sum_{f \in M_m} \lambda(f) t^{\deg(f)} &= \sum_{f \in M} \lambda(f) t^{\deg(f)}, \\ \lim_{m \rightarrow \infty} \prod_{i=1}^m (1 - \lambda(f_i) t^{\deg(f_i)})^{-1} &= \prod_{f \in I} (1 - \lambda(f) t^{\deg(f)})^{-1}, \end{cases}$$

where

$$\sum_{f \in M_m} \lambda(f) t^{\deg(f)} = \prod_{i=1}^m (1 - \lambda(f_i) t^{\deg(f_i)})^{-1},$$

the unicity of the limit shows that

$$\sum_{f \in M} \lambda(f) t^{\deg(f)} = \prod_{f \in I} (1 - \lambda(f) t^{\deg(f)})^{-1}.$$

□

Ex. 11.20 If in Theorem 2 we consider the base field to be F_s instead of F , we get a different zeta function, $Z_f^{(s)}(u)$. Show that $Z_f^{(s)}(u)$ and $Z_f(u)$ are related by the equation $Z_f^{(s)}(u^s) = Z_f(u) Z_f(\rho u) \cdots Z_f(\rho^{s-1} u)$, where $\rho = e^{2i\pi/s}$.

Proof. Let Ω be an algebraic closure of \mathbb{F}_p and write \mathbb{F}_q for the unique subfield of Ω with cardinality q , if q is a power of p . Here $F = \mathbb{F}_q$, and $F_s = \mathbb{F}_{q^s}$. Recall that the function zeta only depends on the cardinality of the finite field, not on the choice of this field (see Exercise 3).

Then

$$Z_f^{(s)}(u) = \exp \left(\sum_{t=1}^{\infty} \frac{N_t^{(s)} u^t}{t} \right),$$

where $N_t^{(s)}$ is the number of points of $\overline{H}_f(\mathbb{F}_{q^{st}})$, because the degree of $\mathbb{F}_{q^{st}}$ over \mathbb{F}_{q^s} is

$$[\mathbb{F}_{q^{st}} : \mathbb{F}_{q^s}] = \frac{[\mathbb{F}_{q^{st}} : \mathbb{F}_q]}{[\mathbb{F}_{q^s} : \mathbb{F}_q]} = \frac{st}{s} = t.$$

Therefore $N_t^{(s)} = N_{st}$, where as usual N_s is the number of points of $\overline{H}_f(\mathbb{F}_q)$. This gives

$$Z_f^{(s)}(u) = \exp\left(\sum_{t=1}^{\infty} \frac{N_{st} u^t}{t}\right).$$

Now, since $\ln(Z_f(u)) = \sum_{k=0}^{\infty} N_k \frac{u^k}{k}$, we obtain

$$\ln(Z_f(\rho^j u)) = \sum_{k=0}^{\infty} N_k \rho^j \frac{u^k}{k}, \quad j = 0, 1, \dots, s-1.$$

The sum of these s equalities gives

$$\sum_{j=0}^{s-1} \ln(Z_f(\rho^j u)) = \sum_{k=0}^{\infty} N_k \left(\sum_{j=0}^{s-1} \rho^{kj} \right) \frac{u^k}{k}.$$

Moreover,

$$\sum_{j=0}^{s-1} \rho^{kj} = \begin{cases} \frac{1-\rho^{ks}}{1-\rho^k} = 0 & \text{if } s \nmid k, \\ s & \text{otherwise.} \end{cases}$$

Therefore

$$\begin{aligned} \sum_{j=0}^{s-1} \ln(Z_f(\rho^j u)) &= \sum_{s|k} N_k s \frac{u^k}{k} \\ &= \sum_{t=1}^{\infty} N_{st} \frac{u^{st}}{t} \quad (k = st) \\ &= \ln(Z_f^{(s)}(u^s)). \end{aligned}$$

To conclude,

$$Z_f(u^s) = Z_f(u) Z_f(\rho u) \cdots Z_f(\rho^{s-1} u), \quad (\rho = e^{2i\pi/s}).$$

□

Ex. 11.21 In Exercise 6 we considered the equation $x_0^3 + x_1^3 + x_2^3 = 0$ over the field with four elements. Consider the same equation over the field with two elements. The trouble here is that $2 \not\equiv 1 \pmod{3}$ and so our usual calculations do not work. Prove that in every extension of $\mathbb{Z}/2\mathbb{Z}$ of odd degree every element is a cube and that every extension of even degree, 3 divides the order of the multiplicative group. Use this information to calculate the zeta function over $\mathbb{Z}/2\mathbb{Z}$. [Answer: $(1 + 2u^2)/(1 - u)(1 - 2u)$.]

Proof. Consider the extension \mathbb{F}_{2^s} of degree s over \mathbb{F}_2 .

- If $s = 2k + 1$ is odd, then $2^s - 1 = 2^{2k+1} - 1 \equiv 1 \pmod{3}$, thus $d = (2^s - 1) \wedge 3 = 1$. An element $a \in \mathbb{F}_{2^s}^*$ is a cube if and only if $a^{(2^s-1)/d} = 1$, that is $a^{2^s-1} = 1$, which is true for all elements $a \in \mathbb{F}_{2^s}^*$ (and $0 = 0^3$). So every element is a cube. The number of solutions of $a^3 = 1$ is $N(a^3 = 1) = d = 1$, thus every element of \mathbb{F}_{2^s} is the cube of a unique element.
- If $s = 2k$ is even, then $2^s - 1 = 2^{2k} - 1 \equiv 0 \pmod{3}$, thus $d = (2^s - 1) \wedge 3 = 3$. So $3 \mid 2^s - 1 = |\mathbb{F}_{2^s}^*|$. Therefore there exists a character χ_s of order 3 in \mathbb{F}_{2^s} .

We can now compute N_s .

- If $s = 2k + 1$ is odd, in the field \mathbb{F}_{2^s} ,

$$\begin{aligned} N(x_0^3 + x_1^3 + x_2^3 = 0) &= \sum_{a+b+c=0} N(x_0^3 = a)N(x_1^3 = b)N(x_2^3 = c) \\ &= \sum_{a+b+c=0} 1 \\ &= 2^{2s}. \end{aligned}$$

Thus the number of projective points of $\overline{H}_f(\mathbb{F}_{2^s})$ is

$$N_s = \frac{2^{2s} - 1}{2^s - 1} = 2^s + 1 \quad (s \text{ odd}).$$

(Alternatively, we can compute the number of affine points, which is $N(y_0^3 + y_1^3 = -1) = N(a + b = -1) = 2^s$, and add a unique point $[0, -1, 1]$ at infinity, since $a^3 = -1$ has exactly one solution -1 . We obtain anew $N_s = 2^s + 1$.)

- If $s = 2k$ is even, in the field \mathbb{F}_{2^s} ,

$$\begin{aligned} N(x_0^3 + x_1^3 + x_2^3 = 0) &= \sum_{a+b+c=0} N(x_0^3 = a)N(x_1^3 = b)N(x_2^3 = c) \\ &= \sum_{a+b+c=0} \sum_{i=0}^2 \chi_s^i(a) \sum_{j=0}^2 \chi_s^j(b) \sum_{k=0}^2 \chi_s^k(c) \\ &= \sum_{(i,j,k) \in \llbracket 0,2 \rrbracket^3} \sum_{a+b+c=0} \chi_s^i(a) \chi_s^j(b) \chi_s^k(c) \\ &= \sum_{(i,j,k) \in \llbracket 0,2 \rrbracket^3} J_0(\chi_s^i, \chi_s^j, \chi_s^k). \end{aligned}$$

Using the generalization of Proposition 8.5.1, with $J_0(\varepsilon, \varepsilon, \varepsilon) = 2^{2s}$, we obtain

$$N(x_0^3 + x_1^3 + x_2^3 = 0) = 2^{2s} + \sum_{(i,j,k) \in A} J_0(\chi_s^i, \chi_s^j, \chi_s^k),$$

where A is the set of $(i, j, k) \in \{1, 2\}^3$ such that $i + j + k \equiv 0 \pmod{3}$, that is $(1, 1, 1)$ and $(2, 2, 2)$. Thus

$$N = N(x_0^3 + x_1^3 + x_2^3 = 0) = 2^{2s} + J_0(\chi_s, \chi_s, \chi_s) + J_0(\chi_s^2, \chi_s^2, \chi_s^2).$$

Thus the number of projective points is

$$N_s = \frac{N - 1}{2^s - 1} = 2^s + 1 + \frac{1}{2^s - 1} (J_0(\chi_s, \chi_s, \chi_s) + J_0(\chi_s^2, \chi_s^2, \chi_s^2)).$$

Moreover, the same Proposition 8.5.2 gives, using $\chi_s(-1) = \chi_s(1) = 1$,

$$\begin{aligned} J_0(\chi_s, \chi_s, \chi_s) &= (2^s - 1)J(\chi_s, \chi_s) \\ &= (2^s - 1) \frac{g(\chi_s)^2}{g(\chi_s^2)} \\ &= (2^s - 1) \frac{g(\chi_s)^3}{g(\chi_s)g(\chi_s^{-1})} \\ &= (2^s - 1) \frac{g(\chi_s)^3}{2^s}. \end{aligned}$$

This gives

$$\frac{1}{2^s - 1} J_0(\chi_s, \chi_s, \chi_s) = \frac{1}{2^s} g(\chi_s)^3.$$

(This is also formula (2) in Theorem 2 of Chapter 10). This is the same for χ_s^2 , thus

$$N_s = 2^s + 1 + \frac{1}{2^s} (g(\chi_s)^3 + g(\chi_s^2)^3).$$

We choose a character χ of order 3 on $\mathbb{F}_4 = \mathbb{F}_{2^2}$, given by

$$\begin{array}{c|cccc} t & 0 & 1 & a & a^2 \\ \hline \chi(t) & 0 & 1 & \omega & \omega^2 \end{array}$$

where a is a generator of \mathbb{F}_4 . We can take $\chi_s = \chi \circ N_{\mathbb{F}_{2^s}/\mathbb{F}_{2^2}}$ (this makes sense since $2 \mid s$, so that \mathbb{F}_{2^2} is a subfield of $\mathbb{F}_{2^s} = \mathbb{F}_{2^{2k}}$).

Since \mathbb{F}_{2^s} is an extension of degree $s/2$ of \mathbb{F}_4 , the Hasse-Davenport relation shows that

$$g(\chi_s) = -(-g(\chi))^{s/2}.$$

The computations of $g(\chi)$ and $g(\chi^2)$ are given in Exercise 6. We obtained

$$g(\chi) = g(\chi^2) = 2.$$

Then

$$N_s = 2^s + 1 - 2(-2)^{\frac{s}{2}}.$$

These two results can be written under the form

$$\begin{cases} N_{2k+1} &= 2^{2k+1} + 1 & (k \geq 0), \\ N_{2k} &= 2^{2k} + 1 - 2(-2)^k & (k \geq 1). \end{cases}$$

We can compute $Z_f(u)$.

$$\begin{aligned} \ln(Z_f(u)) &= \sum_{k=1}^{\infty} N_{2k} \frac{u^{2k}}{2k} + \sum_{k=0}^{\infty} N_{2k+1} \frac{u^{2k+1}}{2k+1} \\ &= \sum_{k=1}^{\infty} \left(2^{2k} + 1 - 2(-2)^k \right) \frac{u^{2k}}{2k} + \sum_{k=0}^{\infty} \left(2^{2k+1} + 1 \right) \frac{u^{2k+1}}{2k+1} \\ &= \left(\sum_{k=1}^{\infty} 2^{2k} \frac{u^{2k}}{2k} + \sum_{k=0}^{\infty} 2^{2k+1} \frac{u^{2k+1}}{2k+1} \right) + \left(\sum_{k=1}^{\infty} \frac{u^{2k}}{2k} + \sum_{k=0}^{\infty} \frac{u^{2k+1}}{2k+1} \right) - 2 \sum_{k=1}^{\infty} (-2)^k \frac{u^{2k}}{2k} \\ &= \sum_{l=1}^{\infty} 2^l \frac{u^l}{l} + \sum_{l=1}^{\infty} \frac{u^l}{l} - \sum_{k=1}^{\infty} \frac{(-2u^2)^k}{k} \\ &= -\ln(1-2u) - \ln(1-u) + \ln(1+2u^2). \end{aligned}$$

Therefore

$$Z_f(u) = \frac{1 + 2u^2}{(1 - u)(1 - 2u)}.$$

□

Note: Using Exercise 20, we obtain anew the result of Exercise 6. Here $s = 2$, and $\rho = e^{2\pi i/s} = e^{i\pi} = -1$. This gives

$$\begin{aligned} Z_f^{(2)}(u^2) &= Z_f(u)Z_f(-u) \\ &= \frac{1 + 2u^2}{(1 - u)(1 - 4u)} \frac{1 + 2u^2}{(1 + u)(1 + 4u)} \\ &= \frac{(1 + 2u^2)^2}{(1 - u^2)(1 - 4u^2)}. \end{aligned}$$

Therefore the function zeta of $f(x_0, x_1, x_2) = x_0^3 + x_1^3 + x_2^3$ with base field \mathbb{F}_4 is

$$Z_f^{(2)}(u) = \frac{(1 + 2u)^2}{(1 - u)(1 - 4u)}.$$

Ex. 11.22 Use the ideas developed in Exercise 21 to show that Theorem 2 continues to hold (in a suitable sense) even when the hypothesis $q \equiv 1 \pmod{m}$ is removed.

Proof. ?????

□

Ex. 11.22 Let $p_1 < p_2 < p_3 < \cdots$ denote the positive prime numbers arranged in order. Let $N_m = p_1^m p_2^m \cdots p_m^m$ and let E_m denote the field with q^{N_m} elements. Show that E_m can be considered as a subfield of E_{m+1} and that $E = \bigcup E_m$ is an extension of $E_0 = F$, a finite field with q elements, with the following property; for every positive integer n , E contains one and only one subfield F_n with q^n elements.

Proof. Here $q = p^a$ is a power of p .

We build the family E_m by induction.

For $m = 0$, $N_1 = 1$. Take $E_0 = F$, a finite field with q elements, whose existence is proved in Theorem 3, Chapter 7. Then $|E_0| = q = q^{N_0}$.

Suppose that we know an extension E_m of F with q^{N_m} elements, so that $[E_m : F] = N_m$.

Write $s = N_m$ and $t = N_{m+1}$. Then $t = (p_1 \cdots p_m p_{m+1}^{m+1}) s$, so $s \mid t$, and $k = t/s$ is an integer. By Exercise 7.14, there exists a polynomial $p(x) \in E_m[x]$ of degree k , irreducible over E_m . Then $K = E_m[x]/(p(x))$ is a field, and the map $j : E_m \rightarrow K$ defined by $j(\alpha) = \bar{\alpha} = \alpha + (p(x))$ is injective. This allows us to “identify” E_m and $j(E_m)$.

More explicitly, if we define $E_{m+1} = (K \setminus j(E_m)) \cup E_m$ (that is, we replace the elements of $j(E_m)$ by the corresponding elements in E_m), then $E_m \subset E_{m+1}$ absolutely, and

$$\varphi \begin{cases} K & \rightarrow E_{m+1} \\ \alpha & \mapsto \begin{cases} \beta & \text{if } \alpha = j(\beta) \in j(E_m) \\ \alpha & \text{if } \alpha \notin j(E_m) \end{cases} \end{cases}$$

is a bijection. This bijection allows us to define a structure of field over E_{m+1} by transport of structure, i.e. the laws $+$, \times on E_{m+1} are given by

$$u + v = \varphi(\varphi^{-1}(u) + \varphi^{-1}(v)), \quad u \times v = \varphi(\varphi^{-1}(u) \times \varphi^{-1}(v)), \quad u, v \in E_{m+1}.$$

Then E_{m+1} is a field for these laws, φ is a field isomorphism, and E_m is a subfield of E_{m+1} . Since the degree of $E_{m+1} \simeq K = E_m[x]/(p(x))$ is $k = \deg(p)$, $[E_{m+1} : E_m] = k = N_{m+1}/N_m$, therefore $[E_{m+1} : F] = [E_{m+1} : E_m][E_m : F] = kN_m = N_{m+1}$. Thus $|E_{m+1}| = q^{N_{m+1}}$.

To conclude this part, the sequence $(E_m)_{m \in \mathbb{N}}$ is an increasing sequence for inclusion, and for each $m \in \mathbb{N}$, $|E_m| = q^{N_m}$.

Now consider the set union

$$E = \bigcup_{m \in \mathbb{N}} E_m.$$

We can define additive and multiplicative laws on E . If $\alpha, \beta \in E$, then $\alpha \in E_r, \beta \in E_s$. If $m = \max(r, s)$, then $\alpha, \beta \in E_m$, so that $\alpha + \beta$ is defined in E_m . Moreover, assume that $\alpha, \beta \in E_{m'}$ for another index m' . Then $E_m \subset E_{m'}$, or $E_{m'} \subset E_m$. If we suppose $E_m \subset E_{m'}$ (the other case is similar), E_m is a subfield of $E_{m'}$, so that $\alpha + \beta$ is the same in E_m or $E_{m'}$. This allows us to define $\alpha + \beta$ in E as the sum of α, β in any field E_m such that α, β are both in E_m . Similarly, we define the law \times .

Then the axioms of a field are verified. For instance, if $\alpha, \beta, \gamma \in E$, there is some $m \in \mathbb{N}$ such that $\alpha, \beta, \gamma \in E_m$, where $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$. Thus this equality is true on E .

This shows that $(E, +, \times)$ is a field, and E_m is a subfield of E for every $m \in \mathbb{N}$. In particular, E is an extension of $F = E_0$.

Now we verify that E has the expected property. Let $n \in \mathbb{N}^*$ be a positive integer. Consider

$$F_n = \{\alpha \in E \mid \alpha^{q^n} = \alpha\}.$$

Then F_n is a subfield of E . Indeed, $1 \in F_n$, and if $\alpha, \beta \in F_n$, and $\gamma \in F_n^*$, then

$$\begin{aligned} (\alpha + \beta)^{q^n} &= \alpha^{q^n} + \beta^{q^n} = \alpha + \beta, \\ (\alpha\beta)^{q^n} &= \alpha^{q^n} \beta^{q^n} = \alpha\beta, \\ (\gamma^{-1})^{q^n} &= (\gamma^{q^n})^{-1} = \gamma^{-1} \end{aligned}$$

thus $\alpha + \beta, \alpha\beta, \gamma^{-1} \in F_n$. Let $n = p_1^{a_1} \cdots p_k^{a_k}$ be the decomposition of n in prime factors, for some $k \in \mathbb{N}$, and $a_i \geq 0$, $i = 1, 2, \dots, k$. If $m = \max\{a_1, \dots, a_k\}$, then $n \mid N_m$. By Lemma 2 and 3 of Chapter 7, this shows that $q^n - 1 \mid q^{N_m} - 1$, thus $x^{q^n-1} - 1 \mid x^{q^{N_m}-1} - 1$, thus $x^{q^n} - x \mid x^{q^{N_m}} - x$. By proposition 7.1.1, since E_m is a field with q^{N_m} elements,

$$x^{q^{N_m}} - x = \prod_{\alpha \in E_m} (x - \alpha).$$

therefore the factor $x^{q^n} - x$ of $x^{q^{N_m}} - x$ splits completely over E_m , a fortiori over E , and Corollary 2 shows that all the roots of $x^{q^n} - x$, which are in E_m , are simple roots.

This prove that

$$x^{q^n} - x = \prod_{\alpha \in A} (x - \alpha),$$

where $A \subset E_m \subset E$.

By definition of F_n , for all $\alpha \in E$, α is a root of $x^{q^n} - 1$ if and only if $\alpha \in F_n$, thus $A = F_n$, and

$$x^{q^n} - x = \prod_{\alpha \in F_n} (x - \alpha),$$

The comparison of the degrees gives

$$q^n = |F_n|.$$

This proves that E contains a field F_n with q^n elements.

Suppose that E contains another field F'_n with q^n elements, then the preceding argument shows that

$$x^{q^n} - x = \prod_{\alpha \in F_n} (x - \alpha) = \prod_{\alpha \in F'_n} (x - \alpha),$$

therefore $F_n = F'_n$.

For every positive integer n , E contains one and only one subfield F_n with q^n elements. \square

Note: We can show a little more, that E is an algebraic closure of F .

First, E is algebraic over F , since every $\alpha \in E$ is in some E_m , which is a finite extension of F , thus α is algebraic over F .

Next, we show that E is algebraically closed. Let $p(x) = \sum_{k=0}^l a_k x^k \in E[x]$ be any non constant polynomial with coefficients in E . There is a $m \in \mathbb{N}$ such that all the coefficients a_i are in E_m , so that $p(x) \in E_m[x]$. Let $f(x)$ be an irreducible factor of $p(x)$ over E_m , with $\deg(f) = d \geq 1$.

Then $f(x)$ has a root γ in the field $K = E_m[x]/(f(x))$, where $|K| = q^{dN_m}$, so γ is a root of $x^{q^{dN_m}} - x$. Since $f(x)$ is the minimal polynomial of γ over E_m , this proves that $f(x) \mid x^{q^{dN_m}} - x$. If $n = dN_m$, we have seen that if F_n is the subfield of E with q^n elements, then $x^{q^n} - x = \prod_{\alpha \in F_n} (x - \alpha)$, so that $f(x)$ splits completely over $F_n = F_{dN_m} \subset E$. Therefore $f(x)$ has a root in E , and also $p(x)$.

We have proved that E is an algebraic closure of F (with a concrete construction, without the axiom of choice, used in the general proof of the existence of algebraic closure).