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. □

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. □

Ex. 11.3 *Give the details of the proof that N_s is independant 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 $\sigma : E \to E'$ which fixes the elements of F, by showing that 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 $\sigma_1 : F(\alpha') \to F(x)/(f(x))$ maps α' to $\overline{x} = x + (f(x))$, and maps $a \in F$ on $\overline{a} = a + (f(x))$. 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 $\sigma_2 : F(\alpha) \to F(x)/(f(x))$ maps α to $\overline{x} = x + (f(x))$, and maps $a \in F$ on $\overline{a} = a + (f(x))$.

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

We can now use the isomorphism σ to induce a map

$$\overline{\sigma}\left\{\begin{array}{ccc} P^n(E) & \to & P^n(E') \\ [\alpha_0,\ldots,\alpha_n] & \mapsto & [\sigma(\alpha_0),\ldots,\sigma(\alpha_n)]. \end{array}\right.$$

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

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

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

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

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

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

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

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

Conversely,

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

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

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

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

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

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

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 le 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 $A \to F_s$ 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
$$u \left\{ \begin{array}{ccc} F_s^2 & \to & H_f(F_s) \\ (\beta, \gamma) & \mapsto & (\beta\gamma, \beta, \gamma) \end{array} \right. \qquad \left\{ \begin{array}{ccc} H_f(F_s) & \to & F_s^2 \\ (\alpha, \beta, \gamma) & \mapsto & (\beta, \gamma) \end{array} \right.$$
satisfy $u \circ v = \mathrm{id}, v \circ u = \mathrm{id}$, 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. $\square$