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 $f(u) = 1 + a_1u + a_2u^2 + \cdots \in F[[u]]$ 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 $F = \mathbb{F}_q$. $\square$