Το Θεωρημα του Dwork

Αναστάσιος Κοτρώνης

Μεταπτυχιακή Εργασία

Επιβλέπων Καθηγητής Ν.Γ. Τζανάκης

Τμήμα Μαθηματικών - Πανεπιστήμιο Κρήτης

Φθινοπωρινό εξάμηνο 2007

Επιτροπή αξιολόγησης :

Νικόλαος Τζανάκης

Ιωάννης Αντωνιάδης

Αλέξανδρος Κουβιδάκης

Στον Άκη, με όλη μου την ψυχή.

Η σκέψη σου πάντα να με "βασανίζει".

Περιεχόμενα

ΕΙΣΑΓΩΓΗ

Σκοπός της παρούσης εργασίας είναι η παρουσίαση της απόδειξης του εξής θεωρήματος :

> *Η συνάρτηση ζήτα οποιασδήποτε αλγεβρικής πολλαπλότητας πάνω από κάποιο πεπερασμένο σώμα είναι πηλίκο πολυωνύμων με ακέραιους συντελεστές και σταθερό όρο μονάδα.*

Η παραπάνω πρόταση ήταν μέρος μίας σειράς εικασιών που διατυπώθηκαν από τον A.Weil το 1949 και αποδείχθηκε από τον Bernard Dwork $(1923-1998)$, το 1959.

Μια βασική έννοια, όσον αφορά τις μεθόδους που χρησιμοποιούνται γιά την απόδειξη του παραπάνω θεωρήματος, είναι αυτή του *μη- Αρχιμήδειου* μετρικού χώρου.
Ένας *μη-Αρχιμήδειος* μετρικός χώρος (X,d), είναι ένα σύνολο $X \neq \emptyset$ εφοδιασμένο με μία συνάρτηση $d : X \times X \to \mathbb{R}^+$ τέτοια ώστε να ικανοποιεί τις ακόλουθες ιδιότητες :

$i)$ $d(x,y) = 0 \Leftrightarrow x = y$
$ii)$ $d(x,y) = d(y,x)$
$iii)$ $d(x,y) \leq \max(d(x,z), d(z,y))$ $\forall z \in X$.

Σε ό,τι θα ακολουθήσει, με Ω_p θα συμβολίζουμε την πλήρωση της αλγεβρικής κλειστότητας $\overline{\mathbb{Q}}_p$ του σώματος $\mathbb{Q}_p$ των $p-$αδικών αριθμών, ως προς την *μη-Αρχιμήδεια* μετρική που επάγει στο $\overline{\mathbb{Q}}_p$ η $|\cdot|_p$.

Στις πρώτες τρεις ενότητες της εργασίας, διατυπώνονται και αποδεικνύονται μια σειρά από λήμματα που αφορούν στις τυπικές δυναμοσειρές με συντελεστές από μία ακέραια περιοχή, και ειδικότερα από το σώμα Ω_p. Ακολουθεί ο ορισμός της δυναμοσειράς $F(X,Y)$ και η απόδειξη του ότι οι συντελεστές της ανήκουν στο δακτύλιο $\mathbb{Z}_p$.

Στην ενότητα 5 διατυπώνεται το βασικό θεώρημα της εργασίας και αποδεικνύεται ότι η ισχύς του ανάγεται στην περίπτωση αφφινικής υπερεπειφάνειας, πάνω από πεπερασμένο σώμα, ορισμένης από ένα πολυώνυμο. Δείχνουμε επιπλέον ότι η συνάρτηση ζήτα μιας αφφινικής υπερεπειφάνειας είναι μία δυναμοσειρά με ακέραιους συντελεστές.

Ορίζοντας, στην ακόλουθη ενότητα, τον αντιπρόσωπο Teichmuller ενός στοιχείου πεπερασμένου σώματος, και την δυναμοσειρά $\Theta(T)$, παρουσιάζεται το "πέρασμα", κατά κάποιον τρόπο, από ένα πεπερασμένο σώμα σε ένα άπειρο, το Ω_p εν προκειμένω, το οποίο είναι εφοδιασμένο με μία μετρική και μπορεί κατ' επέκταση κανείς να μελετήσει σε αυτό τις έννοιες της Ανάλυσης.

Σε ό,τι ακολουθεί, δείχνουμε ότι η συνάρτηση ζήτα είναι πηλίκο δυο δυναμοσειρών με συντελεστές από το Ω_p, σταθερό όρο μονάδα και άπειρη ακτίνα σύγκλισης. Με τη βοήθεια, κατόπιν, μίας άμεσης συνέπειας του θεωρήματος του Weierstrass και δυο λημμάτων που αποδεικνύονται στην τελευταία ενότητα, ολοκληρώνεται η απόδειξη.

1 Τυπικές δυναμοσειρές.

Έστω σώμα K χαρακτηριστικής 0. Θεωρούμε το δακτύλιο $K[[X]]$ και $f = \sum_{i=0}^{\infty} a_i X^i$ τα τυπικά του στοιχεία. Ορίζουμε $\text{ord} f \stackrel{\text{ορσ}}{=} d$ όπου $d = \min\{i : a_i \neq 0\}$, καθώς και τη συνάρτηση $|\cdot|_X : K[[X]] \longrightarrow \mathbb{R}$ με $|f|_X = \rho^{\text{ord} f}$, όπου $\rho \in \mathbb{R}$ με $0 < \rho < 1$. Δεχόμαστε ότι $\text{ord} 0 = \infty$ και $\rho^{\infty} = 0$. Με τις συμβάσεις αυτές και καθώς εύκολα μπορεί να δει κανείς ότι $\text{ord}(fg) = \text{ord} f + \text{ord} g$ και ότι $\text{ord}(f+g) \geq \min(\text{ord} f, \text{ord} g)$, η παραπάνω συνάρτηση καθίσταται μία μη αρχιμήδεια νόρμα και ο $K[[X]]$ ένας μη αρχιμήδειος μετρικός χώρος.

Στα λήμματα που θα ακολουθήσουν θα χρησιμοποιηθεί το εξής: Αν $\{f_n\}_{n=1}^{\infty}$ μία ακολουθία στοιχείων του $K[[X]]$ και $g \in K[[X]]$, τότε $|f_n - g|_X \stackrel{n\to\infty}{\longrightarrow} 0 \Leftrightarrow \text{ord}(f_n - g) \stackrel{n\to\infty}{\longrightarrow} \infty$.

Λήμμα 1.1 *Έστω $\{f_j\}_{j=1}^{\infty}$ μία ακολουθία στοιχείων του $K[[X]]$. Τότε το άθροισμα $\sum_{j=1}^{\infty} f_j$ υπάρχει στον $K[[X]]$ αν και μόνο εαν $\text{ord} f_j \stackrel{j\to\infty}{\longrightarrow} \infty$.*

Απόδειξη. ($\Rightarrow$) Έστω ότι το άθροισμα $\sum_{j=1}^{\infty} f_j$ υπάρχει στον $K[[X]]$ και έστω $M > 0$. Βρίσκω n_M τ.ώ.

$$n \geq n_M \Rightarrow \text{ord}(\sum_{j=1}^{n} f_j - \sum_{j=1}^{\infty} f_j) > M \, . \tag{1}$$

Για $\nu \geq 1$ έχουμε

$$\begin{aligned}
\text{ord} f_{n_N+\nu} =& \text{ord}(\sum_{j=1}^{n_M+\nu} f_j - \sum_{j=1}^{\infty} f_j + \sum_{j=1}^{\infty} f_j - \sum_{j=1}^{n_M+\nu-1} f_j) \\
&\geq \min(\text{ord}(\sum_{j=1}^{n_M+\nu} f_j - \sum_{j=1}^{\infty} f_j), \text{ord}(\sum_{j=1}^{n_M+\nu-1} f_j - \sum_{j=1}^{\infty} f_j)) \\
&> M \, ,
\end{aligned}$$

λόγω της (1). Έπεται λοιπόν ότι αν $j \geq n_m + 1$, τότε $\text{ord} f_j > M$.

($\Leftarrow$) Θέτουμε $f_j = \sum_{i=0}^{\infty} a_{j,i} X^i$ γιά κάθε $j \geq 1$. Έστω ότι $\text{ord} f_j \overset{j\to\infty}{\longrightarrow} \infty$. Θα δείξουμε ότι $\sum_{j=1}^{\infty} f_j = \sum_{i=0}^{\infty} b_i X^i$ γιά κάποιο $\sum_{i=0}^{\infty} b_i X^i \in K[[X]]$, του οποίου τους συντελεστές ορίζουμε ως εξής. Γιά κάθε $M > 0$ θέτουμε $j'_M \overset{ορσ}{=} \min\{j_M :$ αν $j \geq j_M$, τότε $\text{ord} f_j > M\}$ και παρατηρούμε ότι, αν $M_1 < M_2$, τότε $j'_{M_1} \leq j'_{M_2}$.

Έστω τώρα M_0, γιά το οποίο ισχύει $j'_{M_0} > 1$.[1] Γιά $M = M_0+1, M_0+2, \ldots$, αν έχουμε $\sum_{j=1}^{j'_M - 1} f_j = \sum_{i=0}^{\infty} c_{j'_M-1,i} X^i$, θέτουμε $b_i = c_{(j'_M-1),i}$ γιά $i = 0, \ldots, j'_M - 1$. Τα b_i έτσι ορίζονται καλώς, διότι αν $M_0 \leq M_1 < M_2$, τότε $\sum_{j=1}^{j'_{M_2}-1} f_j = \sum_{j=1}^{j'_{M_1}-1} f_j + \sum_{j=j'_{M_1}}^{j'_{M_2}-1} f_j$, όπου γιά $j = j'_{M_1}, \ldots, j'_{M_2} - 1$ έχουμε $f_j = \sum_{i=M_1}^{\infty} a_{j,i} X^i$, άρα ο συντελεστής του X^i για $i = 0, \ldots, j'_{M_1-1}$ είναι ο ίδιος και στα δύο μέλη. Επίσης $\text{ord}(\sum_{j=1}^{n} f_j - \sum_{i=0}^{\infty} b_i X^i) \overset{n\to\infty}{\longrightarrow} \infty$ διότι : Έστω $M > 0$. Γιά $n \geq j'_M - 1$ έχουμε

$$\sum_{j=1}^{n} f_j = \sum_{j=1}^{j'_M-1} f_j + \sum_{j=j'_M}^{n} f_j = \sum_{i=0}^{M} c_{j'_M-1,i} X^i + X^{M+1}(\cdots),$$

διότι $\text{ord} f_j \geq M+1$ γιά $j \geq j'_M$. Εξ' ορισμού, όμως, των b_i είναι $c_{j'_M-1,i} = b_i$, άρα $\text{ord}(\sum_{j=1}^{n} f_j - \sum_{i=0}^{\infty} b_i X^i) > M$.

Λήμμα 1.2 *Έστω ακολουθία $\{f_j\}_{j=1}^{\infty}$ στοιχείων του $K[[X]]$ με $\text{ord} f_j = 0$ γιά κάθε $j \geq 1$. Τότε, το γινόμενο $\prod_{j=1}^{\infty} f_j$ υπάρχει στον $K[[X]]$ αν και μόνο εαν*

[1] Αν γιά κάθε $M > 0$ είχαμε $j'_M = 1$, αυτό θα σήμαινε ότι γιά κάθε $M > 0$, αν $j \geq 1$ τότε $\text{ord} f_j > M$, δηλαδή γιά κάθε $j \geq 1$ $\text{ord} f_j = \infty$, ή αλλιώς $f_j \equiv 0$. Αυτή η περίπτωση είναι τετριμμένη και δεν τη λαμβάνουμε υπόψιν.

$\mathrm{ord}(f_j - 1) \overset{j\to\infty}{\longrightarrow} \infty$.

Απόδειξη. Κατ' αρχάς παρατηρούμε ότι, αν $f, g \in K[[X]]$ με $\mathrm{ord}f = 0$, τότε $\mathrm{ord}(g \cdot f - f) > M$ αν και μόνο εαν $\mathrm{ord}(g-1) > M$. Η απόδειξη είναι προφανής .

($\Rightarrow$) Έστω ότι το γινόμενο $\displaystyle\prod_{j=1}^{\infty} f_j$ υπάρχει στον $K[[X]]$ και έστω $M > 0$. Γιά το δοθέν M, βρίσκω $n_M \in N$ τ.ώ.

$$n \geq n_M \Rightarrow \mathrm{ord}(\prod_{j=1}^{n} f_j - \prod_{j=1}^{\infty} f_j) > M \,. \tag{2}$$

Γιά κάθε $\nu \geq 0$ έχουμε:

$$\begin{aligned}
&\mathrm{ord}(f_{n_M+\nu+1} \prod_{j=1}^{n_M+\nu} f_j - \prod_{j=1}^{n_M+\nu} f_j) = \\
&\quad \mathrm{ord}(f_{n_M+\nu+1} \prod_{j=1}^{n_M+\nu} f_j - \prod_{j=1}^{\infty} f_j + \prod_{j=1}^{\infty} f_j - \prod_{j=1}^{n_M+\nu} f_j) \\
&\quad \geq \min(\mathrm{ord}(f_{n_M+\nu+1} \prod_{j=1}^{n_M+\nu} f_j - \prod_{j=1}^{\infty} f_j), \mathrm{ord}(\prod_{j=1}^{n_M+\nu} f_j - \prod_{j=1}^{\infty} f_j)) \\
&\quad > M \,,
\end{aligned}$$

καθώς

$$\mathrm{ord}(\prod_{j=1}^{n_M+\nu+1} f_j - \prod_{j=1}^{\infty} f_j), \mathrm{ord}(\prod_{j=1}^{n_M+\nu} f_j - \prod_{j=1}^{\infty} f_j) > M \,,$$

λόγω της (2). Από την αρχική παρατήρηση έπεται ότι $\mathrm{ord}(f_{n_M+\nu+1} - 1) > M$, άρα λοιπόν, γιά κάθε $j \geq n_M + 1$, έχουμε $\mathrm{ord}(f_j - 1) > M$.

($\Leftarrow$) Θέτουμε $f_j = \displaystyle\sum_{i=0}^{\infty} a_{j,i} X^i$ γιά κάθε $j \geq 1$.

Έστω ότι $\mathrm{ord}(f_j - 1) \overset{j\to\infty}{\longrightarrow} \infty$. Θα δείξουμε ότι $\displaystyle\prod_{j=1}^{\infty} f_j = \sum_{i=0}^{\infty} b_i X^i$ γιά κάποιο $\displaystyle\sum_{i=0}^{\infty} b_i X^i \in K[[X]]$, του οποίου τους συντελεστές ορίζουμε ως εξής. Γιά κάθε $M > 0$, θέτουμε $j'_M \overset{\text{ορσ}}{=} \min\{j_M \ :\ \text{αν } j \geq j_M \text{ τότε } \mathrm{ord}(f_j - 1) > M\}$. Στο

σημείο αυτό, ομοίως με το προηγούμενο λήμμα, παρατηρούμε ότι, αν $M_1 < M_2$, τότε $j_{M_1'} \leq j_{M_2'}$. Επιλέγουμε M_0 γιά το οποίο ισχύει $j'_{M_0} > 1$.[2] Γιά $M = M_0+1, M_0+2, \ldots$, αν έχουμε $\prod_{j=1}^{j'_M-1} f_j = \prod_{j=1}^{j'_M-1} \sum_{i=0}^{\infty} a_{j,i}X^i = \sum_{i=0}^{\infty} c_{(j'_M-1),i}X^i$, τότε θέτουμε $b_i = c_{(j'_M-1),i}$ γιά $i = 0, \ldots, j'_M-1$. Τα b_i έτσι ορίζονται καλώς διότι : αν $M_1 < M_2$, τότε, αν $\prod_{j=1}^{j'_{M_1}-1} f_j = \sum_{i=0}^{\infty} c_{(j'_{M_1}-1),i}X^i$ και $\prod_{j=1}^{j'_{M_2}-1} f_j = \sum_{i=0}^{\infty} c_{(j'_{M_2}-1),i}X^i$, θα έχουμε $\prod_{j=1}^{j'_{M_2}-1} f_j = \prod_{j=1}^{j'_{M_1}-1} f_j \prod_{j=j'_{M_1}}^{j'_{M_2}-1} f_j$, όπου γιά $j = j'_{M_1}, \ldots, j'_{M_2}-1$, έχουμε $f_j = 1 + \sum_{i=M_1+1}^{\infty} a_{j,i}X^i$, άρα από την παρατήρηση, $c_{(j'_{M_2}-1),i} = c_{(j'_{M_1}-1),i}$ γιά $i = 0, \ldots, j'_{M_1}-1$.
Επίσης $\mathrm{ord}(\prod_{j=1}^{n} f_j - \sum_{i=0}^{\infty} b_iX^i) \stackrel{n\to\infty}{\longrightarrow} \infty$ διότι : έστω $M > 0$. Τότε αν $n \geq n_M \stackrel{\text{ορσ}}{=} j'_M-1$, λόγω της κατασκευής του $\sum_{i=0}^{\infty} b_i$, έχουμε ότι $\mathrm{ord}(\prod_{j=1}^{n} f_j - \sum_{i=0}^{\infty} b_iX^i) > M$.

Λήμμα 1.3 *Έστω* $f = \sum_{i=0}^{\infty} a_iX^i \in K[[X]]$ *και* $g \in K[[X]]$. *Γιά κάθε* $i \geq 0$ *ορίζουμε* $f_i = \sum_{j=0}^{i} a_jX^j$. *Ισχύει ότι, αν* $\mathrm{ord}g > 0$, *τότε η ακολουθία* $\{f_i \circ g\}_{i=1}^{\infty}$ *συγκλίνει σε κάποιο στοιχείο του* $K[[X]]$, *το οποίο συμβολίζουμε* $f \circ g$.

Απόδειξη. Έστω $\mathrm{ord}g > 0$, οπότε μπορούμε να γράψουμε $g = \sum_{j=1}^{\infty} b_{1,j}X^j$. Επειδή $\mathrm{ord}g^i = i \cdot \mathrm{ord}g \geq i$, έχουμε $g^i \stackrel{\text{ορσ}}{=} \sum_{j=i}^{\infty} b_{i,j}X^j$, οπότε

[2] Αν γιά κάθε $M > 0$ είχαμε $j'_M = 1$, αυτό θα σήμαινε ότι γιά κάθε $M > 0$, αν $j \geq 1$ τότε $\mathrm{ord}(f_j - 1) > M$, δηλαδή γιά κάθε $j \geq 1$ $\mathrm{ord}(f_j - 1) = \infty$, ή αλλιώς $f_j \equiv 1$. Αυτή η περίπτωση είναι τετριμμένη και δεν τη λαμβάνουμε υπόψιν.

$$f_i \circ g = a_0 + a_1 \sum_{j=1}^{\infty} b_{1,j} X^j + a_2 \sum_{j=2}^{\infty} b_{2,j} X^j + \ldots + a_i \sum_{j=i}^{\infty} b_{i,j} X^j .$$

Θέτουμε $c_0 = a_0$ και γιά $j \geq 1$, $c_j = a_1 b_{1,j} + a_2 b_{2,j} + \ldots + a_j b_{j,j}$ και έχουμε ότι $\mathrm{ord}(f_i \circ g - \sum_{j=0}^{\infty} c_j X^j) \overset{i \to \infty}{\longrightarrow} \infty$.

Λήμμα 1.4 *Έστω $f \in K[[X]]$, και $\{g_\kappa\}_{\kappa=1}^{\infty}$ ακολουθία στοιχείων του $K[[X]]$ που συγκλίνει στο $g \in K[[X]]$. Υποθέτουμε επιπλέον ότι $\mathrm{ord} g > 0$ γιά κάθε $\kappa \geq 1$. Τότε ορίζεται η $f \circ g$ και μάλιστα είναι το όριο της ακολουθίας $\{f \circ g_k\}_{k \geq 1}$*

Απόδειξη. Έστω $f = \sum_{i=0}^{\infty} a_i X^i$. Αφού γιά κάθε $\kappa \geq 1$ έχουμε $\mathrm{ord} g_\kappa > 0$, έπεται ότι και $\mathrm{ord} g > 0$, άρα, από το λήμμα 1.3 ορίζεται η $f \circ g$. Έστω τώρα $M > 0$. Επιλέγουμε κ_M τ.ώ.

$$\kappa \geq \kappa_M \Rightarrow \mathrm{ord}(g_\kappa - g) > M \; . \tag{3}$$

Τότε, επιπλέον, έχουμε και ότι γιά κάθε $i \geq 1$ και κάθε $\kappa \geq \kappa_M$, είναι

$$\mathrm{ord}(g_\kappa^i - g^i) = \mathrm{ord}(g_\kappa - g) + \mathrm{ord}(g_\kappa^{i-1} + g_\kappa^{i-2} g + \cdots + g_\kappa g^{i-2} + g^{i-1}) > M \, , \tag{4}$$

λόγω της (3). Αν λοιπόν $\kappa \geq \kappa_M$, τότε

$$\begin{aligned}
\mathrm{ord}(f \circ g_\kappa - f \circ g) =& \mathrm{ord}(\sum_{i=1}^{M} a_i (g_\kappa^i - g^i) + \sum_{i=M+1}^{\infty} a_i (g_\kappa^i - g^i)) \\
& \geq \min(\mathrm{ord}(\sum_{i=1}^{M} a_i (g_\kappa^i - g^i)), \mathrm{ord}(\sum_{i=M+1}^{\infty} a_i (g_\kappa^i - g^i))) \\
& > M \, ,
\end{aligned}$$

αφού $\mathrm{ord}(\sum_{i=1}^{M} a_i (g_\kappa^i - g^i)) > M$, λόγω της (4) και $\mathrm{ord}(\sum_{i=M+1}^{\infty} a_i (g_\kappa^i - g^i)) > M$ καθώς $\mathrm{ord} g_\kappa, \mathrm{ord} g > 0$.

Λήμμα 1.5 *Έστω κ θετικός ακέραιος και γιά κάθε $j = 1, \ldots, \kappa$ έχω μία ακολουθία $\{f_{ji}\}_{i=1}^{\infty}$ στοιχείων του $K[[X]]$ τέτοια ώστε $\mathrm{ord} f_{ij} = 0$ γιά κάθε i, το άπειρο* *γινόμενο* $\prod_{i=1}^{\infty} f_{ji}$ *υπάρχει και ισούται, έστω, με* $f_j \in K[[X]]$. *Τότε υπάρχει και το άπειρο γινόμενο* $\prod_{i=1}^{\infty}\prod_{j=1}^{\kappa} f_{ji}$ *και ισούται με* $\prod_{j=1}^{\kappa} f_j (= \prod_{j=1}^{\kappa}\prod_{i=1}^{\infty} f_{ji})$.

Απόδειξη. Έστω $M > 0$. Αφού γιά κάθε $j = 1, \ldots, \kappa$, εχουμε $\mathrm{ord}(\prod_{i=1}^{r} f_{ji} - f_j) \overset{r\to\infty}{\longrightarrow} \infty$ γιά κάποιο $f_j \in K[[X]]$, έπεται από το λήμμα 1.2 ότι γιά κάθε $j = 1, \ldots, \kappa$ ισχύει $\mathrm{ord}(f_{ji} - 1) \overset{i\to\infty}{\longrightarrow} \infty$, δηλαδή γιά το δοθέν $M > 0$ υπάρχει i_0 τέτοιο ώστε, γιά κάθε $i \geq i_0$, και γιά κάθε $j = 1, \ldots, \kappa$ ισχύει ότι $\mathrm{ord}(f_{ji} - 1) > M$, οπότε, γιά κάθε $i \geq i_0$, είναι και

$$\begin{aligned}
&\mathrm{ord}(\prod_{j=1}^{\kappa} f_{ji} - 1) = \\
&\quad \mathrm{ord}\{(f_{\kappa i}\prod_{j=1}^{\kappa-1} f_{ji} - \prod_{j=1}^{\kappa-1} f_{ji}) + (f_{\kappa-1,i}\prod_{j=1}^{\kappa-2} f_{ji} - \prod_{j=1}^{\kappa-2} f_{ji}) + \\
&\qquad\qquad \cdots + (f_{1i}f_{2i} - f_{1i}) + (f_{1i} - 1)\} \\
&\quad \geq \min\{\mathrm{ord}(f_{\kappa i}\prod_{j=1}^{\kappa-1} f_{ji} - \prod_{j=1}^{\kappa-1} f_{ji}), \mathrm{ord}(f_{\kappa-1,i}\prod_{j=1}^{\kappa-2} f_{ji} - \prod_{j=1}^{\kappa-2} f_{ji}), \\
&\qquad\qquad \ldots, \mathrm{ord}(f_{1i}f_{2i} - f_{1i}), \mathrm{ord}(f_{1i} - 1)\} \\
&\quad > M
\end{aligned}$$

(βλ. παρατήρηση λήμματος 1.2). Τα παραπάνω δείχνουν ότι $\mathrm{ord}(\prod_{j=1}^{\kappa} f_{ji} - 1) \overset{i\to\infty}{\longrightarrow} \infty$, άρα από το λήμμα 1.2 έχουμε ότι το άπειρο γινόμενο $\prod_{i=1}^{\infty}\prod_{j=1}^{\kappa} f_{ji}$ υπάρχει στον $K[[X]]$. Έστω $M > 0$. Ψάχνω n_0 τ.ώ.

$$n \geq n_0 \Rightarrow \mathrm{ord}(\prod_{j=1}^{\kappa}\prod_{i=1}^{\infty} f_{ji} - \prod_{i=1}^{n}\prod_{j=1}^{\kappa} f_{ji}) > M\,.$$

Έχουμε ότι γιά κάθε $j = 1, \ldots, \kappa$ υπάρχει i_{j_M} τ.ώ. αν $i \geq i_{j_M}$ τότε $\mathrm{ord}(f_{ji} - 1) > M$. Θέτουμε $n_0 \overset{o\rho\sigma}{=} \max_{1\leq j\leq\kappa}\{i_{j_M}\}$. Αν τώρα $i \geq n_0$, τότε $\mathrm{ord}(f_{ji} - 1) > M$ γιά κάθε $j = 1, \ldots, \kappa$, άρα λοιπόν, γιά κάθε $j = 1, \ldots, \kappa$ και γιά κάθε $n \geq n_0$ έχουμε

$\operatorname{ord}(\prod_{i=n}^{\infty} f_{ji} - 1) > M$, άρα και $\operatorname{ord}(\prod_{j=1}^{\kappa}\prod_{i=n}^{\infty} f_{ji} - 1) > M$. Αν λοιπόν $n \geq n_0$, συνολικά έχουμε:

$$\begin{aligned}
\operatorname{ord}(\prod_{j=1}^{\kappa}\prod_{i=1}^{\infty} f_{ji} - \prod_{i=1}^{n}\prod_{j=1}^{\kappa} f_{ji}) &= \operatorname{ord}(\prod_{j=1}^{\kappa}\prod_{i=1}^{n} f_{ji}(\prod_{j=1}^{\kappa}\prod_{i=n+1}^{\infty} f_{ji} - 1)) \\
&= \operatorname{ord}(\prod_{j=1}^{\kappa} f_{ji}) + \operatorname{ord}(\prod_{j=1}^{\kappa}\prod_{i=n+1}^{\infty} f_{ji} - 1) \\
&= 0 + \operatorname{ord}(\prod_{j=1}^{\kappa}\prod_{i=n+1}^{\infty} f_{ji} - 1) \\
&> M\ .
\end{aligned}$$

Έπεται λοιπόν ότι $\prod_{i=1}^{\infty}\prod_{j=1}^{\kappa} f_{ji} = \prod_{j=1}^{\kappa} f_j$.

Λήμμα 1.6 *Έστω $\{f_j\}_{j=1}^{\infty}$ ακολουθία αντιστρεψίμων στοιχείων του $K[[X]]$, η οποία συγκλίνει σε κάποιο $f \in K[[X]]$. Τότε το f είναι αντιστρέψιμο στοιχείο του $K[[X]]$ και μάλιστα, $f^{-1} = \lim_{j\to\infty} f_j^{-1}$.*

Απόδειξη. Έστω $f_j = \sum_{i=0}^{\infty} a_{ji}X^i$ γιά $j \geq 1$ και $f = \sum_{i=0}^{\infty} a_i X^i$.

Αφού $\operatorname{ord}(f_j - f) \overset{j\to\infty}{\longrightarrow} \infty$, υπάρχει $j_0 \in \mathbb{N}$ τ.ώ. αν $j \geq j_0$, τότε $\operatorname{ord}(f_j - f) > 0$. Ειδικότερα, αυτό συνεπάγεται ότι $a_0 = a_{j_0}$, άρα $a_0 \neq 0$. Συνεπώς, το f είναι αντιστρέψιμο στοιχείο του $K[[X]]$. Έστω γιά $j = 1, 2, \ldots$ $f_j^{-1}(X) = \sum_{i=0}^{\infty} b_{ji}X^i$ και $f^{-1}(X) = \sum_{i=0}^{\infty} b_i X^i$. Τα b_{ji} καθορίζονται μονοσήμαντα από τις σχέσεις

$$\begin{cases} a_{j0}b_{j0} = 1 \\ a_{j1}b_{j0} + a_{j0}b_{j1} = 0 \\ \vdots \\ a_{ji}b_{j0} + \ldots + a_{j0}b_{ji} = 0 \\ \vdots \end{cases}$$

και τα b_i ομοίως από τις

$$\begin{cases} a_0 b_0 = 1 \\ a_1 b_0 + a_0 b_1 = 0 \\ \vdots \\ a_i b_0 + \ldots + a_0 b_i = 0 \\ \vdots \end{cases}$$

Έστω $M > 0$. Βρίσκουμε j_M τ.ώ. αν $j \geq j_M$, τότε $\mathrm{ord}(f_j - f) > 0$. Δηλαδή γιά κάθε $j \geq j_M$, $a_{ji} = a_i$ γιά $i = 0, \ldots, M$. Αν λοιπόν $j \geq j_M$, από τις παραπάνω σχέσεις, και επειδή $a_{ji} = a_i$ γιά $i = 0, \ldots, M$, προκύπτει ότι $b_{ji} = b_i$ γιά $i = 0, \ldots, M$, δηλαδή αν $j \geq j_M$, $\mathrm{ord}(f_j^{-1} - f^{-1}) > M$. Άρα $\mathrm{ord}(f_j^{-1} - f^{-1}) \xrightarrow{j \to \infty} \infty$.

2 Τρεις σημαντικές δυναμοσειρές στο $\Omega_p[[X]]$.

Σε αυτήν την ενότητα εξετάζουμε κάποιες σημαντικές δυναμοσειρές όταν το σώμα K είναι το Ω_p. Αυτές οι δυναμοσειρές $\sum_n a_n X^n$ ορίζουν συγκλίνουσες σειρές $\sum_n a_n x^n$ γιά x σε κατάλληλο δίσκο D, κέτρου 0, του Ω_p.

Έστω $f = \sum_{n=0}^{\infty} a_n X^n \in \Omega_p[[X]]$ και $x \in \Omega_p$. Έχει νόημα να δώσει κανείς την τιμή $\sum_{n=0}^{\infty} a_n x^n$ στο $f(x)$, όταν, αντικαθιστώντας το x στο X, η σειρά $\sum_{n=0}^{\infty} a_n x^n$ συγκλίνει, ή ισοδύναμα $|a_n x^n|_p \xrightarrow{n\to\infty} 0$. Κατ΄ αναλογία με το $\mathbb{R}$ και το $\mathbb{C}$, η ακτίνα σύγκλισης της δυναμοσειράς $\sum_{n=0}^{\infty} a_n X^n$ ορίζεται ως $r = \frac{1}{\limsup_{n\to\infty} |a_n|_p^{\frac{1}{n}}}$. Όπως και στην περίπτωση του $\mathbb{R}$ ή του $\mathbb{C}$, ο όρος ακτίνα σύγκλισης δικαιολογείται από το ότι, καθώς αποδεικνύεται, αν $|x|_p < r$, τότε η σειρά $\sum_{n=0}^{\infty} a_n x^n$ συγκλίνει, ενώ αν $|x|_p > r$, τότε η σειρά $\sum_{n=0}^{\infty} a_n x^n$ αποκλίνει.

Πραγματικά, έστω $x \in \Omega_p$ με $|x|_p < r$. Θέτουμε $|x|_p = (1-\varepsilon)r$ όπου $0 < \varepsilon \leq 1$. Αφού $\limsup |a_n|_p^{\frac{1}{n}} = \frac{1}{r}$, έπεται ότι υπάρχει $n_0 \in \mathbb{N}$ τ.ώ. αν $n \geq n_0$, τότε $|a_n|_p^{\frac{1}{n}} \leq \frac{1}{r} < \frac{1}{r(1-\frac{1}{2}\varepsilon)}$. Άρα έχουμε ότι

$$\lim_{n\to\infty} |a_n x^n|_p = \lim_{n\to\infty} (|a_n|_p^{\frac{1}{n}})^n (r(1-\varepsilon))^n < \lim_{n\to\infty} r^n (\frac{1}{r(1-\frac{1}{2}\varepsilon)})^n (1-\varepsilon)^n = \lim_{n\to\infty} (\frac{(1-\varepsilon)r}{(1-\frac{1}{2}\varepsilon)r})^n = 0.$$

Έστω $x \in \Omega_p$ με $|x|_p > r$. Θέτουμε $|x|_p = (1+\varepsilon)r$ όπου $0 < \varepsilon$. Έχουμε ότι $\lim_{\kappa\to\infty} |a_{n_\kappa}|_p^{\frac{1}{n_\kappa}} = \frac{1}{r}$ όπου a_{n_κ} μία υπακολουθία της a_n, άρα υπάρχει κ_0 τ.ώ. αν $\kappa \geq \kappa_0$, τότε $|a_{n_\kappa}|_p^{\frac{1}{n_\kappa}} > \frac{1}{r(1+\frac{1}{2}\varepsilon)}$. Έχουμε λοιπόν ότι

$$\lim_{\kappa\to\infty} |a_{n_\kappa} x^{n_\kappa}|_p > \lim_{\kappa\to\infty} r^{n_\kappa} (1+\varepsilon)^{n_\kappa} (\frac{1}{r(1+\frac{1}{2}\varepsilon)})^{n_\kappa} = \infty,$$

συνεπώς $|a_n x^n|_p \overset{n\to\infty}{\not\longrightarrow} 0$.

2.1 Η λογαριθμική συνάρτηση.

Έστω η τυπική δυναμοσειρά $\sum_{n=1}^{\infty}(-1)^{n+1}\frac{X^n}{n} \in \Omega_p[[X]]$. Έχουμε $r = \frac{1}{\limsup_{n\to\infty} p^{\frac{\mathrm{ord}_p n}{n}}}$. Επειδή όμως $\frac{\mathrm{ord}_p n}{n} \leq \frac{log_p n}{n} \stackrel{n\to\infty}{\longrightarrow} 0$, έχουμε ότι $r = 1$. Επιπλέον, αν $x \in \Omega_p$ με $|x|_p = 1$, τότε $|a_n x^n|_p = p^{\mathrm{ord}_p n} \geq 1$, συνεπώς η $\sum_{n=1}^{\infty}(-1)^{n+1}\frac{x^n}{n}$ αποκλίνει γιά όλα τα $x \in \Omega_p$ με $|x|_p = 1$.

Η δυναμοσειρά $\sum_{n=1}^{\infty}(-1)^{n+1}\frac{X^n}{n}$ ορίζει, λοιπόν, μία συνάρτηση από τον ανοιχτό δίσκο $D(1-)$ στο Ω_p που απεικονίζει το $x \in D(1-)$ στο $\sum_{n=1}^{\infty}(-1)^{n+1}\frac{x^n}{n}$. Αυτήν τη συνάρτηση θα τη συμβολίζουμε $\log_p(1+X)$ και συνεπώς θα έχουμε $\log_p(1+x) = \sum_{n=1}^{\infty}(-1)^{n+1}\frac{x^n}{n}$ γιά κάθε $x \in D(1-)$.

2.2 Η εκθετική συνάρτηση.

Έστω η τυπική δυναμοσειρά $\sum_{n=0}^{\infty}\frac{X^n}{n!} \in \Omega_p[[X]]$. Έχουμε $r = \frac{1}{\limsup_{n\to\infty} p^{\frac{\mathrm{ord}_p n!}{n}}}$. Ισχύει το εξής φράγμα :

$$\frac{\mathrm{ord}_p n!}{n} = \frac{1}{n}\sum_{i=1}^{\infty}[\frac{n}{p^i}] \leq \frac{1}{n}\sum_{i=1}^{\infty}\frac{n}{p^i} = \frac{1}{p-1}.$$

Αν θεωρήσουμε την υπακολουθία a_{p^N} της a_n τότε :

$$\lim_{N\to\infty} |a_{p^N}|_p^{\frac{1}{p^N}} = \lim_{N\to\infty} p^{\frac{1}{p^N}\sum_{i=1}^{\infty}[\frac{p^N}{p^i}]} =$$

$$\lim_{N\to\infty} p^{\frac{1}{p^N}(p^{N-1}+p^{N-2}+\ldots+p+1)} = \lim_{N\to\infty} p^{\frac{p^N-1}{p^{N+1}-p^N}} = p^{\frac{1}{p-1}},$$

άρα η ακτίνα σύγκλισης είναι $r = \frac{1}{p^{\frac{1}{p-1}}} = p^{-\frac{1}{p-1}}$. Επιπλέον, αν $|x|_p = r$, η σειρά αποκλίνει διότι η ακολουθία με γενικό όρο $a_n x^n = \frac{x^n}{n!}$ δεν είναι μηδενική. Πράγματι, αν θεωρήσουμε την υπακολουθία $\{a_{n_k}x^{n_k}\}$, $n_k = p^k$, τότε

$$\mathrm{ord}_p(a_{n_k}x^{n_k}) = -\mathrm{ord}_p(p^k!) + \tfrac{p^k}{p-1} = -(1+p+\ldots+p^{k-1}) + \tfrac{p^k}{p-1} = \tfrac{1}{p-1},$$

άρα η υπακολουθία $\{|a_{n_k}x^{n_k}|_p\}$ δεν είναι μηδενική.

Η δυναμοσειρά $\displaystyle\sum_{n=0}^{\infty}\frac{X^n}{n!}$ ορίζει, λοιπόν, μία συνάρτηση από τον ανοιχτό δίσκο $D(p^{-\frac{1}{p-1}}-)$ στο Ω_p που απεικονίζει το $x \in D(p^{-\frac{1}{p-1}}-)$ στο $\displaystyle\sum_{n=0}^{\infty}\frac{x^n}{n!}$. Αυτήν τη συνάρτηση θα τη συμβολίζουμε $\exp_p(X)$ και συνεπώς θα έχουμε $\exp_p(x) = \displaystyle\sum_{n=0}^{\infty}\frac{x^n}{n!}$ γιά κάθε $x \in D(p^{-\frac{1}{p-1}}-)$.

2.3 Η διωνυμική συνάρτηση.

Γιά κάθε $\alpha \in \Omega_p$, ορίζουμε την τυπική δυναμοσειρά $B_{\alpha,p}(X) \overset{\text{ορσ}}{=} 1 + \displaystyle\sum_{n=1}^{\infty}\frac{\alpha(\alpha-1)\cdot\ldots\cdot(\alpha-n+1)}{n!}X^n = \sum_{n=0}^{\infty}a_nX^n$, η οποία εναλλακτικώς συμβολίζεται και ως $(1+X)^{\alpha}$. Γιά τη μελέτη της σύγκλισής της θα διακρίνουμε κάποιες περιπτώσεις, ανάλογα με την τιμή $|\alpha|_p$, καθώς η ακτίνα σύγκλισής της εξαρτάται από την τιμή αυτή.

Έστω ότι $|\alpha|_p > 1$. Τότε καθώς γιά κάθε $i \in \mathbb{Z}$ ισχύει ότι $|\alpha - i|_p = |\alpha|_p$, έχουμε ότι $r = \dfrac{1}{\limsup\limits_{n\to\infty}|\frac{\alpha^n}{n!}|_p^{\frac{1}{n}}} = \frac{p^{-\frac{1}{p-1}}}{|\alpha|_p}$, αφού συμφωνα με τα παραπάνω $\limsup\limits_{n\to\infty}(\dfrac{1}{n!})^{\frac{1}{n}} = p^{\frac{1}{p-1}}$. Επιπλέον, αν $x \in \Omega_p$ με $|x|_p = \frac{p^{-\frac{1}{p-1}}}{|\alpha|_p}$, τότε

$$\lim_{\to\infty}|a_nx^n|_p = \lim_{n\to\infty}\frac{|\alpha|_p^n}{|n!|_p}\frac{p^{-\frac{1}{p-1}}}{|\alpha|_p^n} = p^{-\frac{s_n}{p-1}} \overset{n\to\infty}{\not\longrightarrow} 0,$$

πάλι συμφωνα με τα παραπάνω, συνεπώς η $1+\displaystyle\sum_{n=1}^{\infty}\frac{\alpha(\alpha-1)\cdot\ldots\cdot(\alpha-n+1)}{n!}x^n$ αποκλίνει γιά κάθε $x \in \Omega_p$ με $|x|_p = \frac{p^{-\frac{1}{p-1}}}{|\alpha|_p}$. Όταν λοιπόν $|\alpha|_p > 1$, ο δίσκος σύκλισης της $B_{\alpha,p}(X)$ είναι ο $D(\frac{p^{-\frac{1}{p-1}}}{|\alpha|_p}-)$.

Έστω τώρα ότι $|\alpha|_p \le 1$. Τότε γιά κάθε $i \in \mathbb{N}$, $|\alpha - i|_p \le 1$, άρα γιά κάθε $x \in \Omega_p$, $|a_nx^n|_p \le |\frac{x^n}{n!}|_p$. Από όσα είπαμε γιά την $\displaystyle\sum_{n=0}^{\infty}\frac{X^n}{n!}$ έπεται ότι η $B_{\alpha,p}(X)$ συγκλίνει τουλάχιστον στο δίσκο $D(p^{-\frac{1}{p-1}}-)$.

Στην περίπτωση που $|\alpha|_p \leq 1$ και ειδικότερα αν $\alpha \in \mathbb{Z}_p$, θα δείξουμε ότι $B_{\alpha,p}(X) \in \mathbb{Z}_p[[x]]$ και συνεπώς συγκλίνει τουλάχιστον στο δίσκο $D(1-)$.[3] Δηλαδή, πρέπει να δείξουμε ότι, αν $\alpha \in \mathbb{Z}_p$, τότε $\frac{\alpha(\alpha-1)\cdot\ldots\cdot(\alpha-n+1)}{n!} \in \mathbb{Z}_p$.

Αφού $\alpha \in \mathbb{Z}_p$, έχουμε ότι $\alpha = b_0+b_1p+b_2p^2+\ldots$ με τους $b_i \in \{0,1,\ldots,p-1\}$. Ειδικότερα, $\alpha = b+p^n\beta$, όπου $b \in \mathbb{Z}$ και $\beta \in \mathbb{Z}_p$. Άρα $\alpha(\alpha-1)\cdot\ldots\cdot(\alpha-n+1) = b(b-1)\cdot\ldots\cdot(b-n+1)+p^n\gamma$ με $\gamma \in \mathbb{Z}_p$. Έπεται ότι $\frac{\alpha(\alpha-1)\cdot\ldots\cdot(\alpha-n+1)}{n!} = \binom{b}{n} + \frac{p^n}{n!}\gamma$. Αλλά τώρα $\binom{b}{n} \in \mathbb{Z}$ και $\frac{p^n}{n!} \in \mathbb{Z}_p$, αφού $\mathrm{ord}_p(\frac{p^n}{n!}) = n - \mathrm{ord}_p(n!) > n - \frac{n}{p-1} \geq 0$. Άρα $\frac{\alpha(\alpha-1)\cdot\ldots\cdot(\alpha-n+1)}{n!} \in \mathbb{Z}_p$.

[3] Αν $f = \sum_{n=0}^{\infty} a_n X^n \in \mathbb{Z}_p[[X]]$ και $x \in \Omega_p$ με $|x|_p < 1$, τότε $|a_n x^n|_p \leq |x|_p^n \overset{n\to\infty}{\longrightarrow} 0$, άρα η $f(X)$ συγκλίνει τουλάχιστον στον δίσκο $D(1-)$.

3 Δυναμοσειρές πολλών μεταβλητών.

Στην ενότητα αυτή γενικεύουμε την έννοια των τυπικών δυναμοσειών από μία σε περισσότερες μεταβλητές. Διατυπώνουμε και αποδεικνύουμε μία σειρά από λήμματα, αντίστοιχα αυτών της ενότητας 1, και εξετάζουμε κάποιες ιδιότητες που τις αφορούν.

Έστω R ακέραια περιοχή. Ορίζουμε ως το σύνολο των τυπικών δυναμοσειρών n μεταβλητών με συντελεστές από την R, και το συμβολίζουμε $R[[X_1,\ldots,X_n]]$, το συνολο $\{f \ : \ f : \mathbb{N}_0^n \to R\}$. Το τυπικό στοιχείο $f \in R[[X_1,\ldots,X_n]]$ το συμβολίζουμε $\sum r_{i_1,\ldots i_n} X_1^{i_1} \cdot \ldots \cdot X_n^{i_n}$.

Μεταξύ των στοιχείων του $R[[X_1,\ldots,X_n]]$ ορίζουμε πρόσθεση και πολλαπλασιασμό ως εξής : Αν $f, g \in R[[X_1,\ldots,X_n]]$ με $f = \sum r_{i_1,\ldots i_n} X_1^{i_1} \cdot \ldots \cdot X_n^{i_n}$ και $g = \sum s_{i_1,\ldots i_n} X_1^{i_1} \cdot \ldots \cdot X_n^{i_n}$, τότε ορίζουμε

$$f + g = \sum (r_{i_1,\ldots i_n} + s_{i_1,\ldots i_n}) X_1^{i_1} \cdot \ldots \cdot X_n^{i_n}$$

και

$$f \cdot g = \sum t_{i_1,\ldots,i_n} X_1^{i_1} \cdot \ldots \cdot X_n^{i_n},$$

όπου $t_{i_1,\ldots,i_n} = \sum\limits_{\substack{(j_1,\ldots,j_n),(k_1,\ldots,k_n) \text{ με} \\ (j_1,\ldots,j_n)+(k_1,\ldots,k_n)= \\ (i_1,\ldots,i_n)}} r_{j_1,\ldots,j_n} s_{k_1,\ldots,k_n}.$

Επίσης, γιά κάθε $f = \sum r_{i_1,\ldots i_n} X_1^{i_1} \cdot \ldots \cdot X_n^{i_n} \in R[[X_1,\ldots,X_n]]$ ορίζουμε ως βαθμό του f, και συμβολίζουμε με $\mathrm{ord} f$, τον αριθμό

$$d \overset{\text{ορσ}}{=} \min\{d' \in \mathbb{N}_0 \ : \ d' = i_1 + \ldots + i_n \text{γιά κάποιο } r_{i_1,\ldots i_n} \neq 0\},$$

κάνοντας την σύμβαση ότι $f = 0 \Leftrightarrow \mathrm{ord} f = \infty$.
Κατόπιν των παραπάνω είναι φανερό ότι το σύνολο $R[[X_1,\ldots,X_n]]$ έχει δομή δακτυλίου.

Σταθεροποιούμε $\mathbb{R}^+ \ni \rho < 1$ και ορίζουμε τη συνάρτηση $|\cdot|_{X_1,\ldots,X_n} : R[[X_1,\ldots,X_n]] \to \mathbb{R}$ ως εξής : Αν $f = \sum r_{i_1,\ldots i_n} X_1^{i_1} \cdot \ldots \cdot X_n^{i_n} \in R[[X_1,\ldots,X_n]]$, τότε $|f|_{X_1,\ldots,X_n} \overset{\text{ορσ}}{=} \rho^{\mathrm{ord} f}$.

Λήμμα 3.1 *Η* $|\cdot|_{X_1,\ldots,X_n}$ *είναι μία μη αρχιμήδεια νόρμα του δακτυλίου* $R[[X_1,\ldots,X_n]]$.

Απόδειξη : $i)$ Έχουμε εξ' ορισμού $|f|_{X_1,\ldots,X_n} = 0 \Leftrightarrow \rho^{\mathrm{ord} f} = 0 \Leftrightarrow \mathrm{ord} f = \infty \Leftrightarrow f = 0$

$ii)$Έστω $f = \sum r_{i_1,\ldots i_n} X_1^{i_1} \cdot \ldots \cdot X_n^{i_n}$ και $g = \sum s_{i_1,\ldots i_n} X_1^{i_1} \cdot \ldots \cdot X_n^{i_n}$ στον $R[[X_1,\ldots,X_n]]$, με $\mathrm{ord} f = d_1$ και $\mathrm{ord} g = d_2$. Θα δείξουμε ότι $\mathrm{ord} fg = \mathrm{ord} f + \mathrm{ord} g = d_1 + d_2$. Αν αυτό δειχθεί, τότε θα έχουμε :

$$|fg|_{X_1,\ldots,X_n} = \rho^{\mathrm{ord} fg} = \rho^{\mathrm{ord} f + \mathrm{ord} g} = \rho^{\mathrm{ord} f} \rho^{\mathrm{ord} g} = |f|_{X_1,\ldots,X_n} |g|_{X_1,\ldots,X_n}.$$

Έστω λοιπόν ότι $f \cdot g = \sum t_{i_1,\ldots,i_n} X_1^{i_1} \cdot \ldots \cdot X_n^{i_n}$.
Ισχύει ότι $\mathrm{ord}(fg) \geq d_1 + d_2$.
Πράγματι, αφού όλοι οι όροι της f είναι βαθμού $\geq d_1$ και όλοι οι όροι της g είναι βαθμού $\geq d_2$, έπεται ότι όλοι οι όροι της $f \cdot g$ είναι βαθμού $\geq d_1 + d_2$ άρα και ο ελαχιστοβάθμιος όρος της $f \cdot g$ είναι βαθμού $d_1 + d_2$.
Επιπλέον ισχύει ότι το πολυώνυμο

$$\Big(\sum_{j_1+\ldots+j_n=d_1} r_{j_1,\ldots,j_n} X_1^{j_1} \cdot \ldots \cdot X_n^{j_n}\Big)\Big(\sum_{k_1+\ldots+k_n=d_2} s_{k_1,\ldots,k_n} X_1^{k_1} \cdot \ldots \cdot X_n^{k_n}\Big),$$

που είναι "τμήμα" της σειράς $f \cdot g$, είναι μη μηδενικό (άρα βαθμού $d_1 + d_2$). Πράγματι, αν ήταν μηδενικό, τότε, αφού ο R είναι ακέραια περιοχή, έπεται και ότι το $R[X_1,\ldots,X_n]$ είναι ακέραια περιοχή, συνεπώς,

$$\text{ή} \sum_{j_1+\ldots+j_n=d_1} r_{j_1,\ldots,j_n} X_1^{j_1} \cdot \ldots \cdot X_n^{j_n} = 0,$$

$$\text{είτε} \sum_{k_1+\ldots+k_n=d_2} s_{k_1,\ldots,k_n} X_1^{k_1} \cdot \ldots \cdot X_n^{k_n} = 0.$$

Όμως, καθώς $\mathrm{ord} f = d_1$ και $\mathrm{ord} g = d_2$, καμμία όμως από τις παραπάνω περιπτώσεις δεν είναι δυνατή. Τα παραπάνω δείχνουν ότι $\mathrm{ord}(f \cdot g) = d_1 + d_2$.
$iii)$Θα δείξουμε ότι $\mathrm{ord}(f+g) \geq \min(\mathrm{ord} f, \mathrm{ord} g)$. Αν αυτό δειχθεί, τότε θα έχουμε : $|f+g|_{X_1,\ldots,X_n} = \rho^{\mathrm{ord}(f+g)} \leq \rho^{\min(\mathrm{ord} f, \mathrm{ord} g)} = \max(\rho^{\mathrm{ord} f}, \rho^{\mathrm{ord} g}) = \max(|f|_{X_1,\ldots,X_n}, |g|_{X_1,\ldots,X_n})$.
Αν $d_1 \neq d_2$, τότε προφανώς $\mathrm{ord}(f+g) = \min(d_1, d_2)$. Αν $d_1 = d_2$, τότε $\mathrm{ord}(f+g) \geq \min(d_1, d_2)$, καθώς ενδέχεται να έχουμε $r_{i_1,\ldots,i_n} + s_{i_1,\ldots,i_n} = 0$ γιά κάθε μη μηδενικούς $r_{i_1,\ldots,i_n}$, $s_{i_1,\ldots,i_n}$ με $i_1 + \ldots + i_n = d_1 + d_2$. Συνολικά λοιπόν $\mathrm{ord}(f+g) \geq \min(d_1, d_2)$.

Λήμμα 3.2 *Ο δακτύλιος $R[[X_1,\ldots,X_n]]$ είναι πλήρης ως προς την $|\cdot|_{X_1,\ldots,X_n}$.*

Απόδειξη : Έστω $\{f_m\}_{m\in\mathbb{N}_0}$ με $f_m = \sum r_{m_{i_1,\ldots,i_n}} X_1^{i_1},\ldots,X_n^{i_n}$ ακολουθία Cauchy στοιχείων του $R[[X_1,\ldots,X_n]]$. Θα δείξουμε ότι $\mathrm{ord}(f_m - f) \stackrel{m\to\infty}{\longrightarrow} \infty$ γιά κάποιο $f = \sum r_{i_1,\ldots,i_n} X_1^{i_1},\ldots,X_n^{i_n} \in R[[X_1,\ldots,X_n]]$. Αφού η $\{f_m\}_{m\in\mathbb{N}_0}$ είναι Cauchy έχουμε ότι γιά κάθε $M \geq 0$ μπορούμε να βρούμε m_M τ.ώ. αν $m_2 > m_1 \geq m_M$, τότε $\mathrm{ord}(f_{m_2} - f_{m_1}) > M$. Ορίζουμε το $f = \sum r_{i_1,\ldots,i_n} X_1^{i_1},\ldots,X_n^{i_n}$ ως εξής : Γιά $M = 0, 1, \ldots$ θέτουμε

$$m_M^{'} = \min\{m_M \ : \ m_2 > m_1 \geq m_M \Rightarrow \mathrm{ord}(f_{m_2} - f_{m_1}) > M\}.$$

Παρατηρούμε ότι, αν $M_1 < M_2$, τότε $m_{M_1}^{'} \leq m_{M_1}^{'}$.
Γιά κάθε $(i_1,\ldots,i_n)$ με $i_1+\ldots+i_n \leq M$, θέτω $r_{i_1,\ldots,i_n} := r_{m'_{M\, i_1,\ldots,i_n}}$. Τα $r_{i_1,\ldots,i_n}$ έτσι ορίζονται καλώς, διότι αν $M_1 < M_2$, τότε $m_{M_1}^{'} \leq m_{M_2}^{'}$, άρα $\mathrm{ord}(f_{m'_{M_2}} - f_{m'_{M_1}}) > M_1$, δηλαδή $r_{m'_{M_2\, i_1,\ldots,i_n}} = r_{m'_{M_1\, i_1,\ldots,i_n}}$ γιά κάθε $(i_1,\ldots,i_n)$ με $i_1+\ldots+i_n \leq M$.
Θα δείξουμε τώρα ότι $\mathrm{ord}(f_m - f) \stackrel{m\to\infty}{\longrightarrow} \infty$.
Έστω $M \geq 0$. Αν $m \geq m_M^{'}$ έχουμε : $\mathrm{ord}(f_m - f_{m'_M}) > M$ από την ιδιότητα του $m_M^{'}$, αλλά και $\mathrm{ord}(f_{m'_M} - f) > M$ από τον ορισμό του f. Συνεπώς

$$\begin{aligned}\mathrm{ord}(f_m - f) = \mathrm{ord}(f_m - f_{m'_M} + f_{m'_M} - f)&\\ &\geq \min(\mathrm{ord}(f_m - f_{m'_M}), \mathrm{ord}(f_{m'_M} - f))\\ &> M.\end{aligned}$$

Λήμμα 3.3 *Έστω $\{f_m\}_{m\in\mathbb{N}_0}$ ακολουθία στοιχείων του $R[[X_1,\ldots,X_n]]$ με $\mathrm{ord} f_m = 0$ γιά κάθε $m \geq 0$. Τότε το γινόμενο $\prod_{i=0}^{\infty} f_i$ υπάρχει στον $R[[X_1,\ldots,X_n]]$ αν και μόνο αν $\mathrm{ord}(f_m - 1) \stackrel{m\to\infty}{\longrightarrow} \infty$.*

Απόδειξη : Κατ΄ αρχάς παρατηρούμε ότι, αν $f,\ g \in R[[X_1,\ldots,X_n]]$ με $\mathrm{ord} f = 0$, τότε $\mathrm{ord}(gf - f) > M$ αν και μόνο εάν $\mathrm{ord}(g-1) > M$. Πράγματι

$$\mathrm{ord}(fg - f) > M \Leftrightarrow \mathrm{ord} f + \mathrm{ord}(g-1) > M \Leftrightarrow 0 + \mathrm{ord}(g-1) > M.$$

Θέτουμε $f_m = \sum r_{m_{i_1,\ldots,i_n}} X_1^{i_1},\ldots,X_n^{i_n}$. Έστω ότι $\mathrm{ord}(\prod_{i=0}^{m} f_i - f) \stackrel{m\to\infty}{\longrightarrow} \infty$ γιά κάποιο $f = \sum r_{i_1,\ldots,i_n} X_1^{i_1},\ldots,X_n^{i_n} \in R[[X_1,\ldots,X_n]]$, και έστω $M \geq 0$. Βρίσκουμε $m_M \in \mathbb{N}_0$ τ.ώ. αν $m \geq m_M$, τότε $\mathrm{ord}(\prod_{i=0}^{m} f_i - f) > M$.

Γιά κάθε $n \geq 0$ έχουμε:

$$
\begin{aligned}
\mathrm{ord}(f_{m_M+n+1}\prod_{i=0}^{m_M+n} f_i - \prod_{i=0}^{m_M+n} f_i) = \\
& \mathrm{ord}(f_{m_M+n+1}\prod_{i=0}^{m_M+n} f_i - f + f - \prod_{i=0}^{m_M+n} f_i) \\
& \geq \min(f_{m_M+n+1}\mathrm{ord}(\prod_{i=0}^{m_M+n} f_i - f), \mathrm{ord}(\prod_{i=0}^{m_M+n} f_i - f)) \\
& > M \,,
\end{aligned}
$$

καθώς

$$
\mathrm{ord}(\prod_{i=0}^{m_M+n+1} f_i - f), \mathrm{ord}(\prod_{i=0}^{m_M+n} f_i - f) > M \,.
$$

Από την παρατήρηση έπεται ότι $\mathrm{ord}(f_{m_M+n+1} - 1) > M$, άρα λοιπόν, γιά κάθε $m \geq m_M + 1$, έχουμε $\mathrm{ord}(f_m - 1) > M$.
Αντίστροφα, έστω ότι $\mathrm{ord}(f_m - 1) \overset{m\to\infty}{\longrightarrow} \infty$. Θα δείξουμε ότι η ακολουθία $\{\prod_{i=0}^{m} f_i\}_{m\in\mathbb{N}_0}$ είναι Cauchy. Έστω $M > 0$. Βρίσκουμε $m_M \in \mathbb{N}_0$ τ.ώ. αν $m \geq m_M$, τότε $\mathrm{ord}(f_m - 1) > M$. Έστω $m_2 > m_1 \geq m_M$. Τότε :

$$
\begin{aligned}
\mathrm{ord}(\prod_{i=0}^{m_2} f_i - \prod_{i=0}^{m_1} f_i) = \mathrm{ord}\{\prod_{i=0}^{m_1} f_i(\prod_{i=m_1+1}^{m_2} f_i - 1)\} = \\
& \mathrm{ord}(\prod_{i=0}^{m_1} f_i) + \mathrm{ord}\{\prod_{m_1+1}^{m_2} f_i - \prod_{m_1+1}^{m_2-1} f_i + \prod_{m_1+1}^{m_2-1} f_i - \prod_{m_1+1}^{m_2-2} f_i + \prod_{m_1+1}^{m_2-2} f_i - \\
& \qquad \ldots + f_{m_1+1} - f_{m_1+1} - 1\} \\
& \geq \mathrm{ord}(\prod_{i=0}^{m_1} f_i) + \min\{\mathrm{ord}(f_{m_2}\prod_{i=m_1+1}^{m_2-1} f_i - \prod_{i=m_1+1}^{m_2-1} f_i), \ldots, \mathrm{ord}(f_{m_1+2}f_{m_1+1} - f_{m_1+1}), \\
& \qquad , \mathrm{ord}(f_{m_1+1} - 1)\} \\
& \geq \min(\mathrm{ord}(f_{m_2}\prod_{i=m_1+1}^{m_2-1} f_i - \prod_{i=m_1+1}^{m_2-1} f_i), \ldots, \mathrm{ord}(f_{m_1+2}f_{m_1+1} - f_{m_1+1}), \\
& \qquad , \mathrm{ord}(f_{m_1+1} - 1)\} \\
& > M
\end{aligned}
$$

λόγω της παρατήρησης, καθώς $\mathrm{ord}(f_m - 1) > M$ γιά $m = m_1 + 1, \ldots, m_2$ από την υπόθεση. Συνεπώς η ακολουθία $\{\prod_{i=0}^{m} f_i\}_{m \in \mathbb{N}_0}$ είναι Cauchy.

Λήμμα 3.4 *Έστω* $f = \sum r_{j_1,\ldots,j_n} X_1^{j_1} \ldots X_n^{j_n} \in R[[X_1, \ldots, X_n]]$. *Ορίζουμε* $f_d = \sum r_{j_1,\ldots,j_n} X_1^{j_1}, \ldots, X_n^{j_n}$ *με* $r_{j_1,\ldots,j_n} = 0$ *γιά κάθε* $(j_1, \ldots, j_n)$ *με* $j_1 + \ldots + j_n > d$. *Ακόμα, γιά* $k = 1, \ldots, n$, *έστω* $g_k \in R[[X_1, \ldots, X_n]]$ *με* $\mathrm{ord}(g_k) > 0$. *Τότε η ακολουθία* $\{f_d(g_1, \ldots, g_n)\}_{d \in \mathbb{N}_0}$ *είναι* Cauchy. [4]

Απόδειξη : Γιά κάθε $k = 1, \ldots, n$ θέτουμε $g_k = \sum s_{k_{i_1,\ldots,i_n}} X_1^{i_1} \ldots X_n^{i_n}$. Έστω $M \geq 0$. Αρκεί να δείξουμε ότι αν $d > M$, τότε $\mathrm{ord}(f_d(g_1, \ldots, g_n) - f_M(g_1, \ldots, g_n)) > M$, διότι αν το παραπάνω ισχύει και $d_2 > d_1 \geq M + 1$, τότε

$$\begin{array}{rcl} \mathrm{ord}(f_{d_2}(g_1, \ldots, g_n) - f_{d_1}(g_1, \ldots, g_n)) & \geq & \\ \min\{\mathrm{ord}(f_{d_2}(g_1, \ldots, g_n) - f_M(g_1, \ldots, g_n)) & , & \mathrm{ord}(f_{d_1}(g_1, \ldots, g_n) - f_M(g_1, \ldots, g_n))\} \\ & > & M\ . \end{array}$$

Έστω λοιπόν $d > M$ και έστω $(j_1, \ldots, j_n)$ με $j_1 + \ldots + j_n \leq M$. Θα δείξουμε ότι οι αντίστοιχοι συντελεστές των $f_d(g_1, \ldots, g_n)$ και $f_M(g_1, \ldots, g_n)$ είναι ίσοι. Έχουμε ότι :

$$f_M(g_1, \ldots, g_n) =$$

$$\sum r_{j_1,\ldots,j_n} (\sum s_{1_{i_1 \ldots i_n}} X_1^{i_1} \ldots X_n^{i_n})^{j_1} \ldots (\sum s_{k_{i_1,\ldots,i_n}} X_1^{i_1} \ldots X_n^{i_n})^{j_n},$$

όπου $r_{j_1,\ldots,j_n} = 0$ γιά κάθε $(j_1, \ldots, j_n)$ με $j_1 + \ldots + j_n > M$, και

$$f_d(g_1, \ldots, g_n) = f_M(g_1, \ldots, g_n) + A,$$

όπου

$$A \overset{\text{ορσ}}{=} \sum r_{j_1,\ldots,j_n} (\sum s_{1_{i_1 \ldots i_n}} X_1^{i_1} \ldots X_n^{i_n})^{j_1} \ldots (\sum s_{k_{i_1,\ldots,i_n}} X_1^{i_1} \ldots X_n^{i_n})^{j_n}$$

με $r_{j_1,\ldots,j_n} = 0$ γιά κάθε $(j_1, \ldots, j_n)$ με $j_1 + \ldots + j_n \leq M$ ή $j_1 + \ldots + j_n > d$. Έστω $k_{j_1,\ldots,j_n}$ ο αντίστοιχος συντελεστής του $f_M(g_1, \ldots, g_n)$. Τότε ο αντίστοιχος συντελεστής του $f_d(g_1, \ldots, g_n)$ θα είναι $k_{j_1,\ldots,j_n} + t_{j_1,\ldots,j_n}$, όπου $t_{j_1,\ldots,j_n}$ είναι ο αντίστοιχος συντελεστής στο A. Όμως, καθώς $\mathrm{ord}(\sum s_{k_{i_1,\ldots,i_n}} X_1^{i_1} \ldots X_n^{i_n}) \geq 1$ γιά κάθε $k = 1, \ldots, n$, κάθε προσθεταίος του A είναι στοιχείο του $R[[X_1, \ldots, X_n]]$

[4] Παρατηρούμε ότι γιά κάθε $d \geq 0$, το $f_d(g_1, \ldots, g_n)$ ορίζεται καλώς, αφού είναι πεπερασμένο άθροισμα στοιχείων του $R[[X_1, \ldots, X_n]]$.

με βαθμό $\geq j_1+\ldots+j_n > M$, άρα $t_{j_1,\ldots,j_n} = 0$. Έπεται λοιπόν ότι οι αντίστοιχοι συντελεστές των $f_M(g_1,\ldots,g_n)$ και $f_d(g_1,\ldots,g_n)$ είναι ίσοι.

Θεωρούμε γνωστό από την Ανάλυση ότι ισχύουν οι παρακάτω δυο προτάσεις:

Πρόταση 3.1 *Έστω $f, f_d, g_1, \ldots, g_k$ όπως στην εκφώνηση του λήμματος 3.4, όπου τώρα $R = \mathbb{R}$. Έστω ακόμα ότι γιά κάποιο $\epsilon > 0$ οι δυναμοσειρές $f, g_1, \ldots, g_k$ είναι απολύτως συγκλίνουσες γιά $X_i = x_i$ στο διάστημα $[-\epsilon, \epsilon] \subseteq \mathbb{R}$. Τότε η δυναμοσειρά $f \circ g$ είναι απολύτως συγκλίνουσα στο $[-\epsilon', \epsilon'] \subseteq [-\epsilon, \epsilon]$ γιά κάποιο $\epsilon' > 0$.*

Πρόταση 3.2 *Αν, υπό τις προυποθέσεις του προηγούμενου λήμματος, $f \circ g(x_1, \ldots, x_n) = 0$ γιά κάθε $(x_1, \ldots, x_n) \in [-\epsilon, \epsilon]^n$, τότε η $f \circ g$ είναι η μηδενική δυναμοσειρά στο $\mathbb{R}[X_1, \ldots, X_n]$.*

Στα παρακάτω το K συμβολίζει ένα σώμα χαρακτηριστικής 0, οπότε το K είναι επέκταση του σώματος $\mathbb{Q}$. Γιά n ακέραιο ≥ 1 ορίζουμε τις εξής δυναμοσειρές του $K[[X_1, \ldots, X_n]]$:

$$\log(1+X_i) \overset{\text{ορσ}}{=} \sum_{k=1}^{\infty} X_i^k, \qquad \exp X_i \overset{\text{ορσ}}{=} \sum_{k=0}^{\infty} \frac{1}{k!} X_i^k \qquad (i = 1, \ldots, n),$$

$$\log \prod_{i=1}^{n} (1+X_i) \overset{\text{ορσ}}{=} \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k} \big((1+X_1) \cdot \ldots \cdot (1+X_n)\big)^k$$

$$\exp \sum_{i=1}^{n} X_i \overset{\text{ορσ}}{=} \sum_{k=0}^{\infty} \frac{1}{k!} (X_1 + \ldots + X_n)^k.$$

Γιά κάθε $f, g \in K[[X_1, \ldots, X_n]]$ με $\mathrm{ord} f, \mathrm{ord} g > 0$,

$$B_{g,p}(f) \overset{\text{ορσ}}{=} (1+f)^g \overset{\text{ορσ}}{=} 1 + \sum_{k=1}^{\infty} \frac{g(g-1) \cdot \ldots \cdot (g-k+1)}{k!} f^k.$$

Σύμφωνα με τη θεωρία που μέχρι τώρα εκθέσαμε, όλες οι παραπάνω δυναμοσειρές είναι καλώς ορισμένα στοιχεία του $K[[X_1, \ldots, X_n]]$. Όλες αυτές τις σειρές μπορούμε να τις δούμε και ως τυπικές δυναμοσειρές με συντελεστές από το $\mathbb{Q}$, και όπως θα δούμε σε κάθε περίπτωση, κάθε μία από αυτές τις σειρές ορίζει απολύτως συγκλίνουσα δυναμοσειρά n μεταβλητών σε κατάλληλο ϵ-κύβο του $\mathbb{R}^n$. Εδώ, "ϵ-κύβος του $\mathbb{R}^n$" (γιά $\epsilon > 0$) σημαίνει το σύνολο

$$\{(x_1,\ldots,x_n)\in\mathbb{R}^n \ : \ |x_k|<\epsilon \text{ γιά όλα τα } k=1,\ldots,n\}.$$

Από τα συμφραζόμενα θα είναι σαφές πότε μία δυναμοσειρά με ρητούς συντελεστές τη βλέπουμε ως στοιχείο του $K[[X_1,\ldots,X_n]]$ και πότε ως συνάρτηση n μεταβλητών ορισμένη σε κάποιο ϵ-κύβο του $\mathbb{R}^n$.

ΤΑΥΤ. 3.1 *Γιά κάθε* $n\geq 1$, *ισχύει* $\displaystyle\sum_{i=1}^{n}\log(1+X_i)=\log(\prod_{i=1}^{n}(1+X_i))$.

Απόδειξη : Θα δείξουμε ότι $\log(1+X_1)+\log(1+X_2)=\log((1+X_1)(1+X_2))$, οπότε, γιά $n>2$, το ζητούμενο έπεται από απλή επαγωγή. Δουλεύουμε στο δακτύλιο $K[[X_1,\ldots,X_n]]$. Θεωρούμε τη δυναμοσειρά $f=\displaystyle\sum_{n=1}^{\infty}(-1)^{n+1}\frac{X_1^n+X_2^n-X_3^n}{n}$. Ως συνάρτηση ορισμένη στον $\mathbb{R}^3$, η f είναι απολύτως συγκλίνουσα στον $\frac{1}{3}-$κύβο διότι γιά κάθε (x_1,x_2,x_3) στον $\frac{1}{3}-$κύβο έχουμε : $|(-1)^{n+1}\frac{x_1^n+x_2^n-x_3^n}{n}|\leq\frac{1}{3^{n-1}n}$ και η $\displaystyle\sum_{n=1}^{\infty}\frac{1}{3^{n-1}n}$ συγκλίνει. Θεωρούμε ακόμα τις δυναμοσειρές $g_1=X_1$, $g_2=X_2$, $g_3=X_1+X_2+X_1X_2$, οι οποίες είναι απολύτως συγκλίνουσες στον $\frac{1}{3}-$κύβο του $\mathbb{R}^3$. Από την πρόταση 3.1, γιά κάποιο $0<\epsilon^{'}\leq\epsilon$, αν (x_1,x_2,x_3) στον $\epsilon^{'}$-κύβο, η $f(g_1(x_1,x_2,x_3),g_2(x_1,x_2,x_3),g_3(x_1,x_2,x_3))$ είναι συγκλίνουσα. Όμως

$$f(g_1(x_1,x_2,x_3),g_2(x_1,x_2,x_3),g_3(x_1,x_2,x_3))=f(x_1,x_2,x_1+x_2+x_1x_2)=$$

$$\log(1+x_1)+\log(1+x_2)-\log(1+x_1+x_2+x_2x_2)=$$

$$\log(1+x_1)+\log(1+x_2)-\log((1+x_1)(1+x_2))=0.$$

Άρα από το λήμμα 3.2 όλοι οι συντελεστές της δυναμοσειράς $f(X_1,X_2,X_1+X_2+X_1X_2)$ είναι 0. Αν κάνουμε δηλαδή πράξεις στο άθροισμα

$$\sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n}(X_1^n+X_2^n-(X_1+X_2+X_1X_2)^n), \tag{5}$$

θα βρούμε ότι οι συντελεστές του $X_1^iX_2^j$ γιά κάθε $(i,j)\in\mathbb{N}^2$ είναι μηδέν. Στις πράξεις όμως αυτές υπεισέρχονται μόνο οι ρητοί και οι ιδιότητές τους, συνεπώς, αν δούμε την 5 ως δυναμοσειρά με συντελεστές από οποιαδήποτε επέκταση του $\mathbb{Q}$ θα προκύψει πάλι το ίδιο συμπέρασμα.
Καταλήγουμε λοιπόν στο συμπέρασμα ότι, στον $K[[X_1,X_2]]$ ισχύει η ταυτότητα

$$\sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n}X_1^n+\sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n}X_2^n=\sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n}(X_1+X_2+X_1X_2)^n,$$

δηλαδή

$$\log(1+X_1)+\log(1+X_2)=\log((1+X_1)(1+X_2)).$$

ΤΑΥΤ. 3.2 *Γιά κάθε* $n\geq 1$, *ισχύει* $\prod_{i=1}^{n}\exp(X_i)=\exp(\sum_{i=1}^{n}X_i)$.

Απόδειξη :Θα δείξουμε ότι $\exp(X_1)\exp(X_2)=\exp(X_1+X_2)$, οπότε γιά $n>2$, το ζητούμενο έπεται από απλή επαγωγή. Δουλεύουμε στον $K[[X_1,X_2,X_3]]$. Θεωρούμε τη δυναμοσειρά $f=\sum_{n=0}^{\infty}(\sum_{k=0}^{n}\frac{X_1^k}{k!}\frac{X_2^{n-k}}{(n-k)!}-\frac{X_3^n}{n!})$ η οποία είναι απολύτως συγκλίνουσα στον $\frac{1}{3}-$κύβο του $\mathbb{R}^3$, διότι, γιά κάθε (x_1,x_2,x_3) στον $\frac{1}{3}-$κύβο έχουμε : $|\sum_{k=0}^{n}\frac{x_1^k}{k!}\frac{x_2^{n-k}}{(n-k)!}-\frac{x_3^n}{n!}|\leq\frac{n+2}{3^n}$ και η $\sum_{n=1}^{\infty}\frac{n+2}{3^n}$ συγκλίνει. Θεωρούμε ακόμα τις δυναμοσειρές $g_1=X_1$, $g_2=X_2$, $g_3=X_1+X_2$, οι οποίες είναι απολύτως συγκλίνουσες στον $\frac{1}{3}$-κύβο του $\mathbb{R}^3$. Από την πρόταση 3.1, γιά κάποιο $\epsilon'\leq\frac{1}{3}$, αν (x_1,x_2,x_3) στον ϵ'-κύβο, η $f(g_1(x_1,x_2,x_3),g_2(x_1,x_2,x_3),g_3(x_1,x_2,x_3))$ είναι συγκλίνουσα. Όμως

$$f(g_1(x_1,x_2,x_3),g_2(x_1,x_2,x_3),g_3(x_1,x_2,x_3))=$$

$$f(x_1,x_2,x_1+x_2)=\exp(x_1)+\exp(x_2)-\exp(x_1+x_2)=0.$$

Άρα από την πρόταση 3.2, όλοι οι συντελεστές της δυναμοσειράς $f(X_1,X_2,X_1+X_2)$ είναι 0. Τώρα με επιχείρημα όμοιο με αυτό του ΤΑΥΤ. 3.1, καταλήγουμε στο συμπέρασμα ότι στον $K[[X_1,X_2]]$ ισχύει η ταυτότητα

$$\sum_{n=0}^{\infty}(\sum_{k=0}^{n}\frac{X_1^k}{k!}\frac{X_2^{n-k}}{(n-k)!})=\sum_{n=0}^{\infty}\frac{X_1^n}{n!}\sum_{n=0}^{\infty}\frac{X_2^n}{n!}=\sum_{n=0}^{\infty}\frac{(X_1+X_2)^n}{n!},$$

δηλαδή

$$\exp(X_1)\cdot\exp(X_2)=\exp(X_1+X_2).$$

ΤΑΥΤ. 3.3 $\log(\exp(X))=X$.

Απόδειξη : Δουλεύουμε στον $K[[X_1,X_2]]$. Θεωρούμε τη δυναμοσειρά $f=\sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n}X_1^n-X_2$, η οποία είναι απολύτως συγκλίνουσα στον $\frac{1}{3}-$κύβο του $\mathbb{R}^2$, διότι, αν $|x_1|\leq\frac{1}{3}$, η $\sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n}x_1^n$ συγκλίνει απολύτως. Θεωρούμε ακόμα τις δυναμοσειρές $g_1=\sum_{n=1}^{\infty}\frac{X_1^n}{n!}$, $g_2=X_1$, οι οποίες είναι απολύτως συγκλίνουσες στον $\frac{1}{3}$-κύβο του $\mathbb{R}^2$. Από την πρόταση 3.1, γιά κάποιο $\epsilon^{'}\leq\frac{1}{3}$, αν (x_1,x_2) στον $\epsilon^{'}$-κύβο, η $f(g_1(x_1,x_2),g_2(x_1,x_2))$ είναι συγκλίνουσα. Όμως

$$f(g_1(x_1,x_2),g_2(x_1,x_2))=f(\exp(x_1)-1,x_1)=$$

$$\sum_{n=1}^{\infty}\frac{(-1)^n}{n}[\exp(x_1)-1]^n-x_1=\log(\exp(x_1))-x_1=0.$$

Άρα από την πρόταση 3.2 όλοι οι συντελεστές της δυναμοσειράς $f(g_1(X_1,X_2),X_1)=\log[1+(\exp(X_1)-1)]-X_1=\log(\exp(X_1))-X_1$ είναι 0. Έπεται λοιπόν, όμοια με πριν, ότι ισχύει η ταυτότητα

$$\log(\exp(X))=X.$$

ΤΑΥΤ. 3.4 $\exp(\log(1+X))=1+X$.

Απόδειξη : Δουλεύουμε στον $K[[X_1,X_2]]$. Θεωρούμε τη δυναμοσειρά $f=\sum_{n=0}^{\infty}\frac{X_1^n}{n!}-X_2$, η οποία είναι απολύτως συγκλίνουσα στον $\frac{1}{3}-$κύβο του $\mathbb{R}^2$. Θεωρούμε ακόμα τις δυναμοσειρές $g_1=\sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n}X_1^n$, $g_2=1+X_1$ οι οποίες είναι απολύτως συγκλίνουσες στον $\frac{1}{3}-$κύβο του $\mathbb{R}^2$. Από την πρόταση 3.1, γιά κάποιο $\epsilon^{'}\leq\frac{1}{3}$, αν (x_1,x_2) στον $\epsilon^{'}$-κύβο, η $f(g_1(x_1,x_2),g_2(x_1,x_2))$ είναι συγκλίνουσα. Όμως

$$f(g_1(x_1,x_2),g_2(x_1,x_2))=f(\log(1+x_1),1+x_1)=$$

$$\sum_{n=1}^{\infty}\frac{1}{n!}[\log(1+x_1)]^n-(1+x_1)=\exp(\log(1+x_1))-(1+x_1)=0.$$

Άρα από την πρόταση 3.2, όλοι οι συντελεστές της δυναμοσειράς $f(g_1(X_1,X_2),g_2(X_1,X_2))=\exp(\log(1+X_1))-(1+X_1)$ είναι 0. Έπεται λοιπόν, όμοια με πριν, ότι ισχύει η ταυτότητα

$$\exp(\log(1+X)) = 1+X.$$

ΤΑΥΤ. 3.5 *Γιά κάθε* $m \in \mathbb{Z}^*$, *ισχύει* $[(1+X)^{\frac{1}{m}}]^m = 1+X$.

Απόδειξη : Δουλεύουμε στον $K[[X_1, X_2]]$. Θεωρούμε τη δυναμοσειρά $f = X_1^m - X_2$. Η f είναι απολύτως συγκλίνουσα στον $\frac{1}{3}$−κύβο του $\mathbb{R}^2$. Θεωρούμε ακόμα τις δυναμοσειρές $g_1 = (1+X_1)^{\frac{1}{m}} = 1 + \sum_{n=1}^{\infty} \frac{\frac{1}{m}(\frac{1}{m}-1)\cdot \ldots \cdot (\frac{1}{m}-n+1)}{n!} X_1^n$, $g_2 = 1 + X_1$. Η g_2 είναι απολύτως συγκλίνουσα στον $\frac{1}{3}$−κύβο. Το ίδιο ισχύει και γιά την g_1 διότι :

-Αν $m = 1$, τότε $g_1 = 1 + X_1$, η οποία συγκλίνει απολύτως κατα τετριμμένο τρόπο στον $\frac{1}{3}$−κύβο.

-Αν $m = -1$, τότε $g_1 = (1+X_1)^{-1} = 1 - \sum_{n=1}^{\infty} X_1^n$, η οποία συγκλίνει απολύτως στον $\frac{1}{3}$−κύβο.

-Αν $|m| \geq 2$, ή ισοδύναμα $|\frac{1}{m}| \leq \frac{1}{2}$, τότε, γιά κάθε $k \in \mathbb{N}$ έχουμε $|\frac{1}{m} - k| \leq \frac{2k+1}{2}$. Άρα, αν (x_1, x_2) στον $\frac{1}{3}$−κύβο, τότε

$$|\tfrac{\frac{1}{m}(\frac{1}{m}-1)\cdot\ldots\cdot(\frac{1}{m}-n+1)}{n!} x_1^n| < \tfrac{1\cdot 3\cdot \ldots \cdot (2n-1)}{2^n n!}|x_1|^n = \tfrac{1}{2^n n!}\tfrac{(2n-1)!}{2\cdot 4\cdot\ldots\cdot(2n-2)}|x_1|^n =$$

$$\tfrac{1}{2^n n!}\tfrac{(2n-1)!}{2^{n-1}(n-1)!}|x_1|^n = \tfrac{\binom{2n-1}{n}}{2^{2n-1}}|x_1|^n \leq {}^5|x_1|^n,$$

συνεπώς η g_1 συγκλίνει απολύτως στον $\frac{1}{3}$−κύβο.

Από την πρόταση 3.1 τώρα, γιά κάποιο $\epsilon' \leq \frac{1}{3}$, αν (x_1, x_2) στον ϵ'-κύβο, η $f(g_1(x_1,x_2), g_2(x_1,x_2))$ είναι απολύτως συγκλίνουσα. Όμως

$$f(g_1(x_1,x_2), g_2(x_1,x_2)) = f((1+x_1)^{\frac{1}{m}}, 1+x_1) =$$

$$[(1+x_1)^{\frac{1}{m}}]^m - (1+x_1) = 0.$$

Άρα από την πρόταση 3.2 όλοι οι συντελεστές της δυναμοσειράς $f(g_1(X_1,X_2), g_2(X_1,X_2)) = [(1+X_1)^{\frac{1}{m}}]^m - (1+X_1)$ είναι 0. Έπεται λοιπόν, όμοια με πριν, ότι ισχύει η ταυτότητα

[5] Με απλή επαγωγή βλέπει κανείς ότι ισχύει $\binom{2n-1}{n} \leq 2^{2n-1}$

$$[(1+X_1)^{\frac{1}{m}}]^m = (1+X_1).$$

ΤΑΥΤ. 3.6 *Γιά κάθε m θετικό ακέραιο,* $\frac{1}{(1+X_2)^{mX_1}} = (1+X_2)^{-mX_1}$.

Απόδειξη :Παρατηρούμε κατ΄ αρχάς ότι, γιά (x_1, x_2) στον $\frac{1}{2}$-κύβο του $\mathbb{R}^2$, η διωνυμική σειρά $(1+x_1)^{x_2} = 1 + \sum_{n=1}^{\infty} \frac{x_2(x_2-1)\cdot\ldots\cdot(x_2-n+1)}{n!} x_1^n$ είναι απολύτως συγκλίνουσα. Πράγματι, γιά $k \in \mathbb{N}$, έχουμε $|x_2 - k| \leq \frac{2k+1}{2}$, άρα $|\frac{x_2(x_2-1)\cdot\ldots\cdot(x_2-n+1)}{n!} x_1^n| < \frac{\binom{2n-1}{n}}{2^{2n-1}} |x_1|^n \leq |x_1|^n$. Δουλεύουμε στον $K[[X_1, X_2]]$. Θεωρούμε τις δυναμοσειρές $f = \frac{1}{1+X_1} - X_2$, $g_1 = (1+X_2)^{mX_1} - 1$ και $g_2 = (1+X_2)^{-mX_1}$. Γιά (x_1, x_2) στον $\frac{1}{2m}$−κύβο, οι σειρές $f(x_1, x_2)$, $g_1(x_1, x_2)$, $g_2(x_1, x_2)$ είναι απολύτως συγκλίνουσες. Από την πρόταση 3.1 τώρα, γιά κάποιο $\epsilon^{'} \leq \frac{1}{2m}$, αν (x_1, x_2) στον $\epsilon^{'}$-κύβο, η $f(g_1(x_1, x_2), g_2(x_1, x_2))$ είναι απολύτως συγκλίνουσα. Όμως

$$f(g_1(x_1, x_2), g_2(x_1, x_2)) = f((1+x_2)^{mx_1} - 1, (1+x_2)^{-mx_1}) =$$

$$\tfrac{1}{(1+x_2)^{mx_1}} - (1+x_2)^{-mx_1} = 0.$$

Όμοια λοιπόν με τα παραπάνω, γιά κάθε m θετικό ακέραιο, ισχύει η ταυτότητα

$$\tfrac{1}{(1+X_2)^{mX_1}} = (1+X_2)^{-mX_1}.$$

ΤΑΥΤ. 3.7 $(1+X_2)^{X_1}(1+X_3)^{X_1} = ((1+X_2)(1+X_3))^{X_1}$.

Απόδειξη : Δουλεύουμε στον $K[[X_1, X_2, X_3, X_4]]$. Θεωρούμε τη δυναμοσειρά

$$f = (1+X_2)^{X_1}(1+X_3)^{X_1} - (1+X_4)^{X_1}$$

Η f είναι απολύτως συγκλίνουσα στον $\frac{1}{3}$-κύβο διότι : Αν (x_1, x_2, x_3, x_4) στον $\frac{1}{3}$-κύβο, τότε

$$|\sum_{k=1}^{n} \frac{x_1(x_1-1)\cdot\ldots\cdot(x_1-k+1)}{k!} x_2^k \frac{x_1(x_1-1)\cdot\ldots\cdot(x_1-(n-k)+1)}{(n-k)1} x_3^{n-k} -$$
$$\frac{x_1(x_1-1)\cdot\ldots\cdot(x_1-k+1)}{n!} x_4^n| < n\frac{1}{3^n} + \frac{1}{3^n} = \frac{n+1}{3^n}$$

και η $\sum_{n=1}^{\infty} \frac{n+1}{3^n}$ συγκλίνει. Θεωρούμε ακόμα τις δυναμοσειρές $g_1 = X_1$, $g_2 = X_2$, $g_3 = X_3$, $g_4 = (1+X_2)(1+X_3)$. Οι g_1, g_2, g_3, g_4 είναι απολύτως συγκλίνουσες στον $\frac{1}{3}$-κύβο. Από την πρόταση 3.1 τώρα, γιά κάποιο $\epsilon^{'} \leq \frac{1}{3}$, αν (x_1, x_2, x_3, x_4) στον $\epsilon^{'}$-κύβο, η $f(g_1, g_2, g_3, g_4)(x_1, x_2, x_3, x_4)$ είναι απολύτως συγκλίνουσα. Όμως

$$f(g_1, g_2, g_3, g_4)(x_1, x_2, x_3, x_4) = f(x_1, x_2, x_3, (1+x_2)(1+x_3) - 1) =$$

$$(1+x_2)^{x_1}(1+x_3)^{x_1} - [(1+x_2)(1+x_3)]^{x_1} = 0.$$

Άρα από την πρόταση 3.2, όλοι οι συντελεστές της δυναμοσειράς $f(X_1, X_2, X_3, (1+X_2)(1+X_3) - 1)$ είναι 0. Έπεται λοιπόν, όμοια με πριν, ότι ισχύει η ταυτότητα

$$(1+X_2)^{X_1}(1+X_3)^{X_1} = ((1+X_2)(1+X_3))^{X_1}.$$

ΤΑΥΤ. 3.8 *Γιά κάθε m θετικό ακέραιο,* $[(1+X_1)^m]^{X_2} = (1+X_1)^{mX_2}$.

Απόδειξη :Δουλεύουμε στον $K[[X_1, X_2, X_3, X_4]]$. Θεωρούμε τις δυναμοσειρές $f = (1+X_1)^{X_2} - (1+X_3)^{X_4}$, $g_1 = (1+X_1)^m - 1$, $g_2 = X_2$, $g_3 = X_1$, $g_4 = mX_2$. Οι παραπάνω δυναμοσειρές είναι απολύτως συγκλίνουσες στον $\frac{1}{2m}$-κύβο. Από την πρόταση 3.1, γιά κάποιο $\epsilon^{'} \leq \frac{1}{2m}$, αν (x_1, x_2, x_3, x_4) στον $\epsilon^{'}$-κύβο, η $f(g_1, g_2, g_3, g_4)(x_1, x_2, x_3, x_4)$ είναι απολύτως συγκλίνουσα. Όμως

$$f(g_1, g_2, g_3, g_4)(x_1, x_2, x_3, x_4) = f((1+x_1)^m - 1, x_2, x_1, mx_2) =$$

$$[(1+x_1)^m]^{x_2} - (1+x_1)^{mx_2} = 0.$$

Έπεται λοιπόν, όμοια με πριν, ότι γιά κάθε m θετικό ακέραιο ισχύει η ταυτότητα

$$[(1+X_1)^m]^{X_2} = (1+X_1)^{mX_2}.$$

ΤΑΥΤ. 3.9 $(1+X_1)^{X_2}(1+X_1)^{X_3} = (1+X_1)^{X_2+X_3}$, *σε κάθε σώμα K, με $K \supseteq \mathbb{Q}$.*

Απόδειξη :Δουλεύουμε στον $K[[X_1, X_2, X_3, X_4]]$. Θεωρούμε τις δυναμοσειρές $f = (1+X_1)^{X_2}(1+X_1)^{X_3} - (1+X_1)^{X_4}$, $g_1 = X_1$, $g_2 = X_2$, $g_3 = X_3$, $g_4 = X_2 + X_3$. Οι παραπάνω δυναμοσειρές είναι απολύτως συγκλίνουσες στον $\frac{1}{2}$-κύβο. Από την πρόταση 3.1, γιά κάποιο $\epsilon^{'} \leq \frac{1}{2}$, αν (x_1, x_2, x_3, x_4) στον $\epsilon^{'}$-κύβο, η $f(g_1, g_2, g_3, g_4)(x_1, x_2, x_3, x_4)$ είναι απολύτως συγκλίνουσα. Όμως

$$f(g_1, g_2, g_3, g_4)(x_1, x_2, x_3, x_4) = f(x_1, x_2, x_3, x_2 + x_3) =$$

$$(1+x_1)^{x_2}(1+x_1)^{x_3}-(1+x_1)^{x_2+x_3}=0.$$

Έπεται λοιπόν, όμοια με πριν, ότι ισχύει η ταυτότητα

$$(1+X_1)^{X_2}(1+X_1)^{X_3}=(1+X_1)^{X_2+X_3}.$$

Ως άμεση συνέπεια τώρα των παραπάνω ταυτοτήτων και του λήμματος 3.4, σελίδα 20, προκύπτουν τα εξής : Αν K σώμα με $K \geq \mathbb{Q}$, τότε,

- Γιά κάθε $f_1,\ldots,f_n \in K[[X]]$, με $\mathrm{ord} f_i > 0$ γιά κάθε $i \in \{1,\ldots n\}$, ισχύει

$$\sum_{i=1}^{n}\log(1+f_i)=\log(\prod_{i=1}^{n}(1+f_i)) \text{ και } \prod_{i=1}^{n}\exp(f_i)=\exp(\sum_{i=1}^{n}f_i). \tag{6}$$

- Γιά κάθε $f \in K[[X]]$ με $\mathrm{ord} f > 0$, ισχύει

$$\log(\exp(f))=f \text{ και } \exp(\log(1+f))=1+f. \tag{7}$$

- Γιά κάθε $m \in \mathbb{Z}^*$, και $f \in K[[X]]$ με $\mathrm{ord} f > 0$ ισχύει

$$[(1+f)^{\frac{1}{m}}]^m=1+f. \tag{8}$$

- Γιά κάθε m θετικό ακέραιο, και $f_1,f_2 \in K[[X]]$ με $\mathrm{ord} f, \mathrm{ord} f_2 > 0$, ισχύει

$$\frac{1}{(1+f_2)^{mf_1}}=(1+f_2)^{-mf_1}. \tag{9}$$

- Γιά κάθε $f_1,f_2,f_3 \in K[[X]]$, με $\mathrm{ord} f_i > 0$ γιά κάθε $i=1,2,3$, ισχύει

$$(1+f_2)^{f_1}(1+f_3)^{f_1}=((1+f_2)(1+f_3))^{f_1}. \tag{10}$$

- Γιά κάθε m θετικό ακέραιο, και $f_1,f_2 \in K[[X]]$ με $\mathrm{ord} f_1, \mathrm{ord} f_2 > 0$, ισχύει

$$[(1+f_1)^m]^{f_2}=(1+f_1)^{mf_2}. \tag{11}$$

- Γιά κάθε $f_1,f_2,f_3 \in K[[X]]$, με $\mathrm{ord} f_i > 0$ γιά κάθε $i=1,2,3$, ισχύει

$$(1+f_1)^{f_2}(1+f_1)^{f_3}=(1+f_1)^{f_2+f_3}. \tag{12}$$

Επίσης, θα χρειαστούμε το παρακάτω λήμμα.

Λήμμα 3.5 *Αν* $\{f_j\}_{j=1}^{\infty}$ *είναι ακολουθία στοιχείων του* $K[[X]]$, *με* $\mathrm{ord} f_j > 0$ *γιά κάθε* $j \geq 1$ *και,επιπλέον, ορίζεται το άπειρο άθροισμα* $\sum_{j=1}^{\infty} f_j$, *τότε ορίζονται τα* $\exp(\sum_{j=1}^{\infty} f_j)$, *και* $\prod_{j=1}^{\infty} \exp(f_j)$ *και είναι ίσα.*

Απόδειξη. Καθώς $\mathrm{ord} f_j > 0$ γιά κάθε $j \geq 1$ και αφού ορίζεται το άπειρο άθροισμα $\sum_{j=1}^{\infty} f_j$, έπεται και ότι $\mathrm{ord}(\sum_{j=1}^{\infty} f_j) > 0$, άρα ορίζεται και το $\exp(\sum_{j=1}^{\infty} f_j)$. Γιά $n \geq 1$, θέτουμε $f_j^n = \sum_{i=0}^{\infty} a_{n,j,i} X^i$. Έστω $M > 0$. Αφού ορίζεται το $\sum_{j=1}^{\infty} f_j$, από το λήμμα 1.1, σελ. 4 έχουμε ότι $\mathrm{ord}(f_j) \stackrel{j\to\infty}{\longrightarrow} \infty$, δηλαδή γιά το δοθέν $M > 0$ μπορούμε να βρούμε j_M τ.ώ. αν $j \geq j_M$, τότε $\mathrm{ord}(f_j) > M$. Αν λοιπόν $j \geq j_M$, έχουμε ότι γιά κάθε $n \geq 1$, $a_{n,j,0} = \ldots = a_{n,j,M} = 0$, άρα

$$\begin{aligned} \mathrm{ord}(\exp(f_j) - 1) \quad &= \quad \mathrm{ord}(\frac{1}{1!}a_{1,j,1}X + (\frac{1}{1!}a_{1,j,2} + \frac{1}{2!}a_{2,j,1})X^2 + \\ &\ldots \quad +(\frac{1}{1!}a_{1,j,M} + \frac{1}{2!}a_{2,j,(M-1)} + \ldots + \frac{1}{M!}a_{M,j,1})X^M + \ldots) \\ &> \quad M\,. \end{aligned}$$

Άρα έχουμε ότι $\mathrm{ord}(\exp(f_j) - 1) \stackrel{j\to\infty}{\longrightarrow} \infty$, αρα το $\prod_{j=1}^{\infty} \exp(f_j)$ συγκλίνει από το λήμμα 1.2, σελ 5. Επειδή τώρα γιά κάθε $\kappa \geq 2$ $\exp(\sum_{j=1}^{\kappa} f_j) = \prod_{j=1}^{\kappa} \exp(f_j)$ και καθώς $\mathrm{ord}(\prod_{j=1}^{\kappa} \exp(f_j) - \prod_{j=1}^{\infty} \exp(f_j)) \stackrel{\kappa\to\infty}{\longrightarrow} \infty$ και λόγω του προηγούμενου λήμματος $\mathrm{ord}(\exp(\sum_{j=1}^{\kappa} f_j) - \exp(\sum_{j=1}^{\infty} f_j)) \stackrel{\kappa\to\infty}{\longrightarrow} \infty$, έπεται ότι $\exp(\sum_{j=1}^{\infty} f_j) = \prod_{j=1}^{\infty} \exp(f_j)$.

Λήμμα 3.6 *Έστω* $f(X) = \sum_{i=0}^{\infty} a_i X^i \in 1 + X\mathbb{Q}_p[[X]]$. *Τότε* $f(X) \in 1 + X\mathbb{Z}_p[[X]]$ *αν και μόνο εαν* $\frac{f(X^p)}{f^p(X)} \in 1 + pX\mathbb{Z}_p[[X]]$.

Απόδειξη. $(\Rightarrow)$ Λαμβάνοντας υπ'οψιν ότι αν $a, b \in \mathbb{Z}_p$, τότε $(a + b)^p \equiv a^p + b^p (mod p)$ και $a^p \equiv a (mod p)$, έχουμε ότι $f^p(X) = f(X^p) + pg(X)$ όπου

$g(X) \in X\mathbb{Z}_p[[X]]$. [6] Καθώς το $f^p(X)$ είναι αντιστρέψιμο στοιχείο του $\mathbb{Z}_p[[X]]$, [7] έχουμε ότι $\frac{f(X^p)}{f^p(X)} = 1 - \frac{pg(X)}{f^p(X)} \in 1 + pX\mathbb{Z}_p[[X]]$. [8]

($\Leftarrow$) Έστω ότι

$$f(X^p) = f^p(X)g(X) \tag{13}$$

γιά κάποιο $g(X) = \sum_{i=0}^{\infty} b_i X^i \in 1 + pX\mathbb{Z}_p[[X]]$. Θα δείξουμε επαγωγικά ότι $a_i \in \mathbb{Z}_p$ γιά κάθε $i \geq 0$. Γιά $i = 0$, $a_0 = 1 \in \mathbb{Z}_p$. Έστω $a_i \in \mathbb{Z}_p$ γιά κάθε $i < n$ γιά κάποιον $n \geq 1$. Από τη σχέση 13 προκύπτει ότι ο συντελεστής του X^n στο αριστερό μέλος είναι ίσος με τον συντελεστή του X^n στο γινόμενο $(\sum_{i=0}^{n} a_i X^i)^p (1 + \sum_{i=1}^{n} b_i X^i)$. Αν $p|n$ έχουμε : $a_{\frac{n}{p}} = pa_n + a^p_{\frac{n}{p}} + pc$, όπου $c \in \mathbb{Z}_p$, και επειδή $a^p_{\frac{n}{p}} \equiv a_{\frac{n}{p}} \pmod p$, έχουμε $a^p_{\frac{n}{p}} - a_{\frac{n}{p}} = pc'$, όπου $c' \in \mathbb{Z}$, οπότε $a_n = -c - c' \in \mathbb{Z}_p$. Αν $p \not| n$ έχουμε : $0 = pa_n + pc$ όπου $c \in \mathbb{Z}_p$, άρα $a_n \in \mathbb{Z}_p$. Σε κάθε περίπτωση λοιπόν, $a_n \in \mathbb{Z}_p$.

Το παραπάνω λήμμα ισχύει και στην περίπτωση που η f είναι μία δυναμοσειρά δύο μεταβλητών με συντελεστές στο $\mathbb{Q}_p$ και σταθερό όρο μονάδα, δηλαδή :

> Έστω $f(X,Y) \in 1 + X\mathbb{Q}_p[[X,Y]] + Y\mathbb{Q}_p[[X,Y]]$. Τότε $f(X,Y) \in 1 + X\mathbb{Z}_p[[X,Y]] + Y\mathbb{Z}_p[[X,Y]]$ αν και μόνο εαν $\frac{f(X^p,Y^p)}{f^p(X,Y)} \in 1 + pX\mathbb{Z}_p[[X,Y]] + pY\mathbb{Z}_p[[X,Y]]$.

Ορίζουμε $F(X,Y) \in \mathbb{Q}[[X,Y]]$ ως εξής :

[6] Έστω $f_n = 1 + a_1X + a_2X^2 + \ldots + a_nX^n$ γιά $n = 1, 2, \ldots$. Είναι $f_n^p \in 1 + a_1^pX^p + \ldots + a_n^pX^{pn} + pX\mathbb{Z}_p[X]$. Ακόμα, $a_i^p = a_i + pa_i'$, όπου $a_i' \in \mathbb{Z}_p$, γιά $i = 1, 2, \ldots$, άρα $f_n^p = f_n(X^p) + pXg_n$, όπου $g_n \in \mathbb{Z}_p[X]$ (1). Παρατηρούμε ότι $m > n \Rightarrow \mathrm{ord}(g_m - g_n) \geq n$. Πράγματι, καθώς $f_m = f_n + a_{n+1}X^{n+1} + \ldots + a_mX^m$, έχουμε ότι $f_m^p - f_n^p \in X^{n+1}\mathbb{Z}_p[X]$ και $f_m(X^p) - f_n(X^p) \in X^{p(n+1)}\mathbb{Z}_p[X]$. Από την (1) όμως έπεται ότι $(f_m^p - f_n^p) - (f_m(X^p) - f_n(X^p)) = pX(g_m - g_n)$, άρα από τα παραπάνω $pX(g_m - g_n) \in X^{n+1}\mathbb{Z}_p[X]$, συνεπώς $p(g_m - g_n) \in X^n\mathbb{Z}_p[X]$. Αν λοιπόν γιά οποιοδήποτε $k \geq 0$ ορίσουμε c_k να είναι ο συντελεστής του X^k στο πολυώνυμο g_n, όπου n αυθαίρετος δείκτης $> k$, το c_k είναι καλώς ορισμένο στοιχείο του $\mathbb{Z}_p$ και $\lim_n g_n = c_0 + c_1X + c_2X^2 + \ldots \overset{\text{ορσ}}{=} g \in \mathbb{Z}_p[[X]]$. Παίρνοντας τώρα όρια ως προς n στην (1), έχουμε ότι $f^p(X) = f(X^p) + pg(X)$.

[7] Γενικά ισχύει ότι αν R είναι αντιμεταθετικός δακτύλιος με μονάδα, τότε το $\sum_{i=0}^{\infty} a_iX^i \in R[[X]]$ είναι αντιστρέψιμο στοιχείο του $R[[X]]$, αν και μόνο εαν το a_0 είναι αντιστρέψιμο στοιχείο του R. Εδώ το $f^p(X)$ έχει σταθερό όρο 1.

[8] Διότι $\frac{1}{f^p(X)} \in \mathbb{Z}_p[[X]]$ και $g(X) \in X\mathbb{Z}_p[[X]]$.

$$F(X,Y) =$$

$$B_{X,p}(Y)B_{\frac{X^p-X}{p},p}(Y^p)B_{\frac{X^{p^2}-X^p}{p^2},p}(Y^{p^2})\cdot\ldots\cdot B_{\frac{X^{p^n}-X^{p^{n-1}}}{p^n},p}(Y^{p^n})\cdot\ldots =$$

$$(1+Y)^X(1+Y^p)^{\frac{X^p-X}{p}}(1+Y^{p^2})^{\frac{X^{p^2}-X^p}{p^2}}\cdot\ldots\cdot(1+Y^{p^n})^{\frac{X^{p^n}-X^{p^{n-1}}}{p^n}}\cdot\ldots =$$

$$(1+\sum_{i=1}^{\infty}\frac{X(X-1)\cdot\ldots\cdot(X-i+1)}{i!}Y^i)\cdot$$
$$\prod_{n=1}^{\infty}(1+\sum_{i=1}^{\infty}\frac{X^{p^n}-X^{p^{n-1}}}{p^n}(\frac{X^{p^n}-X^{p^{n-1}}}{p^n}-1)\cdot$$
$$\ldots\cdot(\frac{X^{p^n}-X^{p^{n-1}}}{p^n}-i+1)\frac{Y^{ip^n}}{i!}).$$

Το παραπάνω απειρογινόμενο τυπικών δυναμοσειρών συγκλίνει.[9]

Έχουμε λοιπόν ότι $F(X,Y)\in 1+X\mathbb{Q}_p[[X,Y]]+Y\mathbb{Q}_p[[X,Y]]$. Θα δείξουμε ότι $F(X,Y)\in\mathbb{Z}_p[[X,Y]]$.Έχουμε ότι

$\frac{F(X^p,Y^p)}{F^p(X,Y)} = \frac{(1+Y^p)^{X^p}(1+Y^{p^2})^{\frac{X^{p^2}-X^p}{p}}(1+Y^{p^3})^{\frac{X^{p^3}-X^{p^2}}{p^2}}\cdot\ldots}{(1+Y)^{pX}(1+Y^p)^{X^p-X}(1+Y^{p^2})^{\frac{X^{p^2}-X^p}{p}}\cdot\ldots} = \frac{(1+Y^p)^X}{(1+Y)^{pX}}.$ [10]

Από το προηγούμενο λήμμα, γιά την $1+Y$, έχουμε ότι, αφού $1+Y\in 1+Y\mathbb{Z}_p[[X]]$, έπεται ότι $\frac{1+Y^p}{(1+Y)^p}=1+pYg(Y)$ γιά κάποια $g(Y)\in\mathbb{Z}_p[[Y]]$. Άρα λοιπόν

$\frac{(1+Y^p)^X}{(1+Y)^{pX}} = \frac{[(1+Y)^p(1+pYg(Y))]^X}{(1+Y)^{pX}} =^{11} \frac{[(1+Y)^p]^X(1+pYg(Y))^X}{(1+Y)^{pX}} =^{12}$

---

[9] Γενικότερα, αν $\{f_i\}_{i\in\mathbb{N}}$, $\{g_i\}_{i\in\mathbb{N}}$ ακολουθίες στοιχείων του $\Omega_p[[X_1,X_2]]$ με $\mathrm{ord}f_i,\mathrm{ord}g_i>0$ γιά κάθε i, τότε : Αν $\mathrm{ord}f_i\overset{i\to\infty}{\longrightarrow}\infty$, τότε το γινόμενο $\prod_{i=1}^{\infty}(1+f_i)^{g_i}$ υπάρχει στον $\Omega_p[[X_1,X_2]]$. Πράγματι, έστω $M>0$. Καθώς γιά κάθε i, $\mathrm{ord}f_i,\mathrm{ord}g_i>0$, το $(1+f_i)^{g_i}$ υπάρχει στον $\Omega_p[[X_1,X_2]]$ γιά κάθε i. Βρίσκουμε i_0 τ.ώ. αν $i\geq i_0$, τότε $\mathrm{ord}f_i>M$. Αν τώρα $i\geq i_0$, τότε $\mathrm{ord}(1-(1+f_i)^{g_i})=\mathrm{ord}(\sum_{n=1}^{\infty}\frac{g_i(g_i-1)\cdot\ldots\cdot(g_i-n+1)}{n!}f_i^n)\geq \min_n\{\mathrm{ord}(\frac{g_1(g_i-1)\cdot\ldots\cdot(g_i-n+1)}{n!}f_i^n)\}>M$. Άρα $\mathrm{ord}(1-(1+f_i)^{g_i})\overset{i\to\infty}{\longrightarrow}\infty$, άρα το γινόμενο $\prod_{i=1}^{\infty}(1+f_i)^{g_i}$ υπάρχει στον $\Omega_p[[X_1,X_2]]$.

[10] Βλ. παράρτημα

[11] Βλ. σχέση 10, σελ. 28

[12] Βλ. σχέση 11, σελ. 28

$$\frac{(1+Y)^{pX}(1+pYg(Y))^X}{(1+Y)^{pX}} = (1+pYg(Y))^X =$$
$$1 + \sum_{i=1}^{\infty} \frac{X(X-1)\cdot \ldots \cdot (X-i+1)}{i!} p^i (Yg(Y))^i$$
$$\in 1 + pX\mathbb{Z}_p[[X,Y]] + pY\mathbb{Z}_p[[X,Y]].$$

Άρα από το παραπάνω λήμμα, $F(X,Y) \in \mathbb{Z}_p[[X,Y]]$.

4 Πολύγωνα του Newton και το θεώρημα του Weierstrass.

Έστω $f = 1 + \sum_{i=1}^{n} a_i X^i \in 1 + X\Omega_p[X]$ πολυώνυμο. Θεωρούμε στο Καρτεσιανό επίπεδο τα σημεία $(0,0)$,$(i, \mathrm{ord}_p ai)$ όπου $a_i \neq 0$. Ορίζουμε το πολύγωνο του Newton του f και θα το συμβολίζουμε $N.P$, ως την κυρτή θήκη του συνόλου $\{(i, \mathrm{ord}_p a_i) \ : \ i \geq 1$ και $a_i \neq 0\} \cup \{(0,0)\}$.
Το $N.P.$ του f μπορεί πρακτικά να κατασκευαστεί μέσω της παρακάτω διαδικασίας. Θέτουμε $\lambda_1 \overset{\text{ορσ}}{=} \min\{\frac{\mathrm{ord}_p a_i}{i} \ : \ i \geq 1\}$ και κατόπιν $i_1 \overset{\text{ορσ}}{=} \max\{i \geq 1 \ : \ \mathrm{ord}_p a_i = \lambda_1 i\}$. Το πρώτο τμήμα του $N.P.$ του f είναι το ευθύγραμμο τμήμα με άκρα τα σημεία $(0,0)$ και $(i_1, \mathrm{ord}_p a_{i_1})$. Έστω ότι έχουμε κατασκευάσει το κ-οστό τμήμα του $N.P.$ του f. θέτουμε $\lambda_{\kappa+1} \overset{\text{ορσ}}{=} \min\{\frac{\mathrm{ord}_p a_i - \mathrm{ord}_p a_{i_\kappa}}{i - i_\kappa} \ : \ i \geq i_\kappa + 1\}$ και $i_{\kappa+1} \overset{\text{ορσ}}{=} \max\{i \geq i_\kappa + 1 \ : \ \mathrm{ord}_p a_i - \mathrm{ord}_p a_{i_\kappa} = \lambda_{\kappa+1}(i - i_\kappa)\}$. Το $(\kappa+1)$-οστό τμήμα του $N.P.$ του f είναι το ευθύγραμμο τμήμα με άκρα τα σημεία $(i_\kappa, \mathrm{ord}_p a_{i_\kappa})$ και $(i_{\kappa+1}, \mathrm{ord}_p a_{i_{\kappa+1}})$. Η διαδικασία σταματάει στο κ-οστό βήμα που θα έχουμε $i_\kappa = n$, όπου n είναι ο βαθμός του f.

Ο ορισμός του $N.P.$ μπορεί να γενικευτεί και στην περίπτωση που η f είναι μία δυναμοσειρά.
Έστω $f = 1 + \sum_{i=1}^{\infty} a_i X^i \in 1 + x\Omega_p[[X]]$. Το $N.P.$ της f ορίζεται να είναι το όριο ως προς n των $N.P.$ των $f_n \overset{\text{ορσ}}{=} 1 + \sum_{i=1}^{n} a_i X^i$. Το $N.P.$ της f μπορεί πρακτικά να κατασκευαστεί μέσω της παρακάτω διαδικασίας.

Κατάρχήν θεωρούμε στο Καρτεσιανό επίπεδο τα σημεία $(0,0)$,$(i, \mathrm{ord}_p ai)$ όπου $a_i \neq 0$. Θέτουμε $\lambda_1 \overset{\text{ορσ}}{=} \inf\{\frac{\mathrm{ord}_p a_i}{i} \ : \ i \geq 1\}$ και κατόπιν $i_1 \overset{\text{ορσ}}{=} \sup\{i \geq 0 \ : \ \mathrm{ord}_p a_i = \lambda_1 i\}$.
• Αν $i_1 = \infty$, τότε το τελευταίο τμήμα του $N.P.$ της f είναι η ημιευθεία με αρχή το $(0,0)$ και κλίση λ_1.
• Αν $i_1 < \infty$, τότε :
-Αν $i_1 = 0$, ομοίως το τελευταίο τμήμα του $N.P.$ της f είναι η ημιευθεία με αρχή το $(0,0)$ και κλίση λ_1.
-Αν $0 < i_1 < \infty$, τότε θέτουμε $\lambda_2 \overset{\text{ορσ}}{=} \inf\{\frac{\mathrm{ord}_p a_i - \mathrm{ord}_p a_{i_1}}{i - i_1} \ : \ i \geq i_1 + 1\}$.
-Αν $\lambda_2 = \lambda_1$, τότε το τελευταίο τμήμα του $N.P.$ της f είναι η ημιευθεία με αρχή το $(0,0)$ και κλίση $\lambda_2 = \lambda_1$.

-Αν $\lambda_2 > \lambda_1$,[13] τότε το πρώτο τμήμα του $N.P.$ της f είναι το ευθύγραμμο τμήμα με άκρα τα σημεία $(0,0)$ και $(i_1, \mathrm{ord}_p a_{i_1})$ και η διαδικασία συνεχίζεται θέτοντας $i_2 \overset{o\rho\sigma}{=} \sup\{i \geq i_1 \ : \ \mathrm{ord}_p a_i - \mathrm{ord}_p a_{i_1} = \lambda_2(i - i_1)\}$.

Έστω ότι έχουμε κατασκευάσει το n-οστό τμήμα του $N.P.$ της f και ότι $\lambda_{n+1} > \lambda_n$,[14] δηλαδή το n-οστό τμήμα του $N.P.$ της f δεν είναι το τελευταίο.

Θέτουμε $i_{n+1} \overset{o\rho\sigma}{=} \sup\{i \geq i_n \ : \ \mathrm{ord}_p a_i - \mathrm{ord}_p a_{i_n} = \lambda_{n+1}(i - i_n)\}$.

- Αν $i_{n+1} = \infty$, τότε το $(n+1)$-οστό και τελευταίο τμήμα του $N.P.$ της f είναι η ημιευθεία με αρχή το σημείο $(i_n, \mathrm{ord}_p a_{i_n})$ και κλίση λ_{n+1}.
- Αν $i_{n+1} < \infty$, τότε :

-Αν $i_{n+1} = i_n$, τότε το $(n+1)$-οστό και τελευταίο τμήμα του $N.P.$ της f είναι η ημιευθεία με αρχή το σημείο $(i_n, \mathrm{ord}_p a_{i_n})$ και κλίση λ_{n+1}.

-Αν $i_n < i_{n+1} < \infty$, τότε θέτουμε $\lambda_{n+2} \overset{o\rho\sigma}{=} \inf\{\frac{\mathrm{ord}_p a_i - \mathrm{ord}_p a_{i_{n+1}}}{i - i_{n+1}} \ : \ i \geq i_{n+1} + 1\}$.

-Αν $\lambda_{n+2} = \lambda_{n+1}$, τότε το $(n+1)$-οστό και τελευταίο τμήμα του $N.P.$ της f είναι η ημιευθεία με αρχή το $(i_{n+1}, \mathrm{ord}_p a_{i_{n+1}})$ και κλίση $\lambda_{n+2} = \lambda_{n+1}$.

-Αν $\lambda_{n+2} > \lambda_{n+1}$,[15] τότε το $(n+1)$-οστό τμήμα του $N.P.$ της f είναι το ευθύγραμμο τμήμα με άκρα τα σημεία $(i_n, \mathrm{ord}_p a_{i_n})$ και $(i_{n+1}, \mathrm{ord}_p a_{i_{n+1}})$ και η διαδικασία συνεχίζεται θέτοντας $i_{n+2} \overset{o\rho\sigma}{=} \sup\{i \geq i_{n+1} \ : \ \mathrm{ord}_p a_i - \mathrm{ord}_p a_{i_{n+1}} = \lambda_{n+2}(i - i_{n+1})\}$.

Λήμμα 4.1 *Έστω $f = 1 + a_1 X + \ldots + a_n X^n = (1 - \frac{X}{\alpha_1}) \cdots (1 - \frac{X}{\alpha_n})$, με $a_n \neq 0$, όπου $\alpha_1, \ldots, \alpha_n$ οι ρίζες του f.[16] Έστω $\lambda_i \overset{o\rho\sigma}{=} \mathrm{ord}_p \frac{1}{\alpha_i}$. Τότε, αν ένα τμήμα του $N.P.$ του f έχει κλίση λ και προβολή στον οριζόντιο άξονα μήκους l, έπεται ότι γιά ακριβώς l τιμές του $i \in \{1, 2, \ldots, n\}$ έχουμε $\lambda_i = \lambda$.*

Απόδειξη : Υποθέτουμε ότι οι α_i είναι διατεταγμένες έτσι ώστε $\mathrm{ord}_p \frac{1}{\alpha_1} \leq \ldots \leq \mathrm{ord}_p \frac{1}{\alpha_n}$, ή αλλιώς $\lambda_1 \leq \ldots \leq \lambda_n$. Έστω ότι $\lambda_1 = \lambda_2 = \ldots = \lambda_r < \lambda_{r+1}$. Θα δείξουμε ότι το πρώτο τμήμα του $N.P.$ του f είναι το τμήμα με άκρα τα $(0,0)$ και $(r, r\lambda_1)$. Στο σημείο αυτό παρατηρούμε τα εξής : $f = a_n(X^n + \frac{a_{n-1}}{a_n} X^{n-1} + \ldots + \frac{1}{a_n})$ και επειδή γιά $i = 0, \ldots, n-1$ είναι

[13] Σημειωτέον ότι $\lambda_2 \geq \lambda_1$ διότι : Αν $\lambda_2 < \lambda_1$, τότε γιά κάποιο $i_\kappa \geq i_1 + 1$ θα είχαμε $\lambda_2 \leq \frac{\mathrm{ord}_p a_{i_\kappa} - \mathrm{ord}_p a_{i_1}}{i_\kappa - i_1} < \lambda_1$, συνεπώς $\frac{\mathrm{ord}_p a_{i_\kappa} - \mathrm{ord}_p a_{i_1}}{i_\kappa - i_1} < \frac{\mathrm{ord}_p a_{i_\kappa}}{i_\kappa}$. Όμως $\frac{\mathrm{ord}_p a_{i_\kappa} - \mathrm{ord}_p a_{i_1}}{i_\kappa - i_1} < \frac{\mathrm{ord}_p a_{i_\kappa}}{i_\kappa} \Leftrightarrow \frac{\mathrm{ord}_p a_{i_\kappa}}{i_\kappa} < \frac{\mathrm{ord}_p a_{i_1}}{i_1} (= \lambda_1)$, κάτι που είναι άτοπο. Σημειώνουμε επίσης εδώ ότι καθώς έχει οριστεί το λ_2, είναι $0 < i_1 < \infty$.

[14] Όμοια με πριν δείχνει κανείς ότι $\lambda_{n+1} \geq \lambda_n$.

[15] Όμοια $\lambda_{n+2} \geq \lambda_{n+1}$.

[16] Καθώς $f = 1 + a_1 X + \ldots + a_n X^n$, έχουμε $f = a_n(X - \alpha_1) \cdots (X - \alpha_n)$, όπου $a_n(-1)^n \alpha_1 \cdots \alpha_n = 1$. Άρα $f = (-1)^n a_n \alpha_1 \cdots \alpha_n (1 - \frac{X}{\alpha_1}) \cdots (1 - \frac{X}{\alpha_n}) = (1 - \frac{X}{\alpha_1}) \cdots (1 - \frac{X}{\alpha_n})$.

$$\tfrac{a_i}{a_n}=(-1)^{n-i}\sum_{1\le j_1<\ldots<j_{n-i}\le n}\alpha_{j_i}\cdots\alpha_{j_{n-i}},$$

έχουμε ότι γιά $i=0,\ldots,n-1$ είναι

$$a_i=\tfrac{1}{\alpha_1\cdots\alpha_n}\sum_{1\le j_1<\ldots<j_{n-i}\le n}\alpha_{j_i}\cdots\alpha_{j_{n-i}}=(-1)^i\sum_{1\le j_1<\ldots<j_i\le n}\frac{1}{\alpha_{j_1}}\cdots\frac{1}{\alpha_{j_i}}.$$

Όμως καθώς γιά κάθε $1\le j_1<\ldots<j_i\le n$ έχουμε $\mathrm{ord}_p\frac{1}{\alpha_{j_1}}\cdots\frac{1}{\alpha_{j_i}}\ge i\lambda_1$, έπεται ότι $\mathrm{ord}_p a_i\ge i\lambda_1$. Αυτό σημαίνει ότι γιά κάθε $i=0,1,\ldots,$ το σημείο $(i,\mathrm{ord}_p a_i)$ βρίσκεται είτε πάνω στην, ή πάνω από την ευθεία που ενώνει το $(0,0)$ με το $(r,r\lambda_1)$. Θα δείξουμε ότι $\mathrm{ord}_p a_r=r\lambda_1$, δηλαδή το σημείο $(r,\mathrm{ord}_p a_r)$ είναι ουσιαστικά το σημείο $(r,r\lambda_1)$ και ότι γιά κάθε $i>r$ έχουμε $\mathrm{ord}_p a_i>i\lambda_1$, δηλαδή τα σημεία $(i,\mathrm{ord}_p a_i)$ με $i>r$ βρίσκονται πάνω από την ευθεία που ενώνει το $(0,0)$ με το $(r,r\lambda_1)$. Παρατηρούμε ότι ισχύει το εξής : Αν $\{j_1,\ldots,j_r\}=\{1,\ldots,r\}$ τότε $\mathrm{ord}_p\frac{1}{\alpha_{j_1}}\cdots\frac{1}{\alpha_{j_r}}=r\lambda_1$, και αν $\{j_1,\ldots,j_r\}\ne\{1,\ldots,r\}$, τότε $\mathrm{ord}_p\frac{1}{\alpha_{j_1}}\cdots\frac{1}{\alpha_{j_r}}>r\lambda_1$, καθώς στο γινόμενο $\frac{1}{\alpha_{j_1}}\cdots\frac{1}{\alpha_{j_r}}$ θα υπάρχει τουλάχιστον ένας παράγοντας $\frac{1}{\alpha_{j_i}}$ με $\mathrm{ord}_p\frac{1}{\alpha_{j_i}}>\lambda_1$. Έπεται λοιπόν ότι

$$\mathrm{ord}_p((-1)^r\sum_{\substack{1\le j_1<\ldots<j_r\le n\\ \{j_1,\ldots,j_r\}\ne\{1,\ldots,r\}}}\frac{1}{\alpha_{j_1}}\cdots\frac{1}{\alpha_{j_r}})>r\lambda_1,$$

άρα

$$\mathrm{ord}_p a_r=\mathrm{ord}_p((-1)^r\sum_{1\le j_1<\ldots<j_r\le n}\frac{1}{\alpha_{j_1}}\cdots\frac{1}{\alpha_{j_r}})=r\lambda_1.$$

Έστω $i>r$. Επειδή, όμοια με τα παραπάνω έχουμε ότι γιά κάθε $1\le j_1<\ldots<j_i\le n$ έχουμε $\mathrm{ord}_p\frac{1}{\alpha_{j_1}}\cdots\frac{1}{\alpha_{j_i}}>i\lambda_1$, έπεται ότι

$$\mathrm{ord}_p a_i\ge\min_{1\le j_1<\ldots<j_i\le n}(\mathrm{ord}_p\frac{1}{\alpha_{j_1}}\cdots\frac{1}{\alpha_{j_i}})>i\lambda_1.$$

Προκύπτει λοιπόν ότι το πρώτο τμήμα του $N.P.$ του f είναι το τμήμα με άκρα τα $(0,0)$ και $(r,r\lambda_1)$.

Έστω τώρα ότι $\lambda_s<\lambda_{s+1}=\lambda_{s+2}=\ldots=\lambda_{s+r}<\lambda_{s+r+1}$. Θα δείξουμε ότι το τμήμα που ενώνει τα σημεία $(s,\lambda_1+\ldots+\lambda_s)$ και $(s+r,\lambda_1+\ldots+\lambda_s+r\lambda_{s+1})$ είναι τμήμα του $N.P.$ του f. Για αυτό, λαμβάνοντας υπ' όψιν ότι η ευθεία που ενώνει αυτά τα δυο σημεία είναι η $y=\lambda_{s+1}x+(\lambda_1+\ldots+\lambda_s-s\lambda_{s+1})$, βλέπουμε ότι αρκεί να δείξουμε πως

$$\mathrm{ord}_p a_{s+r}=(s+r)\lambda_{s+1}+(\lambda_1+\ldots+\lambda_s-s\lambda_{s+1})=r\lambda_{s+1}+\lambda_1+\ldots+\lambda_s,$$

$$\mathrm{ord}_p a_s = s\lambda_{s+1} + (\lambda_1 + \ldots + \lambda_s - s\lambda_{s+1}) = \lambda_1 + \ldots + \lambda_s,$$

και πως αν $i > s + r$, ή $i < s$, τότε

$$\mathrm{ord}_p a_i > i\lambda_{s+1} + (\lambda_1 + \ldots + \lambda_s - s\lambda_{s+1}).$$

Εντελώς όμοια με τα προηγούμενα βλέπουμε ότι

$$\mathrm{ord}_p a_{s+r} = (s + r)\lambda_{s+1} + (\lambda_1 + \ldots + \lambda_s - s\lambda_{s+1}) = r\lambda_{s+1} + \lambda_1 + \ldots + \lambda_s$$

και ότι

$$\mathrm{ord}_p a_s = s\lambda_{s+1} + (\lambda_1 + \ldots + \lambda_s - s\lambda_{s+1}) = \lambda_1 + \ldots + \lambda_s.$$

Έστω ότι $i > s + r$. Έχουμε ότι

$$i\lambda_{s+1} + (\lambda_1 + \ldots + \lambda_s - s\lambda_{s+1}) = \lambda_1 + \ldots + \lambda_s + r\lambda_{s+1} + (i - (s + r))\lambda_{s+1}.$$

Επειδή γιά κάθε $1 \leq j_1 < \ldots < j_i \leq n$ είναι

$$\mathrm{ord}_p \frac{1}{\alpha_{j_1}} \cdots \frac{1}{\alpha_{j_i}} \geq \lambda_1 + \ldots + \lambda_s + r\lambda_{s+1} + \lambda_{s+r+1} + \ldots + \lambda_i,$$

έχουμε

$$\mathrm{ord}_p a_i \geq \lambda_1 + \ldots + \lambda_s + r\lambda_{s+1} + \lambda_{s+r+1} + \ldots + \lambda_i.$$

Όμως προφανώς

$$\lambda_1 + \ldots + \lambda_s + r\lambda_{s+1} + \lambda_{s+r+1} + \ldots + \lambda_i > \lambda_1 + \ldots + \lambda_s + r\lambda_{s+1} + (i - (s + r))\lambda_{s+1},$$

συνεπώς

$$\mathrm{ord}_p a_i > \lambda_1 + \ldots + \lambda_s + r\lambda_{s+1} + (i - (s + r))\lambda_{s+1}.$$

Έστω ότι $i < s$. Θέτουμε $i = s - k$, όπου $k \geq 1$. Έχουμε ότι

$$i\lambda_{s+1} + (\lambda_1 + \ldots + \lambda_s - s\lambda_{s+1}) = \lambda_1 + \ldots + \lambda_s - k\lambda_{s+1} =$$

$$\lambda_1 + \ldots + \lambda_{s-k} + \lambda_{s-k+1} + \ldots + \lambda_s - k\lambda_{s+1}.$$

Επειδή γιά κάθε $1 \leq j_1 < \ldots < j_i \leq n$ είναι $\mathrm{ord}_p \frac{1}{\alpha_{j_1}} \cdots \frac{1}{\alpha_{j_i}} \geq \lambda_1 + \ldots + \lambda_i$, έχουμε $\mathrm{ord}_p a_i \geq \lambda_1 + \ldots + \lambda_i = \lambda_1 + \ldots + \lambda_{s-k}$ Όμως προφανώς

$$\lambda_1 + \ldots + \lambda_{s-k} > \lambda_1 + \ldots + \lambda_{s-k} + \lambda_{s-k+1} + \ldots + \lambda_s - k\lambda_{s+1},$$

συνεπώς

$$\mathrm{ord}_p a_i > i\lambda_{s+1} + (\lambda_1 + \ldots + \lambda_s - s\lambda_{s+1}).$$

Λήμμα 4.2 *Έστω* $f = 1 + \sum_{i=1}^{\infty} a_i X^i \in \Omega_p[[X]]$ *και έστω* $b = \sup\{\lambda \ :$ λ *είναι κλίση κάποιου τμήματος του N.P. της* $f\}$. *Τότε η ακτίνα σύγκλισης της* f *είναι* p^b.

Απόδειξη : Έστω $x \in \Omega_p$ με $|x|_p < p^b$, ή αλλιώς $\mathrm{ord}_p > -b$. Θέτουμε $\mathrm{ord}_p x \overset{o\rho\sigma}{=} -b^{'}$ με $-b^{'} > -b$, ή $b^{'} < b$. Θα δείξουμε ότι $\mathrm{ord}_p a_i x^i = \mathrm{ord}_p a_i - ib^{'} \overset{i\to\infty}{\longrightarrow} \infty$. Έστω τμήμα του $N.P.$ της f με κλίση b_1 όπου $b^{'} < b_1 \leq b$.[17] Αν αυτό είναι πεπερασμένου μήκους, έστω ότι έχει άκρα τα σημεία $(i_1, \mathrm{ord}_p a_{i_1})$ και $(i_2, \mathrm{ord}_p a_{i_2})$. Έστω ακόμα ότι η ευθεία που διέρχεται από τα άκρα του τέμνει την $y = b^{'}x$ στο σημείο (x_0, y_0). Θέτουμε $i_0 \overset{o\rho\sigma}{=} \max(i_1, i_2, [x_0]) + 1$. Αν $i > i_0$, θα έχουμε $\mathrm{ord}_p a_i - ib^{'} \geq i(b_1 - b^{'}) \overset{i\to\infty}{\longrightarrow} \infty$.
Αν το τμήμα με κλίση b_1 είναι άπειρο, δηλαδή είναι μία ημιευθεία, έστω $(i_1, \mathrm{ord}_p a_{i_1})$ η αρχή της και έστω (x_0, y_0) το σημείο τομής της ευθείας που διέρχεται από αυτό το τμήμα με την ευθεία $y = b^{'}x$. Θέτουμε $i_0 \overset{o\rho\sigma}{=} \max([x_0], i_1) + 1$. Αν $i > i_0$, τότε $\mathrm{ord}_p a_i - ib^{'} \geq i(b_1 - b^{'}) \overset{i\to\infty}{\longrightarrow} \infty$.
Έστω $x \in \Omega_p$ με $|x|_p > p^b$, ή αλλιώς $\mathrm{ord}_p < -b$. Θέτουμε $\mathrm{ord}_p x \overset{o\rho\sigma}{=} -b^{'}$ με $-b^{'} < -b$, ή $b^{'} > b$. Διακρίνουμε τρεις περιπτώσεις :
i) Έστω ότι υπάρχουν άπειρα το πλήθος τμήματα του $N.P.$ της f με κλίση μικρότερη από b. Τότε, αν $(i_\kappa, \mathrm{ord}_p a_{i_\kappa})$ είναι ένα άκρο τέτοιου τμήματος, έχουμε $\mathrm{ord}_p a_{i_\kappa} - b^{'} i_\kappa < \mathrm{ord}_p a_{i_\kappa} - b i_\kappa < 0$. Αφού τα άκρα αυτά είναι άπειρα, υπάρχει υπακολουθία i_{j_κ} της i_κ τ.ώ. γιά κάθε $j \geq 0$ έχουμε $\mathrm{ord}_p a_{i_{j_\kappa}} - b^{'} i_{j_\kappa} < 0$. Έπεται λοιπόν ότι $\mathrm{ord}_p a_i - b^{'} i \overset{i\to\infty}{\not\longrightarrow} \infty$.
ii) Έστω ότι το $N.P.$ της f έχει τελευταίο άπειρου μήκους τμήμα (προφανώς κλίσης b), με άπειρα σημεία $(i_\kappa, \mathrm{ord}_p a_{i_\kappa})$ πάνω σε αυτό. Τότε γιά κάθε τέτοιο σημείο $(i_\kappa, \mathrm{ord}_p a_{i_\kappa})$ έχουμε $\mathrm{ord}_p a_{i_\kappa} - b^{'} i_\kappa < \mathrm{ord}_p a_{i_\kappa} - b i_\kappa \leq 0$, συνεπώς $\mathrm{ord}_p a_i - b^{'} i \overset{i\to\infty}{\not\longrightarrow} \infty$.
iii) Έστω ότι το $N.P.$ της f έχει τελευταίο άπειρου μήκους τμήμα (προφανώς κλίσης b), με πεπερασμένα το πλήθος σημεία $(i_\kappa, \mathrm{ord}_p a_{i_\kappa})$ πάνω σε αυτό και έστω $(i_\kappa^{'}, \mathrm{ord}_p a_{i_\kappa^{'}})$ εκείνο το σημείο από αυτά, με την μεγαλύτερη τετμημένη. Έστω ότι γιά πεπερασμένα i με $i \geq i_\kappa^{'} + 1$ είναι $\mathrm{ord}_p a_i - b^{'} i < 0$. Ισχύει ότι

$$b = \inf\{\tfrac{\mathrm{ord}_p a_i - \mathrm{ord}_p a_{i_\kappa}^{'}}{i - i_\kappa^{'}} \ : \ i \geq i_\kappa^{'} + 1 \text{ και } a_i \neq 0\} =$$

[17] Υπάρχει τέτοιο από την ιδιότητα του b

$$\min(\inf\{\frac{\mathrm{ord}_p a_i - \mathrm{ord}_p a'_{i_\kappa}}{i - i'_\kappa} \ :\ i \geq i'_\kappa + 1,\ \mathrm{ord}_p a_i - b' i < 0 \text{ και } a_i \neq 0\},$$
$$\inf\{\tfrac{\mathrm{ord}_p a_i - \mathrm{ord}_p a'_{i_\kappa}}{i - i'_\kappa} \ :\ i \geq i'_\kappa + 1,\ \mathrm{ord}_p a_i - b' i \geq 0 \text{ και } a_i \neq 0\}).$$

Όμως γιά κάθε $i \geq i'_\kappa + 1$ με $\mathrm{ord}_p a_i - b' i \geq 0$ έχουμε $\frac{\mathrm{ord}_p a_i - \mathrm{ord}_p a'_{i_\kappa}}{i - i'_\kappa} \geq b' > b$, συνεπώς $\inf\{\frac{\mathrm{ord}_p a_i - \mathrm{ord}_p a'_{i_\kappa}}{i - i'_\kappa} \ :\ i \geq i'_\kappa + 1,\ \mathrm{ord}_p a_i - b' i \geq 0 \text{ και } a_i \neq 0\} > b$, και γιά κάθε ένα από τα πεπερασμένα το πλήθος $i \geq i'_\kappa + 1$ με $\mathrm{ord}_p a_i - b' i < 0$ έχουμε $\frac{\mathrm{ord}_p a_i - \mathrm{ord}_p a'_{i_\kappa}}{i - i'_\kappa} > b$,[18] συνεπώς

$$\inf\{\tfrac{\mathrm{ord}_p a_i - \mathrm{ord}_p a'_{i_\kappa}}{i - i'_\kappa} \ :\ i \geq i'_\kappa + 1,\ \mathrm{ord}_p a_i - b' i < 0 \text{ και } a_i \neq 0\} =$$

$$\min\{\tfrac{\mathrm{ord}_p a_i - \mathrm{ord}_p a'_{i_\kappa}}{i - i'_\kappa} \ :\ i \geq i'_\kappa + 1,\ \mathrm{ord}_p a_i - b' i < 0 \text{ και } a_i \neq 0\} > b.$$

Συνολικά λοιπόν $b = \inf\{\frac{\mathrm{ord}_p a_i - \mathrm{ord}_p a'_{i_\kappa}}{i - i'_\kappa} \ :\ i \geq i'_\kappa + 1 \text{ και } a_i \neq 0\} > b$, άτοπο. Άρα υπάρχουν άπειρα $i \geq i'_\kappa$ με $\mathrm{ord}_p a_i - ib' < 0$, οπότε $\mathrm{ord}_p a_i - b' i \overset{i \to \infty}{\not\longrightarrow} \infty$.

Λήμμα 4.3 *Έστω* $f = \sum_{i=0}^{\infty} a_i X^i \in 1 + X[[\Omega_p]]$ *με* λ_1 *να είναι η κλίση του πρώτου τμήματος του N.P. της και έστω* $c \in \Omega_p$ *με* $\mathrm{ord}_p c = \lambda \leq \lambda_1$. *Υποθέτουμε ότι η* f *συγκλίνει (τουλάχιστον) στο δίσκο* $D(p^\lambda)$. *Θέτουμε* $g = (1 - cX)f \in 1 + X[[\Omega_p]]$. *Τότε το N.P. της* g *προκύπτει αν μεταφέρουμε το N.P. της* f *κατά μία μονάδα δεξιά και κατά* λ *προς τα πάνω και του επισυνάψουμε το ευθύγραμμο τμήμα που ενώνει τα σημεία* $(0,0)$ *και* $(1,\lambda)$. *Επιπλέον, αν η* f *έχει τελευταίο τμήμα κλίσης* λ_f *και συγκλίνει στον* $D(p^{\lambda_f})$, *τότε και η* g *έχει τελευταίο τμήμα κλίσης* λ_f *και συγκλίνει επίσης στον* $D(p^{\lambda_f})$.

Απόδειξη :Έστω ότι το λήμμα ισχύει στην περίπτωση που $c = 1$, άρα $\lambda = 0$ και έστω f, g και $c \in \Omega_p$ με $\mathrm{ord}_p c = \lambda$ που ικανοποιούν τις υποθέσεις του λήμματος, δηλαδή το πρώτο τμήμα του $N.P.$ της f έχει κλίση λ_1, $\mathrm{ord}_p c = \lambda \leq \lambda_1$, η f συγκλίνει στον $D(p^\lambda)$ και $g = (1 - cX)f$. Θέτουμε $f_1 \overset{\text{ορσ}}{=} f(\frac{X}{c})$ και

[18] Αν είχα $\frac{\mathrm{ord}_p a_{i_0} - \mathrm{ord}_p a'_{i_\kappa}}{i_0 - i'_\kappa} \geq b' = b$ γιά κάποιο $i_0 \geq i'_\kappa + 1$, τότε το $(i_0, \mathrm{ord}_p a_{i_0})$ θα ανήκε στο τελευταίο τμήμα του $N.P.$ της f, άτοπο λόγω της ιδιότητας του i'_κ.

$g_1 \overset{\text{ορσ}}{=} (1-X)f_1$. Γιά τις f_1, g_1 ισχύουν : Το πρώτο τμήμα του $N.P.$ της f_1 έχει κλίση $\lambda_1 - \lambda$, [19] γιά $\kappa \overset{\text{ορσ}}{=} 1 \in \Omega_p$ έχουμε $\mathrm{ord}_p\kappa = \mathrm{ord}_p 1 = 0 \le \lambda_1 - \lambda$, η f_1 συγκλίνει στον $D(p^{\mathrm{ord}_p\kappa}) = D(1)$[20] και $g_1 = (1-\kappa X)f_1 = (1-X)f_1$. Ακόμα, αν η f έχει τελευταίο τμήμα κλίσης λ_f και συγκλίνει στον $D(p^{\lambda_f})$, τότε η f_1 έχει τελευταίο τμήμα κλίσης $\lambda_f - \lambda$ και συγκλίνει στον $D(p^{\lambda_f - \lambda})$. Έχουμε δηλαδή ότι οι f_1 και g_1 πληρούν τις υποθέσεις του λήμματος, αν όπου c, λ, λ_1 θέσουμε αντίστοιχα $1, 0, \lambda_1 - \lambda$. Από την υπόθεσή μας λοιπόν, έχουμε ότι το $N.P.$ της g_1 προκύπτει από το $N.P.$ της f_1 αν το μεταφέρουμε κατά μία μονάδα δεξιά και του επισυνάψουμε του ευθύγραμμο τμήμα που ενώνει το $(0,0)$ με το $(1,0)$. Όμως τότε, αφού $g = g_1(cX)$ το $N.P.$ της g προκύπτει από το $N.P.$ της g_1 αν σε αυτό προσθέσουμε την ευθεία $y = \lambda x$. Επειδή τώρα το $N.P.$ της f_1 προκύπτει από το $N.P.$ της f αν από αυτό αφαιρέσουμε την ευθεία $y = \lambda x$, έχουμε συνολικά ότι το $N.P.$ της g θα προκύψει από το $N.P.$ της f αν αυτό μεταφερθεί κατά μία μονάδα δεξιά και κατά λ προς τα πάνω και του επισυνάψουμε το ευθύγραμμο τμήμα που ενώνει τα σημεία $(0,0)$ και $(1,\lambda)$. Επιπλέον έχουμε : Αν η f έχει τελευταίο τμήμα κλίσης λ_f και συγκλίνει στον $D(p^{\lambda_f})$, τότε η f_1 έχει τελευταίο τμήμα κλίσης $\lambda_f - \lambda$ και συγκλίνει στον $D(p^{\lambda_f-\lambda})$, συνεπώς, από την υπόθεσή μας, η g_1 έχει τελευταίο τμήμα κλίσης $\lambda_f - \lambda$ και συγκλίνει στον $D(p^{\lambda_f-\lambda})$. Όμως τότε, αφού $g = g_1(cX)$ και η g_1 συγκλίνει στον $D(p^{\lambda_f-\lambda})$, έπεται ότι η g έχει τελευταίο τμήμα κλίσης λ_f και συγκλίνει στον $D(p^{\lambda_f})$.
Από τα παραπάνω φαίνεται ότι αρκεί να αποδείξουμε την ισχύ του λήμματος στην περίπτωση που $c = 1$, άρα $\mathrm{ord}_p c = \lambda = 0$.

Έστω λοιπόν $g = (1-X)f \overset{\text{ορσ}}{=} 1 + \sum_{i=1}^{\infty} b_i X^i$. Θα έχουμε $b_{i+1} = a_{i+1} - a_i$ γιά $i \ge 0$, συνεπώς $\mathrm{ord}_p b_{i+1} \ge \min(\mathrm{ord}_p a_{i+1}, \mathrm{ord}_p a_i)$ με την ισότητα να ισχύει αν $\mathrm{ord}_p a_{i+1} \ne \mathrm{ord}_p a_i$. Καθώς λ_1 είναι η κλίση του πρώτου τμήματος του $N.P.$ της f_X και $\lambda_1 \ge 0$, έπεται ότι και τα δυο σημεία $(i, \mathrm{ord}_p ai)$, $(i, \mathrm{ord}_p a_{i+1})$ βρίσκονται είτε πάνω στο, ή πάνω από το $N.P.$ της f. Αφού λοιπόν $\mathrm{ord}_p b_{i+1} \ge \min(\mathrm{ord}_p a_{i+1}, \mathrm{ord}_p a_i)$, έπεται ότι το ίδιο θα ισχύει και γιά το σημείο $(i, \mathrm{ord}_p b_{i+1})$. Αν επίσης το σημείο $(i, \mathrm{ord}_p a_i)$ είναι κορυφή του $N.P.$ της f, επειδή πάλι $\lambda_1 \ge 0$, θα είναι $\mathrm{ord}_p a_{i+1} > \mathrm{ord}_p a_i$, άρα $\mathrm{ord}_p b_{i+1} = \mathrm{ord}_p a_i$. Τα παραπάνω δείχνουν ότι : Αν το $N.P.$ της f, δεν έχει τελευταίο άπειρου μήκους τμήμα, τότε αν μεταφερθεί

---

[19] Αν $f = 1 + \sum_{i=1}^{\infty} a_i X^i$, $g = 1 + \sum_{i=1}^{\infty} b_i X^i \in 1 + X\Omega_p[[X]]$ και $c \in \Omega_p$ με $\mathrm{ord}_p c = \lambda$ και $g = f(\frac{X}{c})$, τότε το $N.P.$ της g προκύπτει από το $N.P.$ της f αν από αυτό αφαιρέσουμε την γραμμη $y = \lambda x$. Αυτό ισχύει διότι γιά κάθε $i \ge 1$ έχουμε $\mathrm{ord}_p b_i = \mathrm{ord}_p \frac{a_i}{c^i} = \mathrm{ord}_p a_i - i\lambda$.

[20] Αυτό διότι αν $f(\frac{X}{c}) = 1 + \sum_{i=1}^{\infty} d_i X^i$, τότε $\mathrm{ord}_p d_i = \mathrm{ord}_p a_i - i\lambda \overset{i\to\infty}{\longrightarrow} \infty$, καθώς η f συγκλίνει στον $D(p^{\lambda})$.

κατά μία μονάδα δεξιά και του επισυνάψουμε το ευθύγραμμο τμήμα που ενώνει τα $(0,0)$ και $(1,0)$, προκύπτει το $N.P.$ της g. Αν το $N.P.$ της f, έχει τελευταίο άπειρου μήκους τμήμα κλίσης λ_f, τότε αν κάνουμε την παραπάνω μεταφορά μέχρι και την τελευταία κορυφή του $N.P.$ της f και επισυνάψουμε το ευθύγραμμο τμήμα που ενώνει τα $(0,0)$ και $(1,0)$, το σχήμα που θα προκύψει θα πέσει πάνω στο $N.P.$ της g. Επειδή γιά κάθε $i \geq 0$ έχουμε ότι το σημείο $(i, \mathrm{ord}_p b_{i+1})$ βρίσκεται είτε πάνω στο, ή πάνω από το $N.P.$ της f, γιά να αποδειχθεί το ζητούμενο, απομένει να αποκλείσουμε την περίπτωση το $N.P.$ της g να έχει τμήμα κλίσης έστω λ_g με $\lambda_g > \lambda_f$. Αν το $N.P.$ της g είχε ένα τέτοιο τμήμα, τότε γιά κάποιο i_0 αρκούντως μεγάλο, [21] το σημείο $(i_0+1, \mathrm{ord}_p a_{i_0})$ θα βρισκόταν κάτω από το $N.P.$ της g. Τότε όμως θα είχαμε $\mathrm{ord}_p b_j > \mathrm{ord}_p a_{i_0}$ γιά κάθε $j \geq i_0+1$ και επειδή $\mathrm{ord}_p a_{i+1} \geq \min(\mathrm{ord}_p bi + 1, \mathrm{ord}_p a_i)$, θα ήταν $\mathrm{ord}_p a_j = \mathrm{ord}_p a_{i_0}$ γιά κάθε $j \geq i_0+1$, ατόπο αφού $\mathrm{ord}_p a_i \stackrel{i\to\infty}{\longrightarrow} \infty$[22].
Μένει να δείξουμε ότι αν η f συγκλίνει στον $D(\lambda_f)$ τότε το ίδιο ισχύει και γιά την g.
Έστω $x \in \Omega_p$ με $\mathrm{ord}_p x = \kappa \geq 0$ στο οποίο συγκλίνει η f, δηλαδή $\mathrm{ord}_p a_i + i\kappa \stackrel{i\to\infty}{\longrightarrow} \infty$. Έχουμε $\mathrm{ord}_p b_i + i\kappa \geq \min(\mathrm{ord}_p a_i, \mathrm{ord}_p a_{i-1}) + i\kappa$. Έστω $M > 0$. Βρίσκουμε i_0 τ.ώ. αν $i \geq i_0$ τότε $\mathrm{ord}_p a_i + i\kappa > M$. Αν τώρα $i \geq i_0+1$ έχουμε : αν $\mathrm{ord}_p a_i \leq \mathrm{ord}_p a_{i-1}$ τότε $\min(\mathrm{ord}_p a_i, \mathrm{ord}_p a_{i-1}) + i\kappa = \mathrm{ord}_p a_i + i\kappa > M$, αν $\mathrm{ord}_p a_i \geq \mathrm{ord}_p a_{i-1}$ τότε $\min(\mathrm{ord}_p a_i, \mathrm{ord}_p a_{i-1}) + i\kappa = \mathrm{ord}_p a_{i-1} + i\kappa = \mathrm{ord}_p a_{i-1} + (i-1)\kappa + \kappa > M + \kappa > M$, άρα $\mathrm{ord}_p b_i + i\kappa > M$. Αν $\mathrm{ord}_p x = \kappa < 0$, θεωρούμε $M > \kappa$ και ομοίως βρίσκουμε i_0 τ.ώ. αν $i \geq i_0$ τότε $\mathrm{ord}_p b_i + i\kappa > M + \kappa$. Σε κάθε περίπτωση λοιπόν έχουμε $\mathrm{ord}_p b_i + i\kappa \stackrel{i\to\infty}{\longrightarrow} \infty$, συνεπώς η g συγκλίνει στο x. Όπου λοιπόν συγκλίνει η f, συγκλίνει και η g.

Λήμμα 4.4 *Έστω ότι το πρώτο τμήμα του $N.P.$ της $f = 1 + \sum_{i=1}^{\infty} a_i X^i \in \Omega_p[[x]]$ έχει κλίση λ_1 και ότι διέρχεται από τουλάχιστον ένα σημείο $(i, \mathrm{ord}_p a_i)$. Έστω ακόμα ότι η f συγκλίνει (τουλάχιστον) στο δίσκο $D(p^{\lambda_1})$. Τότε υπάρχει $x \in \Omega_p$ τ.ώ. $\mathrm{ord}_x = -\lambda_1$ και γιά το οποίο ισχύει $f(x) = 0$.*

Απόδειξη : Έστω ότι το λήμμα ισχύει γιά $\lambda_1 = 0$ και έστω $f \in 1 + X\Omega_p[[X]]$ που ικανοποιεί τις υποθέσεις του θεωρήματος. Θέτουμε $\pi \in \Omega_p$ μία από τις ρίζες του $X^i - a_i \in \Omega_p[X]$,[23] όπου $(i, \mathrm{ord}_p a_i)$ είναι ένα από τα σημεία

[21] Το i_0 θα είναι μεγαλύτερο από την τετμημένη του σημείου τομής της ευθείας που διέρχεται από το τελευταίο τμήμα του $N.P.$ της f με την ευθεία που διέρχεται από το τμήμα με κλίση λ_g του $N.P.$ της g.

[22] Αυτό διότι υποθέσαμε ότι η f συγκλίνει στον $D(1)$.

[23] Το Ω_p είναι αλγεβρικά κλειστό, συνεπώς $\pi \in \Omega_p$.

από τα οποία διέρχεται το πρώτο τμήμα του $N.P.$ της f. Παρατηρούμε ότι $i\lambda_i = \mathrm{ord}_p a_i = \mathrm{ord}_p \pi^i = i\mathrm{ord}_p\pi$, άρα $\lambda_1 = \mathrm{ord}_p\pi$. Θέτουμε $g = f(\frac{X}{\pi})$. Η g τώρα ικανοποιεί τις υποθέσεις του θεωρήματος γιά $\lambda_1 = 0$, οπότε υπάρχει $x_2 \in \Omega_p$ τ.ώ. $\mathrm{ord}_p x_2 = 0$ και $g(x_2) = 0$. Θέτοντας $x_1 = \frac{x_2}{\pi}$, έχουμε ότι $\mathrm{ord}_p x_1 = -\lambda_1$ και $f(x_1) = f(\frac{x_2}{\pi}) = g(x_2) = 0$.
Αρκεί λοιπόν να αποδείξουμε την ισχύ του λήμματος γιά $\lambda_1 = 0$.
Έστω λοιπόν ότι $\lambda_1 = 0$ και ότι η f συγκλίνει (τουλάχιστον) στον κλειστό δίσκο $D(1)$. Ειδικότερα έχουμε ότι $\mathrm{ord}_p a_i \overset{i\to\infty}{\longrightarrow} \infty$, συνεπώς υπάρχουν πεπερασμένες τιμές του i γιά τις οποίες $\mathrm{ord}_p a_i = 0$. Έστω $N \geq 1$ η μεγαλύτερη τέτοια τιμή. Θέτουμε $f_n = 1 + \sum_{i=1}^{n} a_i X^i$. Από το λήμμα 4.1 , γιά κάθε $n \geq N$, το f_n έχει ακριβώς N ρίζες, έστω τις $x_{n,1}, \ldots, x_{n,N}$, με $\mathrm{ord}_p x_{n,i} = 0$ γιά $i = 1, \ldots, N$. Θέτουμε $x_N \overset{o\rho\sigma}{=} x_{N,1}$ και γιά κάθε $n \geq N$ θέτουμε x_{n+1} μία οποιαδήποτε x_{n+1,j_0}, όπου $j_0 \in \{1, \ldots, N\}$ που ικανοποιεί τη συνθήκη

$$|x_{n+1,j_0} - x_n|_p = \min_{1\leq i\leq N}(|x_{n+1,i} - x_n|_p).$$

Θα δείξουμε ότι η ακολουθία $\{x_n\}_{n=N}^{\infty}$ είναι Cauchy και ότι το όριό της, έστω $x \in \Omega_p$[24] έχει τις ιδιότητες :

$$\mathrm{ord}_p x = 0 \text{ και } f(x) = 0.$$

Γιά $n \geq N$, έστω S_n σύνολο των ριζών του f_n μαζί με τις πολλαπλότητές τους. Τότε γιά $n \geq N$ έχουμε :

$$|f_{n+1}(x_n) - f_n(x_n)|_p = {}^{25}|f_{n+1}(x_n)|_p = \prod_{\kappa\in S_n} |1 - \frac{x_n}{\kappa}|_p =$$

$$\prod_{i=1}^{N} |1 - \frac{x_n}{x_{n+1,i}}|_p{}^{26} = \prod_{i=1}^{N} |x_{n+1,i} - x_n|_p{}^{27} \geq |x_{n+1} - x_n|_p^{N\,28}.$$

Άρα λοιπόν $|x_{n+1} - x_n|_p^N \leq |f_{n+1}(x_n) - f_n(x_n)|_p = |a_{n+1}x_{n+1}^{n+1}|_p = |a_{n+1}|_p$, ή $|x_{n+1} - x_n|_p \leq |a_{n+1}|_p^{\frac{1}{N}} = p^{-\frac{\mathrm{ord}_p a_n}{N}} \overset{n\to\infty}{\longrightarrow} 0$. Έπεται λοιπόν ότι η $\{x_n\}_{n=N}^{\infty}$ είναι

[24] Το Ω_p είναι πλήρες συνεπώς κάθε ακολουθία Cauchy στοιχείων του Ω_p έχει όριο στο Ω_p
[25] Καθώς $f_n(x_n) = 0$
[26] Αν $\kappa \in S_{n+1}\backslash\{x_{n+1,1}, \ldots, x_{n+1,N}\}$, τότε $\mathrm{ord}_p\frac{1}{\kappa} > 0$. Έχουμε λοιπόν $|1 - \frac{x_n}{\kappa}|_p \leq \max(1, |\frac{x_n}{\kappa}|_p)$ με την ισότητα να ισχύει αν $1 \neq |\frac{x_n}{\kappa}|_p$. Επειδή $\mathrm{ord}_p\frac{x_n}{\kappa} = \mathrm{ord}_p x_n + \mathrm{ord}_p\frac{1}{\kappa} = 0 + \mathrm{ord}_p\frac{1}{\kappa} > 0$, έχουμε $|\frac{x_n}{\kappa}|_p < 1$, άρα $|1 - \frac{x_n}{\kappa}|_p = 1$
[27] Καθώς $|x_{n+1,i}|_p = 1$ γιά $i = 1, \ldots, N$
[28] Από τον τρόπο που επιλέχθηκαν τα x_n

Cauchy.[29] Έστω ότι $x_n \stackrel{n\to\infty}{\longrightarrow} x \in \Omega_p$. Κατ' αρχήν έχουμε $\mathrm{ord}_p x = 0$ διότι : αφού $x_n \stackrel{n\to\infty}{\longrightarrow} x$, έπεται ότι υπάρχει $n_0 \geq N$ τ.ώ. γιά κάθε $n \geq n_0$ είναι $|x - x_n|_p < 1$. Γιά κάποιο $n_1 \geq n_0$ λοιπόν έχουμε $|x|_p \leq \max(|x - x_{n_1}|_p, |x_{n_1}|_p)$ με την ισότητα να ισχύει αν $|x - x_{n_1}|_p \neq |x_{n_1}|_p$. Αφού λοιπόν $|x - x_{n_1}|_p < 1 = |x_{n_1}|_p$, έπεται ότι $|x|_p = 1$, ή $\mathrm{ord}_p x = 0$. Θα δείξουμε τώρα ότι $f(x) = 0$. Έχουμε :

$$|f_n(x)|_p = {}^{30}|f_n(x) - f_n(x_n)|_p = |x - x_n|_p \Big|\sum_{i=1}^{n} a_i \frac{x^i - x_n^i}{x - x_n}\Big|_p \leq {}^{31}|x - x_n|_p \stackrel{n\to\infty}{\longrightarrow} 0.$$

Συνεπώς $f(x) = \lim_{n\to\infty} f_n(x) = 0$.

Λήμμα 4.5 *Έστω ότι η* $f = 1 + \sum_{i=1}^{\infty} a_i X^i \in 1 + x\Omega_p[[X]]$ *συκλίνει στο* $\alpha \in \Omega_p$ *και* $f(\alpha) = 0$.[32] *Έστω ακόμα* $g \stackrel{o\rho\sigma}{=} 1 + \sum_{i=1}^{\infty} b_i X^i = f(1 + \frac{1}{\alpha}X + \frac{1}{\alpha^2}X^2 + \ldots + \frac{1}{\alpha^i}X^i = \ldots)$. *Τότε η* g *συγκλίνει στον* $D(|\alpha|_p)$.

Απόδειξη : Έστω $f_n = 1 + \sum_{i=1}^{n} a_i X^i$. Τότε θα έχουμε $b_i = a_i + \frac{a_{i-1}}{\alpha} + \ldots + \frac{a_1}{\alpha^{i-1}} + \frac{1}{\alpha^i}$, άρα $b_i \alpha^i = f_i(\alpha)$. Αν λοιπόν $x \in D(|\alpha|_p)$, τότε : $|b_i x^i|_p \leq |b_i \alpha^i|_p = |f_i(\alpha)|_p \stackrel{i\to\infty}{\longrightarrow} f(\alpha) = 0$. Άρα λοιπόν η g συγκλίνει στο x.

Θεώρημα 4.1 (Weierstrass) *Έστω* $f = 1 + \sum_{i=1}^{\infty} a_i X^i \in 1 + X\Omega_p[[X]]$ *η οποία συγκλίνει (τουλάχιστον) στο δίσκο* $D(p^\lambda)$. *Αν το N.P. της* f *έχει τμήματα με κλίση μεγαλύτερη από* λ, *έστω* N *το συνολικό οριζόντιο μήκος των τμημάτων του με κλίση μικρότερη η ίση από* λ.
Αν το N.P. της f *έχει τελευταίο άπειρου μήκους τμήμα κλίσης* λ *με πεπερασμένα το πλήθος σημεία* $(i, \mathrm{ord}_p a_i)$ *επάνω του, έστω* N *το μεγαλύτερο* i *γιά το οποίο το* $(i, \mathrm{ord}_p a_i)$ *είναι ένα από αυτά τα σημεία.*[33]

---

[29] Σε έναν μη-αρχιμήδειο μετρικό χώρο, $(X, |\cdot|)$όπως το $(\Omega_p, |\cdot|_p)$, ισχύει ότι μία ακολουθία $\{x_n\}_{n=1}^{\infty}$ στοιχείων του X είναι Cauchy αν και μόνο εαν ισχύει $|x_{n+1} - x_n|_p \stackrel{n\to\infty}{\longrightarrow} 0$

[30] Καθώς $f_n(x_n) = 0$

[31] Καθώς $\mathrm{ord}_p a_i \geq 0$, ή $|a_i|_p \leq 1$, και $|\frac{x^i - x_n^i}{x - x_n}|_p = |x^{i-1} + x^{i-2}x_n + \ldots + x x_{n^{i-2}} + x_n^{i-1}|_p \leq 1$, με την τελευταία ανισότητα να ισχύει διότι $|x_n|_p = 1$ και $|x|_p = 1$

[32] Προφανώς $\alpha \neq 0$, αφού αν ήταν έτσι, θα είχαμε $0 = f(\alpha) = 1$

[33] Λόγω του ότι η f συγκλίνει στον κλειστό δίσκο $D(p^\lambda)$, αποκλείεται η περίπτωση το πολύγωνο του Newton της f να έχει άπειρα το πλήθος τμήματα με κλίση μικρότερη ή ίση από λ.

Τότε υπάρχει ένα πολυώνυμο $h \in 1 + X\Omega_p[X]$ *βαθμού* N *και μία δυναμοσειρά* $g = 1 + \sum_{i=1}^{\infty} b_i X^i \in 1 + X\Omega_p[[X]]$, *η οποία συγκλίνει και δε μηδενίζεται στο δίσκο* $D(p^\lambda)$ *γιά τα οποία ισχύει η σχέση* $h = f \cdot g$. *Το πολυώνυμο* h *καθορίζεται μονοσήμαντα από αυτές τις ιδιότητες και το* $N.P.$ *του συμπίπτει με εκείνο της* f *ως το σημείο* $(N, \mathrm{ord}_p a_N)$.

Απόδειξη. Έστω ότι το θεώρημα ισχύει στην περίπτωση που $\lambda = 0$ και έστω f που ικανοποιεί τις υποθέσεις του θεωρήματος. Δηλαδή η f συγκλίνει στον $D(p^\lambda)$ και ακόμα : αν το $N.P.$ της f έχει τμήματα με κλίση μεγαλύτερη από λ, έστω N το συνολικό οριζόντιο μήκος των τμημάτων του με κλίση μικρότερη η ίση από λ, ενώ αν το $N.P.$ της f έχει τελευταίο άπειρου μήκους τμήμα κλίσης λ με πεπερασμένα το πλήθος σημεία $(i, \mathrm{ord}_p a_i)$ επάνω του, έστω N το μεγαλύτερο i γιά το οποίο το $(i, \mathrm{ord}_p a_i)$ είναι ένα από αυτά τα σημεία. Έστω $c \in \Omega_p$ με $\mathrm{ord}_p c = \lambda$. Θέτουμε $f_1 \overset{\text{ορσ}}{=} f(\frac{X}{c})$. Γιά την f_1 ισχύουν : συγκλίνει στον $D(p^0) = D(1)$,[34] αν το $N.P.$ της f έχει τμήματα με κλίση μεγαλύτερη από λ τότε το συνολικό οριζόντιο μήκος των τμημάτων του $N.P.$ της f_1 με κλίση μικρότερη η ίση από 0 είναι N, ενώ αν το $N.P.$ της f έχει τελευταίο άπειρου μήκους τμήμα κλίσης λ με πεπερασμένα το πλήθος σημεία $(i, \mathrm{ord}_p a_i)$ επάνω του τότε το $N.P.$ της f_1 έχει τελευταίο άπειρου μήκους τμήμα κλίσης 0 με πεπερασμένα το πλήθος σημεία $(i, \mathrm{ord}_p a_i)$ επάνω του και N είναι το μεγαλύτερο i γιά το οποίο το $(i, \mathrm{ord}_p a_i)$ είναι ένα από αυτά τα σημεία. Από την ισχύ του θεωρήματος για την περίπτωση που $\lambda = 0$, έχουμε ότι : υπάρχει πολυώνυμο $h_1 \in 1 + X\Omega_p[X]$ βαθμού N και δυναμοσειρά $g_1 = 1 + \sum_{i=1}^{\infty} b_{1,i} X^i$ που συγκλίνει και δε μηδενίζεται στον $D(1)$ τ.ώ. $h_1 = f_1 g_1$. Επίσης το h_1 είναι μοναδικά καθορισμένο από αυτές τις ιδιότητες [35] και το $N.P.$ του συμπίπτει με αυτό της f_1 ως το σημείο $(N, \mathrm{ord}_p a_N)$. Θέτουμε τώρα $h \overset{\text{ορσ}}{=} h_1(cX)$ και $g \overset{\text{ορσ}}{=} g_1(cX)$ και έχουμε : $h = h_1(cX) = f_1(cX) g_1(cX) = f \cdot g$, η g συγκλίνει και δε μηδενίζεται στον $D(p^\lambda)$, [36] το h είναι μοναδικά καθορισμένο από αυτές τις ιδιότητες [37] και το $N.P.$ του h συμπίπτει με αυτό του f ως το

[34] Αυτό διότι λόγω της σύγκλισης της f στον $D(p^\lambda)$ έχουμε $\mathrm{ord}_p a_i + i\lambda \overset{i \to \infty}{\longrightarrow} \infty$

[35] Ειδικότερα, έχει τις ίδιες ρίζες (N το πλήθος) με το f_1 στον $D(1)$ και σταθερό όρο μονάδα.

[36] Αν $g = 1 + \sum_{i=1}^{\infty} b_i X^i$, τότε έχουμε $b_i = c^i b_{1,i}$. Από τη σύγκλιση της g_1 στον $D(1)$ έχουμε $\mathrm{ord}_p b_{1,i} = \mathrm{ord}_p \frac{b_i}{c^i} = \mathrm{ord}_p b_i - i\lambda \overset{i \to \infty}{\longrightarrow} \infty$, συνεπώς η g συγκλίνει στον $D(p^\lambda)$. Αν ακόμα υπήρχε $\alpha \in D(p^\lambda)$ με $g(\alpha) = 0$, τότε $c\alpha \in D(1)$ και $g_1(c\alpha) = g(\alpha) = 0$, άτοπο. Άρα η g δε μηδενίζεται στον $D(p^\lambda)$.

[37] Έχει τις ίδιες ρίζες (N το πλήθος) με το f στον $D(p^\lambda)$ και σταθερό όρο μονάδα. Αυτό ισχύει διότι : $\alpha \in D(1)$ και $f_1(\alpha) = 0$ αν και μόνο αν $\frac{\alpha}{c} \in D(p^\lambda)$ και $f(\frac{\alpha}{c}) = 0$. Ομοίως

σημείο $(N, \mathrm{ord}_p a_N)$. [38]
Τα παραπάνω δείχνουν ότι αρκεί να αποδείξουμε το θεώρημα στην περίπτωση που $\lambda = 0$.
Έστω λοιπόν $f = 1 + \sum_{i=1}^{\infty} a_i X^i$, N και $\lambda(=0)$, όπως στην εκφώνηση του θεωρήματος. Θα κάνουμε επαγωγή ως προς το N. Έστω $N = 0$. Θα δείξουμε ότι η $f^{-1} \overset{\text{ορσ}}{=} g = 1 + \sum_{i=1}^{\infty} b_i X^i$ συγκλίνει και δε μηδενίζεται στον $D(1)$. Από την υπόθεση έχουμε ότι $\mathrm{ord}_p a_i > 0$ γιά κάθε $i \geq 1$ και $\mathrm{ord}_p a_i \overset{i\to\infty}{\longrightarrow} \infty$. Καθώς $f \cdot g = 1$ έπεται ότι $b_i = -(b_{i-1}a_1 + b_{i-2}a_2 + \ldots + b_1 a_{i-1} + a_i)$ γιά $i \geq 1$. Αφού όμως $\mathrm{ord}_p a_i > 0$ γιά κάθε $i \geq 1$, θα είναι και $\mathrm{ord}_p b_i > 0$ γιά κάθε $i \geq 1$. Κατόπιν θα δείξουμε πως $\mathrm{ord}_p b_i \overset{i\to\infty}{\longrightarrow} \infty$. Έστω $M > 0$. Βρίσκουμε m τ.ώ. αν $i > m$ τότε $\mathrm{ord}_p a_i > M$. Θέτουμε

$$\epsilon \overset{\text{ορσ}}{=} \min(\mathrm{ord}_p a_1, \ldots, \mathrm{ord}_p a_m) > 0.$$

Θα δείξουμε ότι

$$i > nm \Rightarrow \mathrm{ord}_p b_i > \min(M, n\epsilon).$$

Αν αυτό δειχθεί, τότε θα έχουμε ότι $\mathrm{ord}_p b_i \overset{i\to\infty}{\longrightarrow} \infty$.[39] Θα δείξουμε την ισχύ της συνεπαγωγής επαγωγικά ως προς το n. Γιά $n = 0$ ισχύει τετριμμένα, καθώς η συνεπαγωγή $i > 0 \Rightarrow \mathrm{ord}_p > 0$ είναι αληθής. Έστω ότι η συνεπαγωγή είναι αληθής γιά $n - 1$ με $n \geq 1$ και έστω $i > nm$. Έχουμε $b_i = -(b_{i-1}a_1 + \ldots + b_{i-m}a_m + b_{i-(m+1)}a_{m+1} + \ldots + a_i)$. Γιά τους όρους $b_{i-j}a_j$ με $j > m$ έχουμε

$$\mathrm{ord}_p b_{i-j} a_j > \mathrm{ord}_p a_j > M$$

ενώ γιά τους όρους με $j \leq m$ έχουμε

$$\mathrm{ord}_p b_{i-j} a_j \geq \mathrm{ord}_p b_{i-j} + \epsilon >^{40} \min(M, (n-1)\epsilon) + \epsilon.$$

$h_1(\alpha) = 0$ αν και μόνο αν $h(\frac{\alpha}{c}) = 0$. Επειδή τώρα το h_1 έχει τις ίδιες ρίζες (N το πλήθος) με το f_1 στον $D(1)$ και σταθερό όρο μονάδα, έπεται ότι το h έχει τις ίδιες ρίζες (N το πλήθος) με το f στον $D(p^\lambda)$ και σταθερό όρο μονάδα.

[38]Το $N.P.$ της f_1 προκύπτει από αυτό της f αν του αφαιρέσουμε την ευθεία $y = \lambda x$. Το $N.P.$ του h_1 συμπίπτει με αυτό της f_1 ως το σημείο $(N, \mathrm{ord}_p a_N)$. Το $N.P.$ του h προκύπτει από αυτό του h_1 αν σε αυτό προσθέσουμε την ευθεία $y = \lambda x$, συνεπώς το $N.P.$ του h συμπίπτει με αυτό του f ως το σημείο $(N, \mathrm{ord}_p a_N)$.

[39]Έστω ότι ισχύει η συνεπαγωγή $i > nm \Rightarrow \mathrm{ord}_p b_i > \min(M, n\epsilon)$. Βρίσκουμε n_0 τ.ώ. $n_{0\epsilon \geq M}$. Αν τώρα $i > n_0 m$, από την ισχύ της συνεπαγωγής έχουμε ότι $\mathrm{ord}_p b_i > \min(M, n_0\epsilon) = M$. Αφού το M ήταν τυχαίο, έπεται ότι $\mathrm{ord}_p b_i \overset{i\to\infty}{\longrightarrow} \infty$.

[40]$i + m - j \geq i > mn$, άρα $i + m - j > nm$, ή ισοδύναμα $i - j > m(n-1)$. Από την επαγωγική υπόθεση λοιπόν έχουμε $\mathrm{ord}_p b_{i-j} > \min(M, (n-1)\epsilon)$.

Γιά όλους λοιπόν τους όρους $b_{i-j}a_j$ με $j = 1, \ldots, i$, έχουμε

$$\mathrm{ord}_p b_{i-j} a_i > \min(M, n\epsilon).^{41}$$

Συνολικά λοιπόν συμπεραίνουμε ότι η $g = 1+\sum_{i=1}^{\infty} b_i X^i = 1-\sum_{i=1}^{\infty}(b_{i-1}a_1+b_{i-2}a_2+ \ldots + b_1 a_{i-1} + a_i)X^i$ συγκλίνει στον $D(1)$. Επίσης η g δε μηδενίζεται στον $D(1)$ καθώς αν υπήρχε $\alpha \in D(1)$ με $g(\alpha) = 0$, τότε θα είχαμε $1 = f(\alpha)g(\alpha) = 0$ άτοπο. Κατά τετριμμένο τρόπο ακόμα ισχύει ότι οι ρίζες του σταθερού πολυωνύμου 1 είναι ακριβώς εκείνες της f στον $D(1)$. Έστω $N \geq 1$ και έστω ότι το θεώρημα ισχύει γιά $N - 1$. Έστω $\lambda_1 \leq 0$ η κλίση του πρώτου τμήματος του. $N.P.$ της f. Αφού $N \geq 1$ και $\lambda_1 \leq 0$, έπεται ότι η f, εκτός από το ότι συγκλίνει στον $D(p^{\lambda_1}) \subseteq D(1)$, το πρώτο τμήμα του $N.P.$ της διέρχεται από τουλάχιστον ένα σημείο $(i, \mathrm{ord}_p a_i) \neq (0, 0)$. Από το λήμμα 4.4, σελ. 40 λοιπόν, έχουμε ότι υπάρχει $\alpha \in \Omega_p$ με $\mathrm{ord}_p \alpha = -\lambda_1$ και $f(\alpha) = 0$. Έστω

$$f_1 = f(1 + \tfrac{X}{\alpha} + \tfrac{X^2}{\alpha^2} + \ldots + \tfrac{X^i}{\alpha^i} + \ldots) \in 1 + X\Omega_p[[X]].$$

Από το λήμμα 4.5, σελ. 42, η f_1 συγκλίνει στον $D(|\alpha|_p) = D(p^{\mathrm{ord}_p \alpha}) = D(p^{\lambda_1})$. Καθώς $\alpha \neq 0$,[42] θέτουμε $c \overset{\text{ορσ}}{=} \frac{1}{\alpha}$, οπότε έχουμε $f = (1 - cX)f_1$. Αν το $N.P.$ της f_1 είχε πρώτο τμήμα κλίσης $\lambda_1^{'} < \lambda_1$, τότε από το λήμμα 4.4, σελ, 40, θα υπήρχε $b \in \Omega_p$ με $f_1(b) = 0$ και $\mathrm{ord}_p = -\lambda_1^{'}$,[43] άρα θα ήταν και $f(b) = 0$, άτοπο. Άρα $\lambda_1^{'} \geq \lambda_1$, συνεπώς ισχύουν οι υποθέσεις του λήμματος 4.3, σελ. 38, όπου τη θέση των $f, g, \lambda_1, \lambda, c$ της εκφώνησης έχουν οι $f_1, f, \lambda_1^{'}, \lambda_1, \frac{1}{\alpha} = c$ αντίστοιχα. Από το λήμμα λοιπόν 4.3, έχουμε ότι η f_1 έχει το ίδιο $N.P.$ με αυτό της f, αν αφαιρέσει κανείς το ευθύγραμμο τμήμα με άκρα τα $(0, 0)$, $(1, \lambda_1)$, και ακόμα αν η f, άρα και η f_1, έχει τελευταίο τμήμα κλίσης $\lambda = 0$, επειδή η f συγκλίνει στον $D(1)$, το ίδιο θα ισχύει και γιά την f_1. Έχουμε λοιπόν ότι η f_1 ικανοποιεί τις υποθέσεις του θεωρήματος, με το $N-1$ στη θέση του N. Από την

[41] Αν $(n-1)\epsilon \leq M \leq n\epsilon$ τότε γιά $j > m$ έχουμε $\mathrm{ord}_p b_{i-j} a_j > M = \min(M, n\epsilon)$ και γιά $j \leq m$ έχουμε $\mathrm{ord}_p b_{i-j} a_j > \min(M, (n-1)\epsilon) + \epsilon = (n-1)\epsilon + \epsilon = n\epsilon \geq M = \min(M, n\epsilon)$, άρα γιά κάθε $j = 1, \ldots, i$ έχουμε $\mathrm{ord}_p b_{i-j} a_j > \min(M, n\epsilon)$. Αν $M \leq (n-1)\epsilon \leq n\epsilon$ τότε γιά $j > m$ έχουμε $\mathrm{ord}_p b_{i-j} a_j > M = \min(M, n\epsilon)$ και γιά $j \leq m$ έχουμε $\mathrm{ord}_p b_{i-j} a_j > \min(M, (n-1)\epsilon) + \epsilon = M + \epsilon > M = \min(M, n\epsilon)$, άρα πάλι γιά κάθε $j = 1, \ldots, i$ έχουμε $\mathrm{ord}_p b_{i-j} a_j > \min(M, n\epsilon)$. Αν $(n-1)\epsilon \leq n\epsilon \leq M$ τότε γιά $j > m$ έχουμε $\mathrm{ord}_p b_{i-j} a_j > M \geq n\epsilon = \min(M, n\epsilon)$ και γιά $j \leq m$ έχουμε $\mathrm{ord}_p b_{i-j} a_j > \min(M, (n-1)\epsilon) + \epsilon = (n-1)\epsilon + \epsilon = n\epsilon = \min(M, n\epsilon)$, άρα πάλι γιά κάθε $j = 1, \ldots, i$ έχουμε $\mathrm{ord}_p b_{i-j} a_j > \min(M, n\epsilon)$.

[42] Βλ. Λήμμα 4.5, σελ. 42.

[43] Επειδή η f_1 συγκλίνει στον $D(p^{\lambda_1}) \supset D(p^{\lambda_1^{'}})$, έπεται ότι είτε το $N.P.$ της έχει τμήματα με κλίσεις $> \lambda_1 > \lambda_1^{'}$, ή έχει τελευταίο τμήμα κλίσης λ_1 με πεπερασμένα σημεία $(i, \mathrm{ord}_p a_i)$ πάνω σε αυτό. Όμως αφού $\lambda_1 > \lambda_1^{'}$, το πρώτο τμήμα του $N.P.$ της, κλίσης $\lambda_1^{'}$ θα διέρχεται από τουλάχιστον ένα σημείο $(i, \mathrm{ord}_p a_i) \neq (0, 0)$.

επαγωγική υπόθεση τώρα υπάρχει πολυώνυμο $h_1 \in 1 + X\Omega_p[X]$ βαθμού $N-1$ και δυναμοσειρά $g \in 1 + X\Omega_p[[X]]$, η οποία συγκλίνει και δε μηδενίζεται στον $D(1)$ τ.ώ.

$$h_1 = f_1 g,$$

οι ρίζες του h_1 είναι ακριβώς οι $N-1$ το πλήθος ρίζες του f_1 στον $D(1)$ και το $N.P.$ του συμπίπτει με αυτό του f_1 ως το σημείο $(N-1, \mathrm{ord}_p a_{N-1})$. Πολλαπλασιάζοντας τώρα τη σχέση 4 με $1-cX$ και θέτοντας $h \overset{\text{ορσ}}{=} (1-cX)h_1$ έχουμε $h = f \cdot g$ όπου οι ρίζες του h είναι ακριβώς οι N ρίζες του f στον $D(1)$[44] και $h \in 1 + X\Omega_p[X]$. Έχουμε λοιπόν ότι το h είναι μονοσήμαντα καθορισμένο και ακόμα ότι, αφού το $N.P.$ του h προκύπτει από το $N.P.$ του h_1, αν του επισυνάψουμε το ευθύγραμμο τμήμα με άκρα τα $(0,0)$, $(1, \lambda_1)$, το $N.P.$ του h συμπίπτει με αυτό του f ως το σημείο $(N, \mathrm{ord}_p a_N)$.

Πόρισμα 4.1 *Έστω $f \in 1+X\Omega_p[[X]]$ η οποία συγκλίνει στο Ω_p. Τότε υπάρχει μοναδικό πολυώνυμο $h \in 1 + X\Omega_p[X]$ και δυναμοσειρά $g \in 1 + X\Omega_p[[X]]$, οποία συγκλίνει και δε μηδενίζεται στο Ω_p, τ.ώ. να ισχύει η σχέση $h = f \cdot g$.*

[44] Σημειωτέον ότι $\frac{1}{c} = \alpha \in D(1)$.

5 Υπερεπιφάνειες - Συναρτήσεις ζήτα - Το θεώρημα του Dwork.

Έστω F σώμα. Συμβολίζουμε με $\mathbb{A}_F^n$ και ονομάζουμε *n-διάστο αφφινικό χώρο πάνω από το σώμα F*, το σύνολο των διατεταγμένων n-άδων $(x_1, \ldots, x_n)$ με $x_i \in F$ γιά $i = 1, \ldots, n$.
Έστω $S \subseteq F[X_1, \ldots, X_n]$. Ονομάζουμε *αφφινική υπερεπιφάνεια ορισμένη από το S στον* $\mathbb{A}_F^n$ το σύνολο

$$H_S \overset{\text{ορσ}}{=} \{(x_1, \ldots, x_n) \in \mathbb{A}_F^n \ : \ f(x_1, \ldots, x_n) = 0 \ \ \forall f \in S\}$$

και καλούμε *διάστασή* του τον αριθμό $n-1$. Αν $S = \{f_1, \ldots, f_m\}$, τότε, γιά λόγους απλούστευσης του συμβολισμού, θα γράφουμε $H_{f_1,\ldots,f_m}$ αντί γιά $H_{\{f_1,\ldots,f_m\}}$.

Επιπλέον, συμβολίζουμε με $\mathbb{P}_F^n$ και ονομάζουμε *n-διάστο προβολικό χώρο πάνω από το σώμα F*, το σύνολο των κλάσεων ισοδυναμίας των στοιχείων του $\mathbb{A}_F^{n+1} \backslash \{(0, \ldots, 0)\}$ ως προς τη σχέση ισοδυναμίας $(x_0, \ldots, x_n) \sim (x_0', \ldots, x_n') \Leftrightarrow \exists \lambda \in F^\times \ : \ x_i' = \lambda x_i$, γιά $i = 0, \ldots, x_n$.
Την κλάση ισοδυναμίας ενός στοιχείου του $\mathbb{A}_F^{n+1} \backslash \{(0, \ldots, 0)\}$ ως προς τη σχέση αυτή, θα τη συμβολίζουμε $[x_0, \ldots, x_n]$.
Σε αυτό το σημείο παρατηρούμε ότι ισχύει η σχέση

$$\mathbb{P}_F^n = \mathbb{A}_F^n \uplus \mathbb{A}_F^{n-1} \uplus \cdots \uplus \mathbb{A}_F^1 \uplus (0, \ldots, 1) \,, \tag{14}$$

(όπου $\uplus \overset{\text{ορσ}}{=}$ξένη ένωση), κατόπιν της ταυτίσεως $[1, x_1, \ldots, x_n] \leftrightarrow (x_1, \ldots, x_n)$, $[0, 1, x_1, \ldots, x_{n-1}] \leftrightarrow (x_1, \ldots, x_{n-1})$, ..., $[0, \ldots, 1, x_1] \leftrightarrow x_1$, $[0, \ldots, 1] \leftrightarrow 1$.

Ως *ομογενές πολυώνυμο βαθμού d*, ορίζεται ένα οποιοδήποτε πολυώνυμο $f(X_0, \ldots, X_n) \in F[X_0, \ldots, X_n]$, που είναι γραμμικός συνδυασμός μονονύμων του ιδίου συνολικού βαθμού d.
Δοθέντος ενός πολυωνύμου $f(X_1, \ldots, X_n) \in F[X_1, \ldots, X_n]$ βαθμού d, ως *ομογενής του πλήρωση*, $\overline{f}(X_0, \ldots, X_n)$, καλείται το πολυώνυμο $X_0^d f(\frac{X_1}{X_0}, \ldots, \frac{X_n}{X_0})$, το οποίο είναι ομογενές βαθμού d.
Παρατηρούμε ότι αν κάποιο πολυώνυμο $\overline{f}(X_0, \ldots, X_n)$ είναι ομογενές, και αν $\overline{f}(x_0, \ldots, x_n) = 0$ γιά κάποιο $(x_0, \ldots, x_n) \in \mathbb{A}_F^{n+1}$, τότε ισχύει και $\overline{f}(\lambda x_0, \ldots, \lambda x_n) = 0$ γιά κάθε $\lambda \in F^\times$, συνεπώς έχει νόημα να κάνει κανείς λόγο γιά το σύνολο των στοιχείων του $\mathbb{P}_F^n$ που μηδενίζουν το $\overline{f}$.
Κατόπιν λοιπόν των παραπάνω, αν $S \subseteq F[X_0, \ldots, X_n]$ με $\overline{f}$ ομογενές γιά κάθε $\overline{f} \in S$, ορίζουμε ως *προβολική υπερεπιφάνεια ορισμένη από το S στο* $\mathbb{P}_F^n$ το σύνολο

$$\overline{H}_S \overset{\text{ορσ}}{=} \{[x_0, \ldots, x_n] \in \mathbb{P}_F^n \ : \ \overline{f}([x_0, \ldots, x_n]) = 0 \ \ \forall \overline{f} \in S\}.$$

Αν $S = \{\overline{f}_1, \ldots, \overline{f}_m\}$, τότε, γιά λόγους απλούστευσης του συμβολισμού, θα γράφουμε $\overline{H}_{\overline{f}_1,\ldots,\overline{f}_m}$ αντί γιά $\overline{H}_{\{\overline{f}_1,\ldots,\overline{f}_m\}}$.

Έστω σώμα K με $F \subset K$. Αν $f(X_1, \ldots, X_n) \in F[X_1, \ldots, X_n]$, τότε και $f(X_1, \ldots, X_n) \in K[X_1, \ldots, X_n]$, συνεπώς, αν $S \subseteq F[X_1, \ldots, X_n]$, μπορούμε να ορίσουμε το σύνολο

$$H_S(K) \overset{\text{ορσ}}{=} \{(x_1, \ldots, x_n) \in \mathbb{A}^n_K \ : \ f(x_1, \ldots, x_n) = 0 \ \ \forall f \in S\} .$$

Αν $S \subseteq F[X_0, \ldots, X_n]$ με $\overline{f}$ ομογενές γιά κάθε $\overline{f} \in S$, όμοια ορίζουμε το σύνολο

$$\overline{H}_S(K) \overset{\text{ορσ}}{=} \{[x_0, \ldots, x_n] \in \mathbb{P}^n_{\mathbb{K}} \ : \ \overline{f}([x_0, \ldots, x_n]) = 0 \ \ \forall \overline{f} \in S\} .$$

Από εδώ και στο εξής θα αναφερόμαστε σε πεπερασμένα σώματα $F = \mathbb{F}_q$ και πεπερασμένες επεκτάσεις τους $K = \mathbb{F}_{q^s}$. Στις περιπτώσεις αυτές παρατηρούμε ότι τα σύνολα $H_S(K)$ και $\overline{H}_S(K)$ είναι πεπερασμένα, καθώς $\#H_S(\mathbb{F}_{q^s}) \leq \#\mathbb{A}^n_{\mathbb{F}_{q^s}} = q^{sn}$ και $\#\overline{H}_S(\mathbb{F}_{q^s}) \leq \#\mathbb{P}^n_{\mathbb{F}_{q^s}} = q^{sn} + \ldots + q^s + 1$.
Γιά κάθε $s \geq 1$ θέτουμε

$$N_s \overset{\text{ορσ}}{=} \#H_S(\mathbb{F}_{q^s}) \quad \text{και} \quad \overline{N}_s \overset{\text{ορσ}}{=} \#\overline{H}_S(\mathbb{F}_{q^s})$$

και ορίζουμε αντίστοιχα τις *συναρτήσεις ζήτα* των H_S και $\overline{H}_S$ ως τις τυπικές δυναμοσειρές

$$Z(H_S/\mathbb{F}_q; T) \overset{\text{ορσ}}{=} \exp(\sum_{s=1}^{\infty} N_s \frac{T^s}{s}) \in \mathbb{Q}[[T]]$$

και

$$Z(\overline{H}_S/\mathbb{F}_q; T) \overset{\text{ορσ}}{=} \exp(\sum_{s=1}^{\infty} \overline{N}_s \frac{T^s}{s}) \in \mathbb{Q}[[T]] .$$

Από το θεώρημα βάσης του Hilbert έπεται ότι, γιά κάθε $S \subseteq F[X_1, \ldots, X_n]$ υπάρχει πεπερασμένο σύνολο $S^{'} \subseteq F[X_1, \ldots, X_n]$, τέτοιο ώστε $H_S = H_{S'}$, καθώς επίσης και ότι γιά κάθε σύνολο $S \subseteq F[X_0, \ldots, X_n]$ ομογενών πολυωνύμων υπάρχει πεπερασμένο σύνολο ομογενών πολυωνύμων $S^{'} \subseteq F[X_0, \ldots, X_n]$, τέτοιο ώστε $\overline{H}_S = \overline{H}_{S'}$. Έπεται λοιπόν ότι

$$Z(H_S/\mathbb{F}_q; T) = Z(H_{S'}/\mathbb{F}_q; T) \text{ και } Z(\overline{H}_S/\mathbb{F}_q; T) = Z(\overline{H}_{S'}/\mathbb{F}_q; T).$$

Θεώρημα 5.1 (Dwork) *Η συνάρτηση ζήτα κάθε αφφινικής υπερεπιφάνειας ορισμένης από κάποιο πολυώνυμο $f(X_1, \ldots, X_n)$ στον $\mathbb{A}^n_{\mathbb{F}_q}$ και κάθε προβολικής υπερεπιφάνειας ορισμένης από κάποιο ομογενές πολυώνυμο $\overline{f}(X_0, \ldots, X_n)$ στον $\mathbb{P}^n_{\mathbb{F}_q}$, όπου το $\mathbb{F}_q$ είναι πεπερασμένο σώμα, είναι κλάσμα δυο πολυωνύμων με συντελεστές στο $\mathbb{Z}$ και σταθερό συντελεστή μονάδα.*

Θα δούμε αμέσως παρακάτω ότι συνέπεια του θεωρήματος 5.1 είναι ότι η συνάρτηση ζήτα κάθε αφφινικής υπερεπιφάνειας ορισμένης από κάποιο σύνολο $S \subseteq \mathbb{F}_q[X_1, \ldots, X_n]$ στον $\mathbb{A}^n_{\mathbb{F}_q}$ και κάθε προβολικής υπερεπιφάνειας ορισμένης από κάποιο σύνολο ομογενών πολυωνύμων $S \subseteq \mathbb{F}_q[X_0, \ldots, X_n]$ στον $\mathbb{P}^n_{\mathbb{F}_q}$ είναι κλάσμα δυο πολυωνύμων με συντελεστές στο $\mathbb{Z}$ και σταθερό όρο μονάδα.

Σύμφωνα με ότι προηγήθηκε του θεωρήματος , αρκεί αυτό να δειχθεί γιά την περίπτωση που το S είναι πεπερασμένο.
Έστω, λοιπόν, ότι έχει αποδειχθεί το θεώρημα 5.1, και $S = \{f_1, f_2\} \subseteq \mathbb{F}_q[X_1, \ldots, X_n]$. Θέτουμε $N_{f_1,s} = \#H_{f_1}(\mathbb{F}_{q^s})$, $N_{f_2,s} = \#H_{f_2}(\mathbb{F}_{q^s})$, $N_{S,s} = \#H_S(\mathbb{F}_{q^s})$ και $N_{f_1 \cdot f_2,s} = \#H_{f_1 \cdot f_2}(\mathbb{F}_{q^s})$. Έχουμε ότι $N_{f_1 \cdot f_2,s} = N_{f_1,s} + N_{f_2,s} - N_{S,s}$, συνεπώς,

$$\begin{aligned} Z(H_{f_1,f_2}/\mathbb{F}_q; T) &= \exp(\sum_{s=1}^{\infty} N_{S,s} \frac{T^s}{s}) \\ &= \exp(\sum_{s=1}^{\infty} (N_{f_1,s} + N_{f_2,s} - N_{f_1 \cdot f_2,s}) \frac{T^s}{s}) \\ &= \frac{Z(H_{f_1}/\mathbb{F}_q; T) Z(H_{f_2}/\mathbb{F}_q; T)}{Z(H_{f_1 \cdot f_2}/\mathbb{F}_q; T)} , \end{aligned}$$

το οποίο είναι προφανώς κλάσμα πολυωνύμων με συντελεστές στο $\mathbb{Z}$ και σταθερό όρο μονάδα.
Αν τώρα $\#S = k \geq 3$, τότε το ζητούμενο έπεται επαγωγικά με τη βοήθεια της συνδυαστικής *αρχής εγκλεισμού-αποκλεισμού*: Αν $A_1, \ldots, A_n$ είναι πεπερασμένα σύνολα, τότε ισχύει η ισότητα

$$\begin{aligned} \#(\cup_{i=1}^n A_i) = &\sum_{1 \leq i_1 \leq n} \#A_{i_1} - \sum_{1 \leq i_1 < i_2 \leq n} \#(A_{i_1} \cap A_{i_2}) \\ &+ \sum_{1 \leq i_1 < i_2 < i_3 \leq n} \#(A_{i_1} \cap A_{i_2} \cap A_{i_3}) - \ldots + (-1)^n \#(\cap_{i=1}^n A_i) . \end{aligned} \tag{15}$$

Η απόδειξη γιά την προβολική περίπτωση είναι εντελώς όμοια.

Το ακόλουθο λήμμα δείχνει πως αρκεί να αποδειχθεί το θεωρημα 5.1 γιά την περίπτωση αφφινικών υπερεπιφανειών.

Λήμμα : 5.1 *Αν το θεώρημα 5.1 ισχύει γιά κάθε αφφινική υπερεπιφάνεια ορισμένη από κάποιο πολυώνυμο $f(X_1, \ldots, X_n)$ στον $\mathbb{A}^n_{\mathbb{F}_q}$, τότε ισχύει και γιά κάθε προβολική υπερεπιφάνεια ορισμένη από κάποιο ομογενές πολυώνυμο $\overline{f}(X_0, \ldots, X_n)$ στον $\mathbb{P}^n_{\mathbb{F}_q}$.*

Απόδειξη. Έστω ότι το θεώρημα του Dwork ισχύει γιά κάθε αφφινική υπερεπιφάνεια, και έστω $\overline{H}_{\overline{f}}$ μία προβολική υπερεπιφάνεια ορισμένη από κάποιο ομογενές πολυώνυμο $\overline{f}(X_0,\ldots,X_n)$ στον $\mathbb{P}^n_{\mathbb{F}_q}$.

Ορίζουμε τα πολυώνυμα $f_n,\ldots,f_0$ ως εξής : $f_n(X_1,\ldots,X_n)=\overline{f}(1,X_1,\ldots,X_n)$ και γιά $i=1,\ldots,n$, $f_{n-i}(X_1,\ldots,X_{n-i})=\overline{f}(\underbrace{0,\ldots,0,1}_{i+1},X_1,\ldots,X_{n-i})$. Ειδικότερα, το f_0 είναι το σταθερό πολυώνυμο.

Παρατηρούμε ότι $\overline{f}([1,x_1,\ldots,x_n])=0\Leftrightarrow f_n(x_1,\ldots,x_n)=0$ και γιά κάθε $i=1,\ldots,n$, $\overline{f}([\underbrace{0,\ldots,0,1}_{i+1},x_1,\ldots,x_{n-i}])=0\Leftrightarrow f_{n-i}(x_1,\ldots,x_{n-i})=0$.

Ορίζουμε ακόμα τα σύνολα $B_n,\ldots,B_0$ ως εξής : $B_n=\{(x_1,\ldots,x_n)\in\mathbb{A}^n_{\mathbb{F}_{q^s}}:\overline{f}(1,x_1,\ldots,x_n)=0\}$ και γιά κάθε $i=1,\ldots,n$ $B_{n-i}=\{(x_1,\ldots,x_{n-i})\in\mathbb{A}^{n-i}_{\mathbb{F}_{q^s}}:\overline{f}(\underbrace{0,\ldots,0,1}_{i+1},x_1,\ldots,x_{n-i})=0\}$. Λόγω της 14 σελ. 47, έχουμε ότι $\overline{N}_s=\#\overline{H}_{\overline{f}}(\mathbb{F}_{q^s})=\#B_n+\#B_{n-1}+\cdots+\#B_1+\#B_0$, άρα

$$\overline{N}_s=\begin{cases}\#H_{f_n}(\mathbb{F}_{q^s})+\#H_{f_{n-1}}(\mathbb{F}_{q^s})+\ldots+\#H_{f_1}(\mathbb{F}_{q^s})+1, & \text{αν } f_0=0\\ \#H_{f_n}(\mathbb{F}_{q^s})+\#H_{f_{n-1}}(\mathbb{F}_{q^s})+\ldots+\#H_{f_1}(\mathbb{F}_{q^s})+0, & \text{αλλιώς}\end{cases}$$

Συνεπώς λοιπόν,

$$Z(\overline{H}_{\overline{f}}/\mathbb{F}_q;T)=\exp(\sum_{s=1}^{\infty}\overline{N}_s\frac{T^s}{s})=$$

$$=\begin{cases}\exp(\sum_{s=1}^{\infty}(\#H_{f_n}(\mathbb{F}_{q^s})+\#H_{f_{n-1}}(\mathbb{F}_{q^s})+\ldots+\#H_{f_1}(\mathbb{F}_{q^s})+1)\frac{T^s}{s}), & \text{αν } f_0=0\\ \exp(\sum_{s=1}^{\infty}(\#H_{f_n}(\mathbb{F}_{q^s})+\#H_{f_{n-1}}(\mathbb{F}_{q^s})+\ldots+\#H_{f_1}(\mathbb{F}_{q^s}))\frac{T^s}{s}), & \text{αλλιώς}\end{cases}$$

$$=\begin{cases}\prod_{i=1}^{n}\exp(\sum_{s=1}^{\infty}(\#H_{f_i}(\mathbb{F}_{q^s})\frac{T^s}{s})\exp(\sum_{s=1}^{\infty}\frac{T^s}{s}), & \text{αν } f_0=0\\ \prod_{i=1}^{n}\exp(\sum_{s=1}^{\infty}(\#H_{f_i}(\mathbb{F}_{q^s})\frac{T^s}{s}), & \text{αλλιώς}\end{cases}$$

$$=\begin{cases}\prod_{i=1}^{n}\exp(\sum_{s=1}^{\infty}(\#H_{f_i}(\mathbb{F}_{q^s})\frac{T^s}{s})\frac{1}{1-T}, & \text{αν } f_0=0\\ \prod_{i=1}^{n}\exp(\sum_{s=1}^{\infty}(\#H_{f_i}(\mathbb{F}_{q^s})\frac{T^s}{s}), & \text{αλλιώς}\end{cases}.$$

Σε κάθε περίπτωση λοιπόν, λόγω της ισχύος του θεωρήματος 5.1 γιά αφφινικές υπερεπιφάνειες, και καθώς γινόμενο κλασμάτων της μορφής που υποδεικνύει το θεώρημα είναι επίσης κλάσμα της ίδιας μορφής, προκύπτει το ζητούμενο.

Λήμμα : 5.2 $Z(H_f/\mathbb{F}_q;T) \in 1 + T\mathbb{Z}[[T]]$.

Απόδειξη. Γιά κάθε $j \in \mathbb{Z}$, έστω $\sigma_j \in \mathrm{Gal}(\overline{\mathbb{F}}_q/\mathbb{F}_q)$ που ορίζεται από την $\sigma_j(x) = x^{q^j}$. Ο αυτομορφισμός σ_j δρα φυσιολογικά στον $\mathbb{A}^n_{\overline{\mathbb{F}}_q}$ ως εξής : Γιά $P = (x_1, \ldots, x_n) \in \mathbb{A}^n_{\overline{\mathbb{F}}_q}$, $P^{\sigma_j} \overset{\text{ορσ}}{=} (\sigma_j(x_1), \ldots, \sigma_j(x_n))$. Ορίζουμε στο $H_f(\overline{\mathbb{F}}_q)$ την εξής σχέση ισοδυναμίας : $P \sim Q \Leftrightarrow Q = P^{\sigma_j}$ γιά κάποιο $j \in \mathbb{Z}$, και συμβολίζουμε με $[P]$ την κλάση ισοδυναμίας του P.
Ισχυρισμός : $\#[P] = \min\{s \in \mathbb{N} \ : \ P \in \mathbb{A}^n(\mathbb{F}_{q^s})\} \overset{\text{ορσ}}{=} s_P$.
Γιά την απόδεξη του ισχυρισμού θα δείξουμε πρώτα ότι τα P^{σ_j}, όπου $j = 0, \ldots, s_P - 1$, είναι διαφορετικά μεταξύ τους, άρα $\#[P] \geq s_P$. Έστω $P = (x_1, \ldots, x_n) \in \mathbb{A}^n(\mathbb{F}_{q^s})$ και $P^{\sigma_i} = P^{\sigma_j}$ γιά κάποια $i, j\{0, \ldots, s_P - 1\}$ με $i \neq j$. Τότε θα έχουμε $\sigma_i(x_k) = \sigma_j(x_k)$ γιά κάθε $k = 1, \ldots, n$. Εφαρμόζοντας τώρα τον σ_{-j} έχουμε $\sigma_{-j}(\sigma_i(x_k) = \sigma_{i-j}(x_k) = x_k$ γιά κάθε $k = 1, \ldots, n$. Η επέκταση $\mathbb{F}_{q^{s_P}}/\mathbb{F}_q$ είναι Galois. Το γεγονός ότι οι συντεταγμένες του P μένουν σταθερές υπό την επίδραση του σ_{i-j}, σημαίνει ότι $\mathbb{F}_q(x_1, \ldots, x_n) \subseteq$ υπόσωμα του $\mathbb{F}_{q^{s_P}}$ που τα στοιχεία του παραμένουν αναλλοίωτα από τον σ_{i-j}. Όμως $\mathbb{F}_q(x_1, \ldots, x_n) =$ (ελάχιστη επέκταση του $\mathbb{F}_q$ που περιέχει τις συντεταγμένες του P) $\overset{\text{ορσ}}{=} \mathbb{F}_{q^{s_P}}$. Άρα όλα τα στοιχεία του $\mathbb{F}_{q^{s_P}}$ μένουν αναλλοίωτα από τον σ_{i-j}. Επειδή όμως η $\mathbb{F}_{q^{s_P}}/\mathbb{F}_q$ είναι Galois, έπεται ότι $\sigma_{i-j} = id$. Άτοπο.

Θα δείξουμε επιπλέον ότι, αν $Q \sim P$, τότε $Q = P^{\sigma_j}$ γιά κάποιο $j \in \{0, 1, \ldots, s_P - 1\}$, άρα $\#[P] \leq s_P$. Έστω λοιπόν $Q \sim P$. Τότε $Q = P^{\sigma_j}$ γιά κάποιο $j \in \mathbb{Z}$. Δηλαδή, αν $Q = (y_1, \ldots, y_n)$ και $P = (x_1, \ldots, x_n)$, τότε $y_i = x_i^{q^j}$ γιά κάθε $i = 1, \ldots, n$. Όμως $P \in \mathbb{A}^n(\mathbb{F}_{q^{s_P}})$ άρα, θέτοντας $j = ks + j_0$ όπου $j_0 \in \{0, 1, \ldots, s_P - 1\}$, έχουμε $y_i = x_i^{q^j} = x_i^{q^{ks+j_0}} = (x_i^{q^{ks}})^{q^{j_0}} = x_i^{q^{j_0}}$ γιά κάθε $i = 1, \ldots, n$, συνεπώς $Q = P^{\sigma_{j_0}}$ γιά κάποιο $j_0 \in \{0, 1, \ldots, s_P - 1\}$.

Επιπλέον έχουμε ότι, αν $Q \sim P$, τότε γιά κάθε $s \geq 1$ ισχύει η ισοδυναμία $Q \in \mathbb{A}^n(\mathbb{F}_{q^s}) \Leftrightarrow P \in \mathbb{A}^n(\mathbb{F}_{q^s})$. Πράγματι, αν $P = (x_1, \ldots, x_n), Q = (y_1, \ldots, y_n)$ και $P \in \mathbb{A}^n(\mathbb{F}_{q^s})$, τότε, καθώς $y_i = x_i^{q^j}$ γιά κάποιο $j \in \mathbb{Z}$, έχουμε $y_i^{q^s} = (x_i^{q^j})^{q^s} = (x_i^{q^s})^{q^j} = x_i^{q^j} = y_i$ γιά κάθε $i = 1, \ldots, n$ άρα $Q \in \mathbb{A}^n(\mathbb{F}_{q^s})$. Το αντίστροφο προκύπτει ομοίως.

Γιά κάθε $P \in H_f(\overline{\mathbb{F}}_q)$ και $s \geq 1$, θέτουμε

$$\epsilon_{P,s} = \begin{cases} 1 & \text{αν } P \in \mathbb{A}^n(\mathbb{F}_{q^s}) \\ 0 & \text{διαφορετικά} \end{cases}$$

Ισχύει ότι $\epsilon_{P,s} = 1 \Leftrightarrow s_P | s$.
Πράγματι, αν $P = (x_1, \ldots, x_n)$, τότε, αφού το $\mathbb{F}_{q^{s_P}}$ είναι η ελάχιστη επέκταση του $\mathbb{F}_q$ που περιέχει τα $x_1, \ldots, x_n$, έπεται ότι $\mathbb{F}_{q^{s_P}} = \mathbb{F}_q(x_1, \ldots, x_n)$. Αν λοιπόν $P \in \mathbb{A}^n(\mathbb{F}_{q^s})$, τότε $\mathbb{F}_{q^s} \supseteq \mathbb{F}_q(x_1, \ldots, x_n) = \mathbb{F}_{q^{s_P}}$, άρα $s_P|s$. Αντίστροφα, αν $s_P|s$, τότε $\mathbb{F}_{q^s} \supseteq \mathbb{F}_{q^{s_P}}$, άρα $P \in \mathbb{A}^n(\mathbb{F}_{q^s})$.

Σύμφωνα λοιπόν με τα παραπάνω έχουμε

$$\begin{aligned}\sum_{s=1}^{\infty} N_s \frac{T^s}{s} &= \sum_{P \in H_f(\overline{\mathbb{F}}_q)} \sum_{s=1}^{\infty} \epsilon_{P,s} \frac{T^s}{s} = \sum_{[P]} \sum_{s=1}^{\infty} \epsilon_{P,s} \#[P] \frac{T^s}{s} \\ &= \sum_{[P]} \sum_{k=1}^{\infty} \frac{s_P}{(k \cdot s_P)} T^{k \cdot s_P} = \sum_{[P]} \sum_{k=1}^{\infty} \frac{(T^{s_P})^k}{k} \\ &= \sum_{[P]} - \log_p(1 - T^{s_P}) \,.\end{aligned}$$

Έχουμε ότι $\mathrm{ord}(\log_p(1 - T^{s_P})) = s_P$ και γιά κάθε $M > 0$, το πολύ πεπερασμένα το πλήθος σημεία P έχουν $s_P \leq M$, άρα $\lim_{P} \mathrm{ord}(\log_p(1 - T^{s_P})) = +\infty$. Η τελευταία σειρά λοιπόν συγκλίνει και καθώς έχει σταθερό όρο μηδέν ορίζεται το εκθετικό της. Από το λήμμα τώρα 3.5, σελ. 29, έχουμε ότι

$$\begin{aligned}&\exp(\sum_{s=1}^{\infty} \frac{N_s}{s} T^s) = \exp(\sum_{[P]} - \log_p(1 - T^{s_P})) = \\ &\prod_{[P]} \frac{1}{1 - T^{s_P}} = \prod_{[P]} (1 + T^{s_P} + T^{2s_P} + \ldots) \in 1 + T\mathbb{Z}[[T]].\end{aligned}$$

Σύμφωνα με το Λήμμα 5.2 και λόγω του ακόλουθου Λήμματος, βλέπει κανείς πως αρκεί να δειχθεί ότι η $Z(H_f/\mathbb{F}_q; T)$ είναι πηλίκο ρητών πολυωνύμων.

Λήμμα : 5.3 *Αν $h(T) \in 1+T\mathbb{Z}[[T]]$ και $h(T) = \frac{f(T)}{g(T)}$ γιά κάποια $f(T), g(T) \in \mathbb{Q}[T]$, τότε $h(T) = \frac{f'(T)}{g'(T)}$ γιά κάποια $f'(T), g'(T) \in 1+T\mathbb{Z}[T]$ πρώτα μεταξύ τους.*

Απόδειξη : Έχουμε ότι $h(T) = \frac{f'(T)}{g'(T)}$ γιά κάποια $f'(T)$, $g'(T) \in \mathbb{Q}[T]$ πρώτα μεταξύ τους πάνω από το $\mathbb{Q}[T]$, αφού κάθε κοινός τους παράγοντας των $f(T)$, $g(T)$ στο $\mathbb{Q}[T]$ μπορεί να απλοποιηθεί. Επιπλέον μπορούμε να υποθέσουμε ότι τα $f'(T)$ και $g'(T)$ έχουν σταθερό όρο μονάδα, καθώς, λόγω του ότι η $h(T)$ έχει σταθερό όρο μονάδα, έπεται ότι τα $f'(T)$, $g'(T)$ έχουν κοινό σταθερό όρο. Έχουμε ότι

$$f'(T) f_1(T) + g'(T) g_1(T) = 1 \tag{16}$$

γιά κάποια $f_1(T)$, $g_1(T) \in \mathbb{Q}[T]$. Έστω τώρα $g^{'}(T) = 1 + b_1 T + \ldots + b_m T^m = \prod_{i=1}^{m}(1 - \frac{1}{\beta_i}T)$, όπου $b_i \in \mathbb{Q}$ γιά $1 \leq b_i \leq m$ και έστω p πρώτος. Αν $|\frac{1}{\beta_i}|_p > 1$ γιά κάποιο $i \in \{1, \ldots, m\}$, τότε $|\beta_i|_p < 1$, άρα $f^{'}(\beta_i) =$ [45]$g^{'}(\beta_i)h(\beta_i) = 0$. Βλέποντας την 16 στο Ω_p ως προς τον πρώτο p, και θέτοντας $T = \beta_i$ έχουμε $0 = 1$. Άτοπο. Άρα $|\frac{1}{\beta_i}|_p < 1$ γιά κάθε $i = 1, \ldots, m$, συνεπώς $|b_i|_p < 1$ γιά κάθε $i = 1, \ldots, m$. Αφού τα b_i είναι ρητοί, θα έχουμε $b_i \in \mathbb{Z}$ γιά κάθε $i = 1, \ldots, m$. Καθώς τώρα $h(T) \in 1 + \mathbb{Z}[[T]]$, $g^{'}(T) \in 1 + \mathbb{Z}[T]$ και $h(T)g^{'}(T) = f^{'}(T)$ έπεται και ότι $f^{'}(T) \in 1 + \mathbb{Z}[T]$. $\square$

Λήμμα : 5.4 *Ο συντελεστής του T^j στην $Z(H_f/\mathbb{F}_q;T)$ είναι $\leq q^{nj}$.*

Απόδειξη. Η μεγαλύτερη τιμή του N_s, είναι $q^{ns} = \#\mathbb{A}^n_{q^s}$, άρα οι συντελεστές της $Z(H_f/\mathbb{F}_q;T)$ είναι μικρότεροι ή ίσοι από q^{ns}. Όμως $\exp(\sum_{s=1}^{\infty} q^{ns}\frac{T^s}{s}) = \exp(-\log(1 - q^n T)) = \frac{1}{1 - q^n T} = \sum_{j=0}^{\infty} q^{nj}T^j$.

[45] Κάθε δυναμοσειρά στο $\Omega_p[[T]]$ συγκλίνει στον $D(1)$.

6 Αντιπρόσωποι Teichmuller και η δυναμοσειρά Θ(Τ).

Γιά την αναλυτικότερη παρουσίαση όσων εκτίθενται σ' αυτήν την ενότητα παραπέμπουμε στο βιβλίο του Koblitz [Ko]. Αρχικά παραθέτουμε κάποιους προκαταρκτικούς ορισμούς.

Έστω K επέκταση του $\mathbb{Q}_p$ με $[K/\mathbb{Q}_p] = n$. Αν $a \in K$, ορίζουμε $\mathrm{ord}_p a \overset{o\rho\sigma}{=} -\log_p |a|_p = -\log_p |\mathrm{N}_{K/\mathbb{Q}_p}(a)|_p^{\frac{1}{n}} = -\frac{1}{n}\log_p |\mathrm{N}_{K\mathbb{Q}_p}(a)|_p$, όπου $\log_p : \mathbb{R}^+ \to \mathbb{R}$ είναι ο συνηθισμένος λογάριθμος με βάση το p. Στο σημείο αυτό παρατηρούμε ότι αν $a, b \in K$, τότε

$$\mathrm{ord}_p(ab) = -\frac{1}{n}\log_p |\mathrm{N}_{K/\mathbb{Q}_p}(ab)|_p = -\frac{1}{n}\log_p |\mathrm{N}_{K/\mathbb{Q}_p}(a)\mathrm{N}_{K/\mathbb{Q}_p}(b)|_p =$$

$$-\frac{1}{n}\log_p |\mathrm{N}_{K/\mathbb{Q}_p}(a)|_p|\mathrm{N}_{K/\mathbb{Q}_p}(b)|_p = -\frac{1}{n}\log_p |\mathrm{N}_{K/\mathbb{Q}_p}(a)|_p - \frac{1}{n}\log_p |\mathrm{N}_{K/\mathbb{Q}_p}(b)|_p = \mathrm{ord}_p a + \mathrm{ord}_p b.$$

Λόγω της παραπάνω ιδιότητας και καθώς $\mathrm{N}_{K/\mathbb{Q}_p}(a) \in \mathbb{Q}_p$ γιά κάθε $a \in K$, αν συμβολίσουμε με $\mathrm{ord}_p(K)$ την εικόνα του K μέσω της απεικόνισης ord_p, θα έχουμε ότι η $\mathrm{ord}_p(K)$ είναι μία προσθετική υποομάδα της $\frac{1}{n}\mathbb{Z}$ της μορφής $\frac{1}{e}\mathbb{Z}$ γιά κάποιον φυσικό e με $e|n$.[46] Τον φυσικό αυτό e τον ονομάζουμε δείκτη διακλάδωσης του K πάνω από το $\mathbb{Q}_p$. Αν $e = 1$, τότε λέμε ότι το K είναι αδιακλάδωτη επέκταση του $\mathbb{Q}_p$, ενώ αντίθετα, αν $e = n$, τότε λέμε ότι το K είναι ολικά διακλαδωμένη επέκταση του $\mathbb{Q}_p$. Γενικότερα, αν $A = \{x \in K \ : \ |x|_p \leq 1\}$ είναι ο δακτύλιος της p-αδικής εκτίμησης και $M = \{x \in K \ : \ |x|_p < 1\}$ είναι το μοναδικό maximal ιδεώδες του A, ισχύει ότι το $\mathbb{F}_p$ είναι υπόσωμα του A/M και ότι $n = [K/\mathbb{Q}_p] = [(A/M)/\mathbb{F}_p] \cdot e$.[47]

Μία χρήσιμη παρατήρηση είναι ότι, αν $\pi \in K$ είναι ένα στοιχείο με $\mathrm{ord}_p\pi = \frac{1}{e}$, τότε κάθε $x \in K$ μπορεί να γραφεί στη μορφή $\pi^m u$ όπου $u \in K$ με $|u|_p = 1$ και $m = e \cdot \mathrm{ord}_p x \in \mathbb{Z}$.
Αυτό διότι : αν $\mathrm{ord}_p x = \frac{m}{e} = m \cdot \mathrm{ord}_p\pi = \mathrm{ord}_p\pi^m$, τότε $\mathrm{ord}_p\frac{x}{\pi^m} = 0$, ή $|\frac{x}{\pi^m}|_p = 1$, και θέτοντας $u \overset{o\rho\sigma}{=} \frac{x}{\pi^m}$ έχουμε $x = \pi^m u$ με $|u|_p = 1$, καθώς επίσης και $m = e \cdot \mathrm{ord}_p x \in \mathbb{Z}$, αφού $\mathrm{ord}_p x \in \frac{1}{e}\mathbb{Z}$.
Συμφωνα λοιπόν με τα παραπάνω, στην περίπτωση αδιακλάδωτης επέκτασης, μπορούμε να θεωρούμε ως π τον p.

[46] Οι προσθετικές υποομάδες της $\frac{1}{n}\mathbb{Z}$ είναι προφανώς της μορφής $\frac{a}{n}\mathbb{Z}$, όπου $a \in \mathbb{Z}$. Όμως γιά κάθε επέκταση K του $\mathbb{Q}_p$ όπως παραπάνω, $1 = \mathrm{ord}_p p \in \mathrm{ord}_p(K)$, καθώς $1 \in K$, άρα $\frac{a}{n}e = 1$ γιά κάποιον $e \in \mathbb{Z}$,(ειδικότερα $e \in \mathbb{N}$), ή $ae = n$. Συνεπώς η $\mathrm{ord}_p(K)$ είναι μία υποομάδα της μορφής $\frac{1}{e}\mathbb{Z}$ γιά κάποιον $e \in \mathbb{N}$.

[47] Βλ. [Gou], πρόταση 5.4.6. σελ.146 .

Έστω $q = p^s$. Αποδεικνύονται τα εξής. Υπάρχει μία μοναδική αδιακλάδωτη επέκταση του $\mathbb{Q}_p$ βαθμού s, την οποία εδώ θα συμβολίζουμε $K_q^{\alpha\delta}$. Ισχύει ότι $K_q^{\alpha\delta} = \mathbb{Q}_p(\gamma)$ γιά οποιαδήποτε αρχική $(q-1)$- ρίζα της μονάδος γ.[48] Έστω A ο δακτύλιος της p-αδικής εκτίμησης

$$A \overset{\text{ορσ}}{=} \{x \in K_q^{\alpha\delta} \ : \ |x|_p \leq 1\} = \{x \in K_q^{\alpha\delta} \ : \ \mathrm{ord}_p x \geq 0\}$$

και M το μοναδικό maximal ιδεώδες του A,

$$M \overset{\text{ορσ}}{=} \{x \in A \ : \ |x|_p < 1\} = \{x \in A \ : \ \mathrm{ord}_p x > 0\}.$$

Καθώς ισχύει ότι $M = \pi A$ [49] και λόγω του ότι η $K_q^{\alpha\delta}$ είναι αδιακλάδωτη, έχουμε ότι $M = pA$.

Κάθε $x \in K_q^{\alpha\delta}$ γράφεται στη μορφή $x = \displaystyle\sum_{i=m}^{\infty} a_i p^i$, όπου $m = \mathrm{ord}_p x$ και κάθε $a_i \in A$ είναι είτε 0 είτε $(q-1)$-ρίζα της μονάδας.[50]

Ειδικότερα, αν $x \in A$, καθώς $\mathrm{ord}_p x \geq 0$, έχουμε $x = \displaystyle\sum_{i=0}^{\infty} a_i p^i$, συνεπώς $x + M = a_0 + M$, όπου $a_0 = 0$ είτε $a_0 = \gamma^k$ γιά κάποιο $k \in \{0, 1, \ldots, q-2\}$.

Επειδή έχουμε $s = [K_q^{\alpha\delta}/\mathbb{Q}_p] = [(A/M)/\mathbb{F}_p] \cdot e$ και $e = 1$, έπεται ότι το A/M είναι ισόμορφο με το $\mathbb{F}_q$. Σύμφωνα λοιπόν με τα παραπάνω, τα στοιχεία του $\mathbb{F}_q$ τα βλέπουμε ως $a + M$, όπου $a = 0$, είτε $a = \gamma^k$ γιά κάποιο $k \in \{0, 1, \ldots, q-2\}$, δηλαδή το τυπικό μη μηδενικό στοιχείο $u \in \mathbb{F}_q$ ταυτίζεται με κάποιο $t + M$, όπου το $t \in A$ είναι κάποια $(q-1)$-τάξεως ρίζα της μονάδας. Αυτό το t καλείται *αντιπρόσωπος* Teichmuller του u. Προφανώς και κάθε $a + M$ με $a \in A$ ταυτίζεται με κάποιο στοιχείο $u \in \mathbb{F}_q$, ακόμα και αν το a δεν είναι $(q-1)$- ρίζα της μονάδας, τότε όμως το a δεν είναι αντιπρόσωπος Teichmuller του u. Καθώς ισχύει η ισομορφική εμφύτευση $\mathbb{F}_p \hookrightarrow A/M$ που ορίζεται από την $z + p\mathbb{Z} \mapsto z + M$ με $z \in \mathbb{Z}$, έπεται ότι μπορεί κανείς να ταυτίσει τα στοιχεία του $\mathbb{F}_p$ με τα $z + M$ όπου $z \in \mathbb{Z}$. Αν θέλουμε να βλέπουμε τα στοιχεία του $\mathbb{F}_p$ ως στοιχεία του $\mathbb{F}_q$, τότε τα ταυτίζουμε με τα

$$0 + M, 1 + M, \zeta + M, \zeta^2 + M, \ldots, \zeta^{p-2} + M \text{ όπου } \zeta = \gamma^{\frac{q-1}{p-1}}.$$

---

[48] Βλ. πρόταση σελ. 67 του [Ko]

[49] $(\supseteq)$ Έστω $a \in A$. Τότε $|\pi a|_p \leq |\pi|_p = \frac{1}{p^{\frac{1}{e}}} < 1$.

$(\subseteq)$ Έστω $\mu \in M$. Τότε $\mu = \pi^{e \cdot \mathrm{ord}_p \mu} u = \pi(\pi^{e \cdot \mathrm{ord}_p \mu - 1} u)$, όπου $|\pi^{e \cdot \mathrm{ord}_p \mu - 1} u|_p = |\pi^{e \cdot \mathrm{ord}_p \mu - 1}|_p = \frac{1}{p^{\frac{e \cdot \mathrm{ord}_p \mu - 1}{e}}} \leq 1$ καθώς $\mathrm{ord}_p \mu > 0$, άρα $e \cdot \mathrm{ord}_p \mu > 0$ και αφού $e \cdot \mathrm{ord}_p \mu > 0 \in \mathbb{Z}$, $e \cdot \mathrm{ord}_p \mu \geq 1$.

[50] Βλ. [Ko], πόρισμα σελ. 68 .

Στα παρακάτω θα χρησιμοποιούμε τον εξής συμβολισμό : Γιά κάθε $g(X) = a_0 + a_1X + \ldots + a_mX^m \in A[X]$, όταν γράφουμε $\overline{g}(X)$, εννοούμε το πολυώνυμο $(a_0 + M) + (a_1 + M)X + \ldots + (a_m + M)X^m \in \mathbb{F}_q[X]$. Αντίστροφα, λόγω των παραπάνω, κάθε πολυώνυμο πάνω από το $\mathbb{F}_q$ είναι της μορφής $\overline{g}(X)$ γιά κάποιο $g(X) \in A[X]$.

Αφού τα μη μηδενικά στοιχεία του $\mathbb{F}_q$ ταυτίζονται ισομορφικά με τα $\gamma^k + M$ με $k = 0, 1, \ldots, q-2$, έπεται ότι αν $0 \leq i, j \leq q-2$ και $\gamma^i + M = \gamma^j + M$, τότε $i = j$. Από αυτό έπεται πολύ εύκολα ότι ο $u \overset{o\rho\sigma}{=} \gamma + M$ είναι ο γεννήτορας της πολλαπλασιαστικής ομάδας $\mathbb{F}_q^\times$, και ότι $\mathbb{F}_q = \mathbb{F}_p(u)$. Κάθε στοιχείο λοιπόν του $\mathbb{F}_q^\times$ είναι της μορφής u^k γιά κάποιο $k \in \{0, \ldots, q-2\}$. Θεωρούμε ένα τέτοιο u^k και θα υπολογίσουμε το $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(u^k)$.

Έστω $\overline{g}_0(u^k) = 0$ γιά κάποιο μονικό ανάγωγο $\overline{g}_0 \in \mathbb{F}_p[X]$ βαθμού d όπου $d|s$ και $g_0 \in \mathbb{Z}_p[X]$. Θέτουμε $\Phi(X) = X^{q-1} - 1 \in \mathbb{Z}[X] \subseteq \mathbb{Z}_p[X]$. Τότε έχουμε $\overline{g}_0|\overline{\Phi}$ και έστω $\overline{\Phi} = \overline{g}_0\overline{h}_0$ γιά κάποιο $h_0 \in \mathbb{Z}_p[X]$. Επειδή το $\overline{\Phi}$ δεν έχει πολλαπλές ρίζες, τα $\overline{g}_0,\overline{h}_0$ είναι πρώτα μεταξύ τους. Από το λήμμα του Hensel,[51] έχουμε ότι υπάρχουν $g, h \in \mathbb{Z}_p[X]$, με το g μονικό βαθμού d, τ.ώ. $\Phi = gh$, $\overline{g} = \overline{g}_0$ και $\overline{h} = \overline{h}_0$. Καθώς το $\overline{g}_0$ είναι ανάγωγο πάνω από το $\mathbb{F}_p$, έπεται ότι το ίδιο ισχύει και γιά το $\overline{g}$, άρα και το g θα είναι ανάγωγο πάνω από το $\mathbb{Z}_p[X]$. Ακόμα, καθώς $\overline{g} = \overline{g}_0$, έπεται ότι $g = g_0 + pg_1$ γιά κάποιο $g_1 \in \mathbb{Z}_p[X]$.

Αναζητούμε τις ρίζες του $g(X)$. Η τυπική του ρίζα, αφού είναι ρίζα του Φ, θα είναι της μορφής γ^i όπου το i παίρνει d διαφορετικές τιμές στο σύνολο $\{0, \ldots, q-2\}$. Θα δείξουμε οι τιμές αυτές είναι ακριβώς οι $k, kp, \ldots, kp^{d-1}$. Αν $g(\gamma^i) = 0$, τότε θα έχουμε :

$$0 = g(\gamma^i) = g_0(\gamma^i) + pg_1(\gamma^i), \text{ άρα } 0 + M = \overline{g}_0(\gamma^i + M) = \overline{g}_0(u^i),$$

δηλαδή η u^i θα είναι ρίζα του $\overline{g}_0 \in \mathbb{F}_p[X]$. Όμως η επέκταση $\mathbb{F}_p(u^k)/\mathbb{F}_p$ είναι Galois και ομάδα Galois της $\mathbb{F}_p(u^k)/\mathbb{F}_p$ είναι κυκλική τάξεως d και παράγεται από τον $\mathbb{F}_p$-αυτομορφισμό σ όπου $\sigma(x)x^p$ γιά κάθε $x \in \mathbb{F}_p(u^k)$. Αφού λοιπόν μία ρίζα του $\overline{g}_0$ είναι η u^k, οι ρίζες του $\overline{g}_0$ θα είναι ακριβώς οι $u^k, \sigma(u^k), \ldots, \sigma^{d-1}(u^k)$, δηλαδή οι $u^k, u^{kp}, \ldots, u^{kp^{(d-1)}}$. Όσον αφορά λοιπόν τις ρίζες του g έχουμε ότι θα είναι της μορφής γ^i γιά κάποια $i \in \{k, kp, \ldots, kp^{d-1}\}$. Όμως το i παίρνει d διαφορετικές τιμές, άρα οι ρίζες του είναι ακριβώς οι $\gamma^k, \gamma^{kp}, \ldots, \gamma^{kp^{d-1}}$. Θα

[51] Λήμμα του Hensel : Έστω $f(X)$ πρωταχικό πολυώνυμο με συντελεστές στο δακτύλιο S των ακεραίων στοιχείων ενός σώματος k πλήρες ως προς μία εκτίμηση. Αν στο σώμα κλάσεων υπολοίπων Σ το πολυώνυμο $\overline{f} \in \Sigma[X]$ έχει παραγοντοποίηση $\overline{f} = \overline{g}_0\overline{h}_0$ $(g_0, h_0 \in A[X])$ με τα $\overline{g}_0, \overline{h}_0$ πρώτα μεταξύ τους, τότε υπάρχουν πολυώνυμα $g, h \in A[X]$, τ.ώ. $f = gh$ με $\overline{g} = \overline{g}_0$, $\overline{h} = \overline{h}_0$ και $deg(g) = deg(\overline{g}_0)$. Στην περίπτωσή μας $f(X) = \Phi(X)$, $A = \mathbb{Z}_p$, $k = \mathbb{Q}_p$. Βλ και [BS], θεώρημα 2 σελ. 275.

έχουμε λοιπόν ότι $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(u^k) = \frac{s}{d}\sum_{j=0}^{d-1} u^{kp^j}$ και $\mathrm{Tr}_{K_q^{\alpha\delta}/\mathbb{Q}_p}(\gamma^k) = \frac{s}{d}\sum_{j=0}^{d-1} \gamma^{kp^j}$.[52] Όμως αφού θέσαμε $u = \gamma + M$, δηλαδή ο αντιπρόσωπος Teichmuller του u είναι ο γ, θα έχουμε και $u^k = (\gamma + M)^k = \gamma^k + M$,αρα ο αντιπρόσωπος Teichmuller του τυπικού στοιχείου $u^k \in \mathbb{F}_q$ θα είναι ο $t \overset{o\rho\sigma}{=} \gamma^k$. Από τα παραπάνω λοιπόν έχουμε τα εξής :

> Αν $x \in \mathbb{F}_q$, τότε γιά τον αντιπρόσωπο Teichmuller t του x ισχύει ότι $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x) = \mathrm{Tr}_{K_q^{\alpha\delta}/\mathbb{Q}_p}(t) + M = \mathrm{Tr}_{K_q^{\alpha\delta}/\mathbb{Q}_p}(t) + pA$.

Η επέκταση $K_q^{\alpha\delta}/\mathbb{Q}_p$ είναι Galois και η ομάδα Galois αυτής της επέκτασης παράγεται από τον $\mathbb{Q}_p-$ισομορφισμό $K_q^{\alpha\delta} \ni x \mapsto x^p$ τάξεως s. Αρα

$$\mathrm{Tr}_{K_q^{\alpha\delta}/\mathbb{Q}_p}(t) = t + t^p + \ldots + t^{p^{s-1}}$$

Έστω ϵ μία p-οστή ρίζα της μονάδας στο Ω_p. Επειδή ο t είναι αλγεβρικός ακέραιος πάνω από τον δακτύλιο $\mathbb{Z}_p$, έπεται ότι $\mathrm{Tr}_{K_q^{\alpha\delta}/\mathbb{Q}_p}(t) \in \mathbb{Z}_p$. Γενικά τώρα, πρέπει να δείξει κανείς ότι γιά $a \in \mathbb{Z}_p$ ορίζεται το ϵ^a και ότι $\epsilon^{pa} = 1$.
Πράγματι, έστω $\epsilon = 1 + \lambda$. Είναι $\mathrm{ord}_p\lambda = \frac{1}{p-1}$.[53] Επειδή $a \in \mathbb{Z}_p$, από την ενότητα 2.3, έχουμε ότι η σειρά $B_{a,p}(x)$ συγκλίνει όταν $|x|_p < 1$, άρα έχει νόημα το $B_{a,p}(\lambda) \in \Omega_p$ και ορίζουμε $\epsilon^a = B_{a,p}(\lambda)$. Ομοίως, γιά $a \in \mathbb{Z}_p$, ϵ^{pa} ορίζεται να είναι το $B_{ap,p}(\lambda)$. Θα δείξουμε ότι $\epsilon^{pa} = 1$. Πράγματι, από την ταυτότητα $(1 + X_1)^{pX_2} = [(1 + X_1)^p]^{X_2}$ έχουμε

$$\epsilon^{pa} = (1+\lambda)^{pa} = [(1+\lambda)^p]^a = [1 + (p\lambda + \tbinom{p}{2}\lambda^2 + \ldots + \lambda^p)]^a =$$

$$1 + \sum_{n=1}^{\infty} \frac{a(a-1)\cdot \ldots \cdot (a-n+1)}{n!}(p\lambda + \binom{p}{2}\lambda^2 + \ldots + \lambda^p)^n.$$

Όμως

$$(p\lambda + \tbinom{p}{2}\lambda^2 + \ldots + \lambda^p) = (-1 + (1+\lambda)^p)^n = (-1 + \epsilon^p)^n = 0^n = 0,$$

άρα

---

[52]Είναι γνωστό από τη θεωρία Galois ότι αν L/K πεπερασμένη επέκταση σωμάτων με $[L : K] = s$ $x \in L$ και $g = Irr(x, K)$ με $degg = d$, τότε $\mathrm{Tr}_{L/K}(x) = \frac{s}{d}\cdot$άθροισμα των ριζών του g.

[53]Έστω p πρώτος διάφορος του 2. Έχουμε ότι $f(X) \overset{o\rho\sigma}{=} Irr(\epsilon, \mathbb{Q}_p) = X^{p-1} + X^{p-2} + \ldots + 1 = \frac{X^p - 1}{X - 1}$, καθώς $f(\epsilon) = 0$ και το $f(X)$ είναι ανάγωγο. Άρα λοιπόν $[\mathbb{Q}_p(\epsilon) : \mathbb{Q}_p] = p - 1$, συνεπώς $|\epsilon|_p = |\mathrm{N}_{\mathbb{Q}_p(\epsilon)/\mathbb{Q}_p}\epsilon|_p^{\frac{1}{p-1}} = |(-1)^{p-1}\cdot 1|_p^{\frac{1}{p-1}} = 1$. Ακόμα $\mathbb{Q}_p(\epsilon - 1) = \mathbb{Q}_p(\epsilon)$, άρα $[\mathbb{Q}_p(\epsilon - 1) : \mathbb{Q}_p] = p - 1$ και επειδή το $f(X + 1)$ είναι ανάγωγο, $f((\epsilon - 1) + 1) = 0$ και $f(0 + 1) = p$, έχουμε ότι $|\epsilon - 1|_p = |(-1)^{p-1}p|_p^{\frac{1}{p-1}} = \frac{1}{p^{\frac{1}{p-1}}}$, δηλαδή $\mathrm{ord}_p(\epsilon - 1) = \frac{1}{p-1}$.

$$\sum_{n=1}^{\infty} \frac{a(a-1)\cdot \ldots \cdot (a-n+1)}{n!}(p\lambda + \binom{p}{2}\lambda^2 + \ldots + \lambda^p)^n = 0,$$

και συνεπώς $\epsilon^{pa} = 1$.

Έστω $x \in \mathbb{F}_q$. Θέτοντας T_x τον ελάχιστο φυσικό από τους αντιπροσώπους της κλάσης $\pmod p$ του $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x) \in \mathbb{F}_p$, μπορούμε να ορίσουμε το $\epsilon^{T_x} \in \Omega_p$ το οποίο από εδώ και στο εξής θα γράφουμε $\epsilon^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)}$ γιά να αποφύγουμε τη χρήση πολλών συμβόλων. Καθώς το στοιχείο $\epsilon^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)}$ εξαρτάται μόνο από την κλάση $\pmod p$ του εκθέτη, και αφού δείξαμε ότι ισχύει $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x) = \mathrm{Tr}_{K_q^{\alpha\delta}/\mathbb{Q}_p}(t) + pA$ έχουμε ότι $\epsilon^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)} = \epsilon^{\mathrm{Tr}_{K/\mathbb{Q}_p}(t)}$.

Στα παρακάτω αναζητούμε μία δυναμοσειρά, την οποία όταν θα καθορίσουμε θα συμβολίζουμε με $\Theta(T)$, η οποία θα έχει την ιδιότητα

$$\Theta(t)\Theta(t^p)\Theta(t^{p^2})\cdot \ldots \cdot \Theta(t^{p^{s-1}}) = \epsilon^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p} x}.$$

Έστω $\lambda = \epsilon - 1$. Θεωρούμε τη δυναμοσειρά

$$F(X,Y) =$$

$$(1+Y)^X (1+Y^p)^{\frac{X^p - X}{p}} (1+Y^{p^2})^{\frac{X^{p^2}-X^p}{p^2}} \cdot \ldots \cdot (1+Y^{p^n})^{\frac{X^{p^n}-X^{p^{n-1}}}{p^n}} \cdot \ldots =$$

$$(1 + \sum_{i=1}^{\infty} \frac{X(X-1)\cdot \ldots \cdot (X-i+1)}{i!} Y^i)\cdot$$
$$\prod_{n=1}^{\infty} (1 + \sum_{i=1}^{\infty} \frac{X^{p^n} - X^{p^{n-1}}}{p^n} (\frac{X^{p^n} - X^{p^{n-1}}}{p^n} - 1)\cdot$$
$$\ldots \cdot (\frac{X^{p^n} - X^{p^{n-1}}}{p^n} - i + 1)\frac{Y^{ip^n}}{i!}).$$

, που ορίστηκε στην σελίδα 31, στη μορφή $F(X,Y) = \sum_{n=0}^{\infty} (X^n \sum_{m=n}^{\infty} a_{m,n} Y^m)$ με $a_{m,n} \in \mathbb{Z}_p$.[54]

Έστω n σταθερό. Καθώς γιά κάθε m $a_{m,n} \in \mathbb{Z}_p$ και $\mathrm{ord}_p \lambda = \frac{1}{p-1}$, έχουμε

[54] Γιά κάθε $n = 0, 1, \ldots$, έχουμε $a_{m,n} = 0$ γιά $m < n$ και αυτό διότι γιά κάθε n, κάθε προσθεταίος της σειράς

$\mathrm{ord}_p a_{m,n}\lambda^m \geq 0+\frac{m}{p-1} \overset{m\to\infty}{\longrightarrow} \infty$, έπεται ότι η σειρά $\sum_{m=n}^{\infty} a_{m,n}\lambda^m$ συγκλίνει. Επειδή τώρα γιά κάθε m,n, $a_{m,n}\lambda^m \in \mathbb{Q}_p(\lambda)=\mathbb{Q}_p(\epsilon)$ και το $\mathbb{Q}_p(\epsilon)$ είναι πλήρες,[55] έχουμε ότι γιά κάθε n, $\alpha_n \overset{\text{ορσ}}{=} \sum_{m=n}^{\infty} a_{m,n}\lambda^m \in \mathbb{Q}_p(\epsilon)$.

Θέτουμε

$$\Theta(T) \overset{\text{ορσ}}{=} F(T,\lambda) = \sum_{n=0}^{\infty} \alpha_n T^n \in \mathbb{Q}_p(\epsilon).$$

Η δυναμοσειρά $\Theta(T)$ συγκλίνει τουλάχιστον στο δίσκο $D(1)$ διότι :
γιά κάθε $x \in D(1)$ έχουμε

$$\mathrm{ord}_p\alpha_n x^n \geq \mathrm{ord}_p\alpha_n 1^n = \mathrm{ord}_p(\sum_{m=n}^{\infty} a_{m,n}\lambda^m) = \mathrm{ord}_p(\lambda^n \sum_{m=0}^{\infty} a_{m+n,n}\lambda^m) =$$

$$n\mathrm{ord}_p\lambda + \mathrm{ord}_p(\sum_{m=0}^{\infty} a_{m+n,n}\lambda^m) \geq \tfrac{n}{p-1} + c_n{}^{56} \geq \tfrac{n}{p-1} \overset{n\to\infty}{\longrightarrow} \infty.$$

Γιά τον αντιπρόσωπο Teichmuller t του x, θεωρούμε τη σειρά

$$(1+Y)^{t+t^p+t^{p^2}+\ldots+t^{p^{s-1}}} = B_{t+t^p+t^{p^2}+\ldots+t^{p^{s-1}},p}(Y).$$

Θα δείξουμε ότι ισχύει η ακόλουθη σχέση στο $\Omega_p[[Y]]$:

$$(1+Y)^{t+t^p+t^{p^2}+\ldots+t^{p^{s-1}}} = F(t,Y)F(t^p,Y)F(t^{p^2},Y)\cdot\ldots\cdot F(t^{p^{s-1}},Y).$$

Έχουμε :

$$F(t,Y)F(t^p,Y)F(t^{p^2},Y)\cdot\ldots\cdot F(t^{p^{s-1}},Y) =$$

$$(1+Y)^t(1+Y^p)^{\frac{t^p-t}{p}}(1+Y^{p^2})^{\frac{t^{p^2}-t^p}{p^2}}\cdot\ldots\cdot(1+Y^{p^n})^{\frac{t^{p^n}-t^{p^{n-1}}}{p^n}}\cdot\ldots\cdot$$

$$\prod_{n=1}^{\infty}(1+\sum_{i=1}^{\infty}\frac{X^{p^n}-X^{p^{n-1}}}{p^n}(\frac{X^{p^n}-X^{p^{n-1}}}{p^n}-1)\cdot\ldots\cdot(\frac{X^{p^n}-X^{p^{n-1}}}{p^n}-i+1)\frac{Y^{ip^n}}{i!}),$$

ομοίως και της $(1+\sum_{i=1}^{\infty}\frac{X(X-1)\cdot\ldots\cdot(X-i+1)}{i!}Y^i)$, έχει το X υψωμένο σε δύναμη μικρότερη η ίση από ip^n, δύναμη στην οποία είναι υψωμένο το αντίστοιχο Y.

[55]Κάθε πεπερασμένη επέκταση K του $\mathbb{Q}_p$ είναι πλήρης ως προς τη μοναδική επέκταση στο K της $|\cdot|_p$. Βλ. [Ca] σελ.115

[56]c_n σταθερά μεγαλύτερη ή ίση του μηδενός, εξαρτόμενη από το n

$$(1+Y)^{t^p}(1+Y^p)^{\frac{t^{p^2}-t^p}{p}}(1+Y^{p^2})^{\frac{t^{p^3}-t^{p^2}}{p^2}}\cdot\ldots\cdot(1+Y^{p^n})^{\frac{t^{p^{n+1}}-t^{p^n}}{p^n}}\cdot\ldots\cdot$$

$$\vdots$$

$$(1+Y)^{t^{p^{s-1}}}(1+Y^p)^{\frac{t^{p^s}-t^{p^{s-1}}}{p}}(1+Y^{p^2})^{\frac{t^{p^{s+1}}-t^{p^s}}{p^2}}\cdot\ldots\cdot(1+Y^{p^n})^{\frac{t^{p^{s+n-1}}-t^{p^{s+n-2}}}{p^n}}\cdot\ldots=$$

$$={}^{57}((1+Y)^t(1+Y)^{t^p}\cdot\ldots\cdot(1+Y)^{t^{p^{s-1}}})\cdot$$

$$((1+Y^p)^{\frac{t^p-t}{p}}((1+Y^p)^{\frac{t^{p^2}-t^p}{p}}\cdot\ldots\cdot(1+Y^p)^{\frac{t^{p^s}-t^{p^{s-1}}}{p}})\cdot$$

$$((1+Y^{p^2})^{\frac{t^{p^2}-t^p}{p^2}}(1+Y^{p^2})^{\frac{t^{p^3}-t^{p^2}}{p^2}}\cdot\ldots\cdot(1+Y^{p^2})^{\frac{t^{p^{s+1}}-t^{p^s}}{p^2}})\cdot\ldots\cdot$$

$$((1+Y^{p^n})^{\frac{t^{p^n}-t^{p^{n-1}}}{p^n}}(1+Y^{p^n})^{\frac{t^{p^{n+1}}-t^{p^n}}{p^n}}(1+Y^{p^n})^{\frac{t^{p^{s+n-1}}-t^{p^{s+n-2}}}{p^n}})\cdot\ldots=$$

$${}^{58}(1+Y)^{t+t^p+t^{p^2}+\ldots+t^{p^{s-1}}}(1+Y^p)^{\frac{t^{p^s}-t}{p}}(1+Y^{p^2})^{\frac{t^{p^{s+1}}-t^p}{p^2}}(1+Y^{p^3})^{\frac{t^{p^{s+2}}-t^{p^2}}{p^3}}\cdot$$
$$\ldots(1+Y^{p^n})^{\frac{t^{p^{s+n-1}}-t^{p^{n-1}}}{p^n}}\cdot\ldots={}^{59}(1+Y)^{t+t^p+t^{p^2}+\ldots+t^{p^{s-1}}}.$$

Αφού ξέρουμε ότι η δυναμοσειρά $\Theta(T)$ συγκλίνει στα $x\in\Omega_p$ με $|x|_p=1$, αντικαθιστώντας τις τιμές $t, t^p, t^{p^2}, \ldots, t^{p^{s-1}}$ και πολλαπλασιάζοντας, έχουμε ότι

$$\Theta(t)\Theta(t^p)\Theta(t^{p^2})\cdot\ldots\cdot\Theta(t^{p^{s-1}})=F(t,\lambda)F(t^p,\lambda)F(t^{p^2},\lambda)\cdot\ldots\cdot F(t^{p^{s-1}},\lambda)=$$

$$(1+\lambda)^{t+t^p+t^{p^2}+\ldots+t^{p^{s-1}}}=\epsilon^{\mathrm{Tr}_{K/\mathbb{Q}_p}(t)}=\epsilon^{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x)}.$$

[57]Από το Λήμμα 1.5.
[58]Βλ. σχέση 12, σελ. 28.
[59]Καθώς $t^{p^s}=t$.

7 Γραμμική απεικόνιση στο χώρο των δυναμοσειρών.

Έστω $R \overset{\text{ορσ}}{=} \Omega_p[[X_1, X_2, \ldots, X_n]]$ ο χώρος των τυπικών δυναμοσειρών με συντελεστές από το Ω_p.

Θα συμβολίζουμε με X^u το μονώνυμο $X_1^{u_1} X_2^{u_2} \cdots X_n^{u_n}$, όπου $u = (u_1, \ldots, u_n) \in U$ με το U να συμβολίζει το σύνολο των διατεταγμένων n-άδων με συντελεστές μη αρνητικούς ακεραίους. Ένα τυπικό στοιχείο τότε του R θα έχει τη μορφή $\sum\limits_{u \in U} a_u X^u$, ή, γιά συντομία, $\sum a_u X^u$, όπου $a_u \in \Omega_p$.
Ο R είναι ένας διανυσματικός χώρος με βάση το $\{X^u | u \in U\}$.

Γιά κάθε $\mathrm{G} \in R$, ορίζουμε τη γραμμική απεικόνιση $\mathrm{G} : R \longrightarrow R$ με $\mathrm{G}(r) = \mathrm{G}r$ και γιά κάθε θετικό ακέραιο q, (όπου το q θα συμβολίζει μία δύναμη κάποιου πρώτου p), τη γραμμική απεικόνιση $\mathrm{T}_q : R \longrightarrow R$ με $\mathrm{T}_q(\sum a_u X^u) = \sum a_u X^{\frac{u}{q}}$ όπου

$$X^{\frac{u}{q}} = \begin{cases} X_1^{\frac{u_1}{q}} \cdot \ldots \cdot X_n^{\frac{u_n}{q}}, & \text{αν } q|u_i \text{ γιά κάθε } i \\ 0, & \text{αλλιώς.} \end{cases}$$

Έστω τώρα $\Psi_{q,\mathrm{G}} \overset{\text{ορσ}}{=} \mathrm{T}_q \circ \mathrm{G} : R \longrightarrow R$. Αν $\mathrm{G} = \sum\limits_{w \in U} g_w X^w$, τότε η γραμμική απεικόνιση $\Psi_{q,\mathrm{G}}$ δρα στα στοιχεία X^u της βάσης του R ως εξής : $\Psi_{q,\mathrm{G}}(X^u) = \mathrm{T}_q(\sum\limits_{w \in U} g_w X^{w+u}) = \sum\limits_{v \in U} g_{qv-u} X^v$. Έστω $\mathrm{G}_q(X) \overset{\text{ορσ}}{=} \mathrm{G}(X^q) = \sum\limits_{w \in U} g_w X^{qw}$. Τότε ισχύουν οι σχέσεις :

$$\mathrm{G} \circ \mathrm{T}_q = \mathrm{T}_q \circ \mathrm{G}_q = \Psi_{q,G_q},^{60} \tag{17}$$

$$\underbrace{T_q \circ \cdots \circ \mathrm{T}_q}_{n} = \mathrm{T}_{q^n}, \tag{18}$$

$$\text{γιά κάθε } n \in \mathbb{N}, \quad (\mathrm{G} \cdot \mathrm{G}_q \cdot \ldots \cdot \mathrm{G}_{q^n})_q \circ \mathrm{G} = \mathrm{G} \cdot \mathrm{G}_q \cdot \ldots \cdot \mathrm{G}_{q^{n+1}}.^{61} \tag{19}$$

Ορίζουμε τη συνάρτηση $|\cdot| : U \longrightarrow \mathbb{N}_0$, με $|u| = \sum\limits_{i=1}^{n} u_i$, και έστω $R_0 \overset{\text{ορσ}}{=} \{\mathrm{G} = \sum\limits_{w \in U} g_w X^w \in R|$ για κάποιο $M > 0$, $\mathrm{ord}_p g_w \geq M|w|$ γιά κάθε

[60] Βλ. παράρτημα
[61] Βλ. παράρτημα

$w \in U\}$.

Είναι εύκολο να δει κανείς ότι το R_0 είναι κλειστό ως προς τον πολλαπλασιασμό[62] και την απεικόνιση $R \ni G \mapsto G_q$.[63]

Έστω $A : V \longrightarrow V$ γραμμική απεικόνιση σε κάποιον πεπερασμένης διάστασης διανυσματικό χώρο V πάνω από ένα σώμα F. Αν το F είναι εφοδιασμένο με μία μετρική, έστω d, γενικεύουμε την έννοια του ίχνους, $\mathrm{Tr}A$, της A, και στην περίπτωση που ο V είναι απειροδιάστατος, ορίζοντας $\mathrm{Tr}A \overset{\text{ορσ}}{=} \sum_{i=1}^{\infty} a_{ii}$ όπου a_{ii} είναι τα διαγώνια στοιχεία του "άπειρου" πίνακα της γραμμικής απεικόνισης A, υπό την προυπόθεση βέβαια ότι η $\sum_{i=1}^{n} a_{ii}$ συγκλίνει ως προς την d.

Λήμμα : 7.1 *Έστω $G \in R_0$ και $\Psi \overset{\text{ορσ}}{=} \Psi_{q,G}$. Τότε το $\mathrm{Tr}(\Psi^s)$ συγκλίνει γιά κάθε $s \in \mathbb{N}$, και*

$$(q^s-1)^n \mathrm{Tr}(\Psi^s) = \sum_{x \in \Omega_p^n \text{ με } x^{q^s-1}=1} \mathrm{G}(x)\mathrm{G}(x^q)\mathrm{G}(x^{q^2})\cdots \mathrm{G}(x^{q^{s-1}}),$$

όπου $x = (x_1, \ldots, x_n)$, $x^{q^i} = (x_1^{q^i}, \ldots, x_n^{q^i})$ και $x^{q^s-1} = 1$ σημαίνει $x_j^{q^s-1} = 1$ γιά $j = 1, \ldots, n$.

Απόδειξη : Θα το αποδείξουμε πρώτα γιά $s = 1$. Έχουμε ότι $\Psi(X^u) = \sum_{v \in U} g_{qv-u} X^v$, άρα $\mathrm{Tr}\Psi = \sum_{u \in U} g_{(q-1)u}$, το οποίο συγκλίνει καθώς $G \in R_0$.[64]
Επειδή γιά κάθε $i = 1, \ldots, n$ ισχύει ότι [65]

$$\sum_{x_i \in \Omega_p \text{ με } x_i^{q-1}=1} x_i^{w_i} = \begin{cases} q-1, & \text{αν } q-1 | w_i \\ 0, & \text{αλλιώς} \end{cases},$$

θα έχουμε , γιά κάθε $w = (w_1, \ldots, w_n)$,

$$\sum_{x \in \Omega_p^n \text{ με } x^{q-1}=1} x^w = \prod_{i=1}^{n} \Big(\sum_{x_j^{q-1}=1} x_j^{w_i} \Big) = \begin{cases} (q-1)^n, & \text{αν } q-1 | w \\ 0, & \text{αλλιώς} \end{cases}$$

[62] Βλ. Παράρτημα

[63] Βλ. Παράρτημα

[64] Αν $u_1, u_2, \ldots, u_n, \ldots$ είναι μία αρίθμηση των στοιχείων του U, τότε $\mathrm{ord}_p(g_{(q-1)u_i}) \geq M(q-1)|u_i|$ αλλά και $|u_i| \overset{i\to\infty}{\longrightarrow} \infty$ (Αν όχι, τότε θα υπήρχε $N > 0$ τ.ώ. γιά κάθε i_0 να είναι δυνατή η εύρεση κάποιου $i_1 > i_0$ με $|u_{i_1}| < N$, άτοπο, καθώς υπάρχουν πεπερασμένα u_i με $|u_i| < N$) άρα το $\mathrm{Tr}\Psi = \sum_{u \in U} g_{(q-1)u}$ συγκλίνει.

[65] Βλ. παράρτημα

Άρα,

$$\sum_{x^{q-1}=1} \mathrm{G}(x) = \sum_{w\in U} g_w \sum_{x^{q-1}=1} x^w = (q-1)^n \sum_{u\in U} g_{(q-1)u} = (q-1)^n \mathrm{Tr}\Psi.$$

Έστω τώρα ότι $s > 1$. Τότε θα έχουμε :

$$\Psi^s = \mathrm{T}_q \circ \mathrm{G} \circ \mathrm{T}_q \circ \mathrm{G} \circ \Psi^{s-2} \stackrel{17}{=} \mathrm{T}_q \circ \mathrm{T}_q \circ \mathrm{G}_q \circ \mathrm{G} \circ \Psi^{s-2} \stackrel{18,19}{=} \mathrm{T}_{q^2} \circ \mathrm{G} \cdot \mathrm{G}_q \circ \Psi^{s-2} =$$

$$\mathrm{T}_{q^2} \circ \mathrm{G} \cdot \mathrm{G}_q \circ \mathrm{T}_q \circ \mathrm{G} \circ \Psi^{s-3} \stackrel{17}{=} \mathrm{T}_{q^2} \circ \mathrm{T}_q \circ (\mathrm{G} \cdot \mathrm{G}_q)_q \circ \mathrm{G} \circ \Psi^{s-3} \stackrel{18,19}{=}$$

$$\mathrm{T}_{q^3} \circ \mathrm{G} \cdot \mathrm{G}_q \cdot \mathrm{G}_{q^2} \circ \Psi^{s-3} = \cdots = \mathrm{T}_{q^s} \circ \mathrm{G} \cdot \mathrm{G}_q \cdot \mathrm{G}_{q^2} \cdots \mathrm{G}_{q^{s-1}} =$$

$$\Psi_{q^s, \mathrm{G}\cdot\mathrm{G}_q\cdot\mathrm{G}_{q^2}\cdots\mathrm{G}_{q^{s-1}}}.$$

Αντικαθιστώντας τώρα όπου q το q^s, και όπου G το $\mathrm{G} \cdot \mathrm{G}_q \cdot \ldots \cdot \mathrm{G}_{q^{s-1}}$, έχουμε το ζητούμενο. □

Στο σημείο αυτό παρεμβάλουμε ένα γενικό λήμμα.

Λήμμα : 7.2 *Έστω $(A_k)_k, (B_k)_k, \ldots, (W_k)_k$ πεπερασμένο πλήθος αυξουσών ακολουθιών δεικτών με $\#A_k, \#B_k, \ldots, \#W_k < \infty$ γιά κάθε k και αντίστοιχες άπειρες ενώσεις $A, B, \ldots, W$. Έστω ακόμα ότι η σειρά $\sum_{a\in A}\sum_{b\in B}\cdots\sum_{w\in W} f(a,b,\ldots,w)$ συγκλίνει στο $s \in \Omega_p$. Τότε $\lim_{k\to\infty} \sum_{a\in A_k}\sum_{b\in B_k}\cdots\sum_{w\in W_k} f(a,b,\ldots,w) = s$.*

Απόδειξη : Θέτουμε, γιά κάθε k, $I_k = A_k \times B_k \times \cdots \times W_k$, οπότε έχω μία αύξουσα ακολουθία συνόλων $(I_k)_k$ με ένωση $I = A \times B \times \cdots \times W$. Η διάταξη των $(a, b, \ldots, w)$ δεν παίζει ρόλο, συνεπώς ξέρουμε ότι $\sum_{i\in I} f(i) = s \in \Omega_p$. Ορίζουμε τυχαία διάταξη στο I_1 και, επαγωγικά, γιά κάθε $k \geq 1$, ορίζουμε τυχαία διάταξη στο I_{k+1} που σέβεται αυτήν του I_k και κάθε $i \in I_{k+1} \backslash I_k$ είναι μεγαλύτερο από κάθε στοιχείο του I_k. Αυτό είναι εφικτό καθώς τα σύνολα I_k είναι πεπερασμένα. Έτσι επάγεται μία διάταξη $\prec$ στο I και θεωρώ $I = \{i_1 \prec i_2 \prec i_3 \prec \ldots\}$, άρα $s = \sum_{\nu=1}^{\infty} f(i_\nu)$. Αν τώρα θέσουμε $z_k = \sum_{i\in I_k} f(i)$, το οποίο είναι ένα πεπερασμένο άθροισμα, τότε η ακολουθία $(z_k)_k$ είναι υπακολουθία της ακολουθίας των μερικών αθροισμάτων $\sum_{\nu=1}^{n} f(i_\nu)$, άρα

$$\lim_{k\to\infty} \sum_{a\in A_k} \sum_{b\in B_k} \cdots \sum_{w\in W_k} f(a,b,\ldots,w) = \lim_{k\to\infty} z_k = s. \ \square$$

Επιστρέφουμε στην προαναφερθείσα F-γραμμική απεικόνιση $A : V \longrightarrow V$ στον πεπερασμένης διάστασης, έστω n, διανυσματικό χώρο V. Γνωρίζουμε ότι το χαρακτηριστικό πολυώνυμο του πίνακα A που ορίζει η A είναι το $\mathrm{char}(A) = \det(I - At) = \sum_{m=0}^{n} b_m t^m$, όπου

$$b_m = (-1)^m \sum_{\substack{1\le i_1<\ldots<i_m\le n \\ \sigma\in S_m}} sgn(\sigma) a_{i_{\sigma(1)},i_1} \cdot \ldots \cdot a_{i_{\sigma(m)},i_m} =$$

$$(-1)^m \sum_{1\le i_1<\ldots<i_m\le n} \begin{vmatrix} a_{i_1,i_1} & \ldots & a_{i_1,i_m} \\ \vdots & \vdots & \vdots \\ a_{i_m,i_1} & \ldots & a_{i_m,i_m} \end{vmatrix}.$$

Αν το σώμα F είναι εφοδιασμένο με μία μετρική d και ο V είναι απειροδιάστατος, δηλαδή ο A είναι ένας άπειρος πίνακας, τότε έχει νόημα να μιλάμε γιά το χαρακτηριστικό του πολυώνυμο $\det(I - At)$ του A ως τυπική δυναμοσειρά με συντελεστές από το F, δεδομένου βέβαια ότι το άθροισμα που καθορίζει τον b_m, που τώρα θα είναι μία άπειρη σειρά της μορφής

$$b_m = (-1)^m \sum_{\substack{1\le i_1<\ldots<i_m \\ \sigma\in S_m}} sgn(\sigma) a_{i_{\sigma(1)},i_1} \cdot \ldots \cdot a_{i_{\sigma(m)},i_m} =$$

$$(-1)^m \sum_{1\le i_1<\ldots<i_m} \begin{vmatrix} a_{i_1,i_1} & \ldots & a_{i_1,i_m} \\ \vdots & \vdots & \vdots \\ a_{i_m,i_1} & \ldots & a_{i_m,i_m} \end{vmatrix}, \tag{20}$$

συγκλίνει ως προς την d. Ορίζουμε

$$b_{m,k} = (-1)^m \sum_{\substack{1\le i_1<\ldots<i_m\le m+k \\ \sigma\in S_m}} sgn(\sigma) a_{i_{\sigma(1)},i_1} \cdot \ldots \cdot a_{i_{\sigma(m)},i_m},$$

γιά $m \ge 1$ και $k \ge 0$, και $b_m = \lim_{k\to\infty} b_{m,k}$, εφόσον το όριο υπάρχει.

Θα εξετάσουμε παρακάτω αν μπορούμε να εφαρμόσουμε τα προαναφερθέντα στην περίπτωση που ο πίνακας A είναι ο πίνακας που ορίζει η Ω_p-γραμμική απεικόνιση $\Psi = \mathrm{T}_q \circ \mathrm{G} : R \longrightarrow R$, όπου $\mathrm{G} \in R_0$.

Θεωρούμε μία αρίθμηση του συνόλου δεικτών $U : u_1, u_2, u_3, \ldots$. Είναι εξυπηρετικό να θεωρήσουμε $u_1 \prec u_2 \prec u_3 \prec \ldots$, όπου $u \prec v$ σημαίνει εξ' ορισμού,

$|u| < |v|$ είτε $|u| = |v|$ και το u είναι "μικρότερο" του v ως προς τη λεξικογραφική διάταξη. Είναι $\Psi(X^{u_j}) = \Psi_{q,G}(X^{u_j}) = \sum_{i=1}^{\infty} g_{qu_i - u_j} X^{u_i}$, άρα ο πίνακας A της Ψ ως προς τη βάση $X^{u_1}, X^{u_2}, \dots$ είναι

$$\mathbf{A} = \begin{pmatrix} g_{qu_1-u_1} & g_{qu_1-u_2} & \cdots & g_{qu_1-u_j} & \cdots \\ g_{qu_2-u_1} & g_{qu_2-u_2} & \cdots & g_{qu_2-u_j} & \cdots \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ g_{qu_i-u_1} & g_{qu_i-u_2} & \cdots & g_{qu_i-u_j} & \cdots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{pmatrix}.$$

Θα δείξουμε ότι γιά κάθε m, το άπειρο άθροισμα b_m στην 20 συγκλίνει στο Ω_p. Γιά τον συγκεκριμένο πίνακα A έχουμε $a_{ij} = g_{qu_i - u_j}$, άρα ο τυπικός προσθεταίος του αθροίσματος 20 είναι $sgn(\sigma) g_{qu_{i_{\sigma(1)}} - u_{i_1}} \cdot \dots \cdot g_{qu_{i_{\sigma(m)}} - u_{i_m}}$, όπου $1 \le i_1 < \ldots < i_m$ και $\sigma \in S_m$. Άρα η ord_p αυτού του όρου είναι $\ge M(|qu_{i_{\sigma(1)}} - u_{i_1}| + \cdots + |qu_{i_{\sigma(m)}} - u_{i_m}|) = M(q \sum_{j=1}^{m} |u_{i_{\sigma(j)}}| - \sum_{j=1}^{m} |u_{i_j}|) =$ [66] $M(q-1) \sum_{j=1}^{m} |u_{i_j}|$.
Ακόμα, στην περίπτωσή μας,

$$b_{m,k} = (-1)^m \sum_{\substack{1 \le i_1 < \ldots < i_m \le m+k \\ \sigma \in S_m}} sgn(\sigma) g_{qu_{i_{\sigma(1)}} - u_{i_1}} \cdot \dots \cdot g_{qu_{i_{\sigma(m)}} - u_{i_m}}.$$

Γιά σταθερό m η ακολουθία $\{b_{m,k}\}_k$ είναι Cauchy. Πράγματι, αν $n_2 > n_1$ τότε

$$b_{m,n_2} - b_{m,n_1} = (-1)^m \sum_{\substack{1 \le i_1 < \ldots < i_m \le m+n_2 \\ \sigma \in S_m}}^{n_1} sgn(\sigma) g_{qu_{i_{\sigma(1)}} - u_{i_1}} \cdot \dots \cdot g_{qu_{i_{\sigma(m)}} - u_{i_m}}, \tag{21}$$

όπου το $\sum^{n_1}$ δηλώνει ότι τουλάχιστον ένα από τα $i_1, \dots, i_m$ είναι $> n_1$.
Όμως, γιά δοθέν M_0, πεπερασμένα το πλήθος $u \in U$ έχουν $|u| \le M_0$, άρα υπάρχει n_0 τ.ώ. αν $k > n_0$, τότε $|u_k| > M_0$. Αν λοιπόν θεωρήσω $n_1 \ge n_0$, τότε η ord_p του τυπικού προσθετέου στο δεξί μέλος της 21 είναι $\ge M(q-1) \sum_{j=1}^{m} |u_{i_j}|$ και $i_{j_0} > n_1 \ge n_0$ γιά κάποιο $j_0 \in \{1, \dots, m\}$. Συνεπώς $|u_{i_{j_0}}| > M_0$ άρα η ord_p είναι $> M(q-1)M_0$.

[66] Καθώς $\sum_{j=1}^{m} |u_{i_{\sigma(j)}}| = \sum_{j=1}^{m} |u_{i_j}|$.

Θα δείξουμε επιπλέον ότι η $\sum_{m=0}^{\infty} b_m t^m$, όπου

$$b_m = (-1)^m \sum_{\substack{1\le i_1<\ldots<i_m \\ \sigma\in S_m}} sgn(\sigma) g_{qu_{i_{\sigma(1)}}-u_{i_1}} \cdot \ldots \cdot g_{qu_{i_{\sigma(m)}}-u_{i_m}} \in \Omega_p,$$

είναι μία συνάρτηση ορισμένη σε όλο το Ω_p. Έχει δηλαδή ως δυναμοσειρά, άπειρη ακτίνα σύγκλισης.

Έχουμε ότι αν $m \geq 2^n e^{n+1}$ τότε $\sum_{j=1}^{m} |u_{i_j}| \geq \dfrac{n}{6e} m^{\frac{n+1}{n}}$, [67] άρα $\mathrm{ord}_p b_{m,k} \geq M(q-1)\sum_{j=1}^{m} |u_{i_j}| \geq M(q-1)\dfrac{n}{6e} m^{\frac{n+1}{n}}$, οπότε και $\mathrm{ord}_p b_m \geq M(q-1)\frac{n}{6e} m^{\frac{n+1}{n}} = Cm^{\frac{1}{n}} m$. Άρα $\frac{1}{m}\mathrm{ord}_p b_m \geq Cm^{\frac{1}{n}}$, συνεπώς $|b_m|_p^{\frac{1}{m}} = p^{-\frac{1}{m}\mathrm{ord}_p b_m} \leq p^{-Cm^{\frac{1}{n}}}$. Έχουμε δηλαδή ότι $\frac{1}{|b_m|_p^{\frac{1}{m}}} \geq p^{Cm^{\frac{1}{n}}}$, όμως $\lim_{m\to\infty} Cm^{\frac{1}{n}} = +\infty$, οπότε η ακτίνα σύγκλισης $r = \dfrac{1}{\limsup_{m\to\infty} |b_m|_p^{\frac{1}{m}}} = +\infty$.

Στο σημείο αυτό ορίζουμε τον πίνακα $\mathbf{A}_{i_1,\ldots,i_m}$ γιά κάθε επιλογή δεικτών $1 \leq i_1 < i_2 < \ldots < i_m$ και επεκτείνουμε τον ορισμό $\det(I - \mathbf{A}t)$ στον άπειρο πίνακα $\mathbf{A}$ ως εξής :

$$\det(I-\mathbf{A}t) \overset{\text{ορσ}}{=} \sum_{m=0}^{\infty} (-1)^m \Big(\sum_{i_1<\ldots<i_m} \det(\mathbf{A}_{i_1,\ldots,i_m}) \Big) t^m \overset{\text{ορσ}}{=} \sum_{m=0}^{\infty} c_{\infty_m} t^m,$$

όπου

$$\mathbf{A}_{i_1,\ldots,i_m} \overset{\text{ορσ}}{=} \begin{pmatrix} g_{qu_{i_1}-u_{i_1}} & g_{qu_{i_1}-u_{i_2}} & \cdots & g_{u_{i_1}-u_{i_m}} \\ g_{qu_{i_2}-u_{i_1}} & g_{qu_{i_2}-u_{i_2}} & \cdots & g_{u_{i_2}-u_{i_m}} \\ \vdots & \vdots & \vdots & \vdots \\ g_{qu_{i_m}-u_{i_1}} & g_{qu_{i_m}-u_{i_2}} & \cdots & g_{qu_{i_m}-u_{i_m}} \end{pmatrix},$$

δηλαδή έχουμε ότι :

[67] Ισχύει ότι όταν $m \geq 2^n e^{n+1}$, τότε $\sum_{j=1}^{m} |u_{i_j}| \geq \dfrac{n}{6e} m^{\frac{n+1}{n}}$. Γιά περισσότερες λεπτομέρειες βλ. σημειώσεις Waldsmidt §3 Lemma 4.3

$$b_m = (-1)^m \sum_{i_1<\ldots<i_m} \det \begin{pmatrix} g_{qu_{i_1}-u_{i_1}} & g_{qu_{i_1}-u_{i_2}} & \cdots & g_{u_{i_1}-u_{i_m}} \\ g_{qu_{i_2}-u_{i_1}} & g_{qu_{i_2}-u_{i_2}} & \cdots & g_{u_{i_2}-u_{i_m}} \\ \vdots & \vdots & \vdots & \vdots \\ g_{qu_{i_m}-u_{i_1}} & g_{qu_{i_m}-u_{i_2}} & \cdots & g_{qu_{i_m}-u_{i_m}} \end{pmatrix}.$$

Θα αποδείξουμε κατόπιν, γιά τον πίνακα $\mathbf{A}$, τον τύπο

$$\det(I-\mathbf{A}t) = \exp\Big\{-\sum_{s=1}^{\infty} \mathrm{Tr}(\mathbf{A}^s)\frac{t^s}{s}\Big\}.$$

Ορίζοντας $\mathbf{A}^{(\kappa)}$ να είναι ο $\kappa \times \kappa$ άνω αριστερά υποπίνακας του $\mathbf{A}$, θέτουμε

$$\det(I-\mathbf{A}^{(\kappa)}t) = \sum_{m=0}^{\kappa}(-1)^m\Big(\sum_{1\le i_1<\ldots<i_m\le\kappa} \det(\mathbf{A}_{i_1,\ldots,i_m})\Big)t^m + 0\cdot t^{\kappa+1} + \ldots \overset{o\rho\sigma}{=}$$
$$\sum_{m=0}^{\infty} c_{\kappa_m} t^m = \mathrm{charpoly}(\mathbf{A}^{(\kappa)}) \in \Omega_p[[t]]$$

και παράλληλα έχουμε ότι

$$\exp\Big(-\sum_{s=1}^{\infty}\mathrm{Tr}((\mathbf{A}^{(\kappa)})^s)\frac{T^s}{s}\Big) = \sum_{n=0}^{\infty}\frac{\Big(-\sum_{s=1}^{\infty}\mathrm{Tr}((\mathbf{A}^{(\kappa)})^s)\frac{T^s}{s}\Big)^n}{n!} =$$
$$1 - \frac{\Big(\sum_{s=1}^{\infty}\mathrm{Tr}((\mathbf{A}^{(\kappa)})^s)\frac{T^s}{s}\Big)}{1!} + \frac{\Big(\sum_{s=1}^{\infty}\mathrm{Tr}((\mathbf{A}^{(\kappa)})^s)\frac{T^s}{s}\Big)^2}{2!} - \ldots$$
$$+(-1)^n\frac{\Big(\sum_{s=1}^{\infty}\mathrm{Tr}((\mathbf{A}^{(\kappa)})^s)\frac{T^s}{s}\Big)^n}{n!} + \ldots =$$
$$1 + \Big(-\frac{\frac{\mathrm{Tr}(\mathbf{A}^{(\kappa)})}{1}}{1!}\Big)T + \Big(-\frac{\frac{\mathrm{Tr}((\mathbf{A}^{(\kappa)})^2)}{2}}{1!} + \frac{\frac{\mathrm{Tr}^2(\mathbf{A}^{(\kappa)})}{1}}{2!}\Big)T^2 + \ldots$$
$$+\Big(\frac{-\frac{\mathrm{Tr}((\mathbf{A}^{(\kappa)})^n)}{n}}{1!} + \frac{\frac{\mathrm{Tr}^n(\mathbf{A}^{(\kappa)})}{1}}{n!}\Big)T^n + \ldots \overset{o\rho\sigma}{=} \sum_{m=0}^{\infty} d_{\kappa_m}T^m \in \Omega_p[[t]]^{68}$$

και ομοίως

$$\exp\Big(-\sum_{s=1}^{\infty}\mathrm{Tr}(\mathbf{A}^s)\frac{T^s}{s}\Big)=\sum_{n=0}^{\infty}\frac{\Big(-\sum\limits_{s=1}^{\infty}\mathrm{Tr}(\mathbf{A}^s)\frac{T^s}{s}\Big)^n}{n!}=$$

$$1-\frac{\Big(\sum\limits_{s=1}^{\infty}\mathrm{Tr}(\mathbf{A}^s)\frac{T^s}{s}\Big)}{1!}+\frac{\Big(\sum\limits_{s=1}^{\infty}\mathrm{Tr}(\mathbf{A}^s)\frac{T^s}{s}\Big)^2}{2!}-\dots$$

$$+(-1)^n\frac{\Big(\sum\limits_{s=1}^{\infty}\mathrm{Tr}(\mathbf{A}^s)\frac{T^s}{s}\Big)^n}{n!}+\dots=$$

$$1+\Big(-\frac{\frac{\mathrm{Tr}(\mathbf{A})}{1}}{1!}\Big)T+\Big(-\frac{\frac{\mathrm{Tr}(\mathbf{A}^2)}{2}}{1!}+\frac{\frac{\mathrm{Tr}^2(\mathbf{A})}{1}}{2!}\Big)T^2+\dots$$

$$+\Big(\frac{-\frac{\mathrm{Tr}(\mathbf{A}^n)}{n}}{1!}+\frac{\frac{\mathrm{Tr}^n(\mathbf{A})}{1}}{n!}\Big)T^n+\dots\overset{o\rho\sigma}{=}\sum_{m=0}^{\infty}d_{\infty_m}\in\Omega_p[[t]]$$

<u>Ισχυρισμός</u> : Γιά κάθε $\kappa>0$, ισχύει ότι

$$\det(I-\mathbf{A}^{(\kappa)}t)=\exp\Big\{-\sum_{s=1}^{\infty}\mathrm{Tr}((\mathbf{A}^{(\kappa)})^s)\frac{t^s}{s}\Big\}$$

<u>Απόδειξη</u> : Έστω $\kappa>0$. Καθώς το Ω_p είναι αλγεβρικά κλειστό, ο πίνακας $\mathbf{A}^{(\kappa)}$ είναι τριγωνίσιμος,[69] όμοιος δηλαδή προς έναν τριγωνικό πίνακα, έστω $\mathbf{A}_{\tau}^{(\kappa)}=\{a_{\kappa_{ij}}\}_{1\leq i,j\leq\kappa}$, και έχουμε ότι $\det(I-\mathbf{A}^{(\kappa)}t)=\det(I-\mathbf{A}_{\tau}^{(\kappa)}t)$, και γιά κάθε $s\geq1$, $\mathrm{Tr}((\mathbf{A}^{(\kappa)})^s)=\mathrm{Tr}((\mathbf{A}_{\tau}^{(\kappa)})^s)$.[70]
Άρα λοιπόν, επειδή $\det(I-\mathbf{A}^{(\kappa)}t)=\prod\limits_{i=1}^{\kappa}(1-a_{\kappa_{ii}}T)$ και $\mathrm{Tr}((\mathbf{A}^{(\kappa)})^s)=\sum\limits_{i=1}^{\kappa}a_{\kappa_{ii}}^s$,

[69] Βλ. παράρτημα

[70] Από την ομοιότητα του $\mathbf{A}^{(\kappa)}$ με τον $\mathbf{A}_{\tau}^{(\kappa)}$ έχουμε ότι $\mathbf{A}^{(\kappa)}=C\mathbf{A}_{\tau}^{(\kappa)}C^{-1}$ γιά κάποιον αντιστρέψιμο πίνακα $C\in\Omega_p^{\kappa^2}$.
Όμως τότε, γιά κάθε $s\geq1$ έχουμε $(\mathbf{A}^{(\kappa)})^s=\underbrace{C\mathbf{A}_{\tau}^{(\kappa)}C^{-1}\cdot\dots\cdot C\mathbf{A}_{\tau}^{(\kappa)}C^{-1}}_{s}=C(\mathbf{A}_{\tau}^{(\kappa)})^sC^{-1}$.
Άρα οι $\mathbf{A}^{(\kappa)}$, $\mathbf{A}_{\tau}^{(\kappa)}$ είναι όμοιοι και συνεπώς $\mathrm{Tr}((\mathbf{A}^{(\kappa)})^s)=\mathrm{Tr}((\mathbf{A}_{\tau}^{(\kappa)})^s)$.

έχουμε ότι

$$\exp\Big\{-\sum_{s=1}^{\infty}\mathrm{Tr}((\mathbf{A}^{(\kappa)})^s)\frac{t^s}{s}\Big\} = \exp\Big\{-\sum_{s=1}^{\infty}\sum_{i=1}^{\kappa} a^s_{\kappa ii}\frac{T^s}{s}\Big\} =$$

$$\exp\Big\{\sum_{i=1}^{\kappa}-\sum_{s=1}^{\infty} a^s_{\kappa ii}\frac{T^s}{s}\Big\} = \prod_{i=1}^{\kappa}\exp\Big\{-\sum_{s=1}^{\infty}\frac{(a_{\kappa ii}T)^s}{s}\Big\} =$$

$$\prod_{i=1}^{\kappa}\exp(\log_p(1-a_{\kappa ii}T)) = \prod_{i=1}^{\kappa}(1-a_{\kappa ii}T).^{71}$$

Σύμφωνα λοιπόν με τον ισχυρισμό, έχουμε ότι γιά κάθε $\kappa > 0$, $c_{\kappa m} = d_{\kappa m}$ γιά κάθε $m \geq 0$.

Όμως γιά κάθε $m \geq 0$,

$$c_{\kappa m} = (-1)^m \sum_{1\leq i_1<\ldots<i_m\leq\kappa} \det(\mathbf{A}_{i_1,\ldots,i_m}) \overset{\kappa\to\infty}{\longrightarrow} =$$

$$(-1)^m \sum_{1\leq i_1<\ldots<i_m} \det(\mathbf{A}_{i_1,\ldots,i_m}) = c_{\infty m},\ ^{72}$$

και ακόμα γιά κάθε $s \geq 1$, $\mathrm{Tr}((\mathbf{A}^{(\kappa)})^s) \overset{\kappa\to\infty}{\longrightarrow} \mathrm{Tr}(\mathbf{A}^s)$, [73] άρα

$$d_{\kappa m} \overset{\kappa\to\infty}{\longrightarrow} d_{\infty m}.$$

---

[72] Από το λήμμα 7.2, σελ. 63.

[73] Έστω $(A^\kappa)_{ij}$ και $(A)_{ij}$ το στοιχείο της i-οστής γραμμής - j-οστής στήλης του πίνακα $\mathbf{A}^\kappa$ και $\mathbf{A}$ αντίστοιχα. Λαμβάνοντας υπ'οψην ότι $((A^\kappa)^2)_{ij} = \sum_{\kappa_1=1}^{\kappa} A_{i\kappa_1}A_{\kappa_1 j}$, εύκολα διαπιστώνει κανείς ότι γιά κάθε $s \geq 1$ έχουμε $((A^\kappa)^s)_{ij} = \sum_{\kappa_{s-1}=1}^{\kappa}\sum_{\kappa_{s-2}=1}^{\kappa}\cdots\sum_{\kappa_1=1}^{\kappa}(A^\kappa)_{i\kappa_1}(A^\kappa)_{\kappa_1\kappa_2}\cdots(A^\kappa)_{\kappa_{s-1}j} = \sum_{\kappa_{s-1}=1}^{\kappa}\sum_{\kappa_{s-2}=1}^{\kappa}\cdots\sum_{\kappa_1=1}^{\kappa}(A)_{i\kappa_1}(A)_{\kappa_1\kappa_2}\cdots(A)_{\kappa_{s-1}j}$ και $(A^s)_{ij} = \sum_{\kappa_{s-1}=1}^{\infty}\sum_{\kappa_{s-2}=1}^{\infty}\cdots\sum_{\kappa_1=1}^{\infty}(A)_{i\kappa_1}(A)_{\kappa_1\kappa_2}\cdots(A)_{\kappa_{s-1}j}$. Έχουμε λοιπόν ότι $\mathrm{Tr}((\mathbf{A}^\kappa)^s) = \sum_{i=1}^{\kappa}\sum_{\kappa_{s-1}=1}^{\kappa}\sum_{\kappa_{s-2}=1}^{\kappa}\cdots\sum_{\kappa_1=1}^{\kappa}(A)_{i\kappa_1}(A)_{\kappa_1\kappa_2}\cdots(A)_{\kappa_{s-1}i}$ και $\mathrm{Tr}((\mathbf{A})^s) = \sum_{\kappa_{s-1}=1}^{\infty}\sum_{\kappa_{s-2}=1}^{\infty}\cdots\sum_{\kappa_1=1}^{\infty}(A)_{i\kappa_1}(A)_{\kappa_1\kappa_2}\cdots(A)_{\kappa_{s-1}i}$, και πιό συγκεκριμένα,
$\mathrm{Tr}((\mathbf{A}^\kappa)^s) = \sum_{i=1}^{\kappa}\sum_{\kappa_{s-1}=1}^{\kappa}\sum_{\kappa_{s-2}=1}^{\kappa}\cdots\sum_{\kappa_1=1}^{\kappa} g_{qu_i-u_{\kappa_{s-1}}}\cdot g_{qu_{\kappa_{s-1}}-u_{\kappa_{s-2}}}\cdot\ldots\cdot g_{qu_{\kappa_1}-u_i}$ και

Έπεται λοιπόν ότι γιά κάθε $m \geq 0$ έχουμε ότι $c_{\infty_m} = d_{\infty_m}$, συνεπώς

$$\det(I - \mathbf{A}t) = \exp\Big\{ -\sum_{s=1}^{\infty} \mathrm{Tr}(\mathbf{A}^s)\frac{t^s}{s}\Big\}$$

Συνοψίζοντας τα παραπάνω, καταλήγουμε στο εξής λήμμα:

Λήμμα 7.3 : Αν $\mathrm{G}(X) = \sum_{w \in U} g_w X^w \in R_0$, $\Psi = \mathrm{T}_q \circ \mathrm{G} : R \longrightarrow R$ και $\mathbf{A} = \{g_{qu_i - u_j}\}_{u_i, u_j \in U}$ είναι ο πίνακας της Ψ, τότε η σειρά $\det(I - \mathbf{A}t)$ είναι ένα καλώς ορισμένο στοιχείο του $\Omega_p[[t]]$ με άπειρη ακτίνα σύγκλισης και ισούται με $\exp\Big\{ -\sum_{s=1}^{\infty} \mathrm{Tr}(\mathbf{A}^s)\frac{t^s}{s}\Big\}$.

$\mathrm{Tr}((\mathbf{A})^s) = \sum_{i=1}^{\infty} \sum_{\kappa_{s-1}=1}^{\infty} \sum_{\kappa_{s-2}=1}^{\infty} \cdots \sum_{\kappa_1=1}^{\infty} g_{qu_i - u_{\kappa_{s-1}}} \cdot g_{qu_{\kappa_{s-1}} - u_{\kappa_{s-2}}} \cdot \ldots \cdot g_{qu_{\kappa_1} - u_i}.$
Την ύπαρξη του $\mathrm{Tr}((\mathbf{A})^s)$ μας εγγυάται το λήμμα 7.1, σελ. 62.
Τώρα, το ότι $\mathrm{Tr}((\mathbf{A}^{(\kappa)})^s) \overset{\kappa\to\infty}{\longrightarrow} \mathrm{Tr}(\mathbf{A}^s)$ είναι άμεση συνέπεια του λήμματος 7.2, σελ. 63.

8 Μία p-αδική αναλυτική έκφραση γιά τη συνάρτηση ζήτα.

Στην ενότητα αυτή θα δείξουμε την εξής πρόταση :

Πρόταση 8.1 *Η συνάρτηση ζήτα, $Z(H_f/\mathbb{F}_q;T) \in 1+T\mathbb{Z}[[T]] \subset 1+T\Omega_p[[T]]$, κάθε υπερεπιφάνειας H_f που ορίζεται από το $f(X_1,\dots,X_n) \in \mathbb{F}_q[X_1,\dots,Xn]$, είναι πηλίκο δυναμοσειρών με συντελεστές στο $\Omega_p[[T]]$, σταθερό όρο μονάδα και άπειρη ακτίνα σύγκλισης, ή αλλιώς, p-αδικά μερόμορφη.*

Θα το αποδείξουμε με επαγωγή ως προς τον αριθμό n των μεταβλητών, ή ισοδύναμα, ως προς τη διάσταση $n-1$ της διάστασης της υπερεπειφάνειας H_f.

Γιά $n=0$ το ζητούμενο ισχύει κατά τετριμμένο τρόπο, αφού τότε $Z(H_f/\mathbb{F}_q;T) = 1$. Έστω ότι το ζητούμενο ισχύει γιά κάθε κ με $0 \le \kappa \le n-1$, όπου κ το πλήθος των μεταβλητών.
Ισχυρισμός : Αρκεί να αποδειχτεί το ζητούμενο γιά την

$$Z'(H_f/\mathbb{F}_q;T) \overset{\text{ορσ}}{=} \exp\Big(\sum_{s=1}^{\infty} N_s' \frac{T^s}{s}\Big),$$

όπου

$$\begin{aligned} N_s' &\overset{\text{ορσ}}{=} \#\{(x_1,\dots,x_n) \in \mathbb{F}_{q^s}^n : f(x_1,\dots,x_n)=0 \ \text{ και } \ x_i \neq 0 \ \forall i=1,\dots,n\} \\ &= \#\{(x_1,\dots,x_n) \in \mathbb{F}_{q^s}^n : f(x_1,\dots,x_n)=0 \ \text{ και } \ x_i^{q^s-1}=1 \ \ \forall i=1,\dots,n\}. \end{aligned}$$

Απόδειξη του ισχυρισμού : Έχουμε ότι

$$Z(H_f/\mathbb{F}_q;T) = Z'(H_f/\mathbb{F}_q;T)\exp\Big(\sum_{s=1}^{\infty}(N_s - N_s')\frac{T^s}{s}\Big)$$

όπου $\exp\Big(\sum_{s=1}^{\infty}(N_s - N_s')\frac{T^s}{s}\Big) = Z(\bigcup_{i=1}^{n} H_i/\mathbb{F}_q;T)$ με

$$H_i = \{(x_1,\dots,x_n) \in \mathbb{F}_{q^s}^n : f(x_1,\dots,x_n)=0 \ \text{ και } \ X_i=0\}\ ^{74}.$$

Όμως βάσει της πρότασης 15, σελ. 49, αποδεικνύεται ότι

[74] $\dim H_i = n-2$

$$Z(\bigcup_{i=1}^{n} H_i/\mathbb{F}_q;T) = \frac{\displaystyle\prod_{\substack{1\le i_1<\ldots<i_m\le n \\ 1\le m \ \text{περιττός} \le n}} Z(H_f/\mathbb{F}_q;T)(H_{i_1,\ldots,i_m}/\mathbb{F}_q;T)}{\displaystyle\prod_{\substack{1\le i_1<\ldots<i_m\le n \\ 2\le m \ \text{άρτιος} \le n}} Z(H_f/\mathbb{F}_q;T)(H_{i_1,\ldots,i_m}/\mathbb{F}_q;T)}$$

όπου

$$H_{i_1,\ldots,i_\kappa} \overset{\text{ορσ}}{=} \{(x_1,\ldots,x_n)\in\mathbb{F}_{q^s}^n : f(x_1,\ldots,x_n)=0 \ \text{ και } \ x_{i_1}=\ldots=x_{i_\kappa}=0\},$$

άρα ο ισχυρισμός είναι αληθής λόγω της επαγωγικής υπόθεσης.

Έστω $s\ge 1$ και $q=p^r$. Υπενθυμίζουμε ότι αν t, είναι ο αντιπρόσωπος Teichmuller του $x\in\mathbb{F}_{q^s}$, τότε η p-οστή ρίζα της μονάδας $\varepsilon^{\mathrm{Tr}(x)}$ ως συνάρτηση του t, δίνεται από τον τύπο : $\varepsilon^{\mathrm{Tr}(x)}=\Theta(t)\Theta(t^p)\Theta(t^{p^2})\cdots\Theta(t^{p^{rs-1}})$.

Καθώς ισχύει ότι [75]

$$\sum_{x_0\in\mathbb{F}_{q^s}} \varepsilon^{\mathrm{Tr}(x_0u)} = \begin{cases} 0, & \text{αν } u\in\mathbb{F}_{q^s}^\times \\ q^s, & \text{αν } u=0 \end{cases} ,$$

αφαιρώντας τον προσθετέο που αντιστοιχεί στο $x_0=0$ έχουμε :

$$\sum_{x_0\in\mathbb{F}_{q^s}^\times} \varepsilon^{\mathrm{Tr}(x_0u)} = \begin{cases} -1, & \text{αν } u\in\mathbb{F}_{q^s}^\times \\ q^s-1, & \text{αν } u=0 \end{cases} .$$

Θέτοντας όπου $u\overset{\text{ορσ}}{=} f(x_1,\ldots,x_n)$ και εφαρμόζοντας το παραπάνω αθροίζοντας πάνω από όλα τα $x_1,\ldots,x_n\in\mathbb{F}_{q^s}^\times$, έχουμε :

$$\sum_{x_0,x_1,\ldots,x_n\in\ F_{q^s}^\times} \varepsilon^{\mathrm{Tr}(x_0 f(x_1,\ldots,x_n))} = (q^s-1)N_s'-((q^s-1)^n-N_s') = q^sN_s'-(q^s-1)^n.$$

Αντικαθιστώντας τώρα τους συντελεστές του $X_0f(X_1,\ldots,X_n)\in\mathbb{F}_q[X_0,\ldots,X_n]$ με τους αντίστοιχους αντιπροσώπους Teichmuller, προκύπτει το πολυώνυμο

$$F(X_0,\ldots,X_n) = (\text{έστω}) \sum_{i=1}^{N} t_iX^{w_i}\in\Omega_p[X_0,\ldots,X_n], \text{ όπου } X^{w_i}=X_0^{w_{i0}}X_1^{w_{i1}}\cdots X_n^{w_{in}}.$$

Άρα λοιπόν, συμβολίζοντας με $\sum'$ το $\displaystyle\sum_{\substack{x_0,x_1\ldots,x_n\in\Omega_p \\ x_0^{q^s-1}=\cdots=x_n^{q^s-1}=1}}$, έχουμε :

[75] Βλ. παράρτημα

$$q^s N_s' = (q^s-1)^n + \sum_{x_0,x_1,\dots,x_n \in \mathbb{F}_{q^s}^\times} \varepsilon^{\mathrm{Tr}(x_0 f(x_1,\dots,x_n))} =$$

$$(q^s-1)^n + \sum{}' \prod_{i=1}^{N} \Theta(t_i x^{w_i})\Theta(t_i^p x^{pw_i})\cdots\Theta(t_i^{p^{rs-1}} x^{p^{rs-1}w_i}) =$$

$$(q^s-1)^n + \sum{}' \prod_{i=1}^{N} \Big(\Theta(t_i x^{w_i})\cdots\Theta(t_i^{p^{r-1}} x^{p^{r-1}w_i})\Big)\Big(\Theta(t_i^{p^r} x^{p^r w_i})\cdots\Theta(t_i^{p^{2r-1}} x^{p^{2r-1}w_i})\Big)\cdot$$
$$\cdots\cdot\Big(\Theta(t_i^{p^{(s-1)r}} x^{p^{(s-1)r}w_i})\cdots\Theta(t_i^{p^{rs-1}} x^{p^{rs-1}w_i})\Big) =^{76}$$
$$(q^s-1)^n + \sum{}' \prod_{i=1}^{N} \Big(\Theta(t_i x^{w_i})\cdots\Theta(t_i^{p^{r-1}} x^{p^{r-1}w_i})\Big)\Big(\Theta(t_i x^{p^r w_i})\cdots\Theta(t_i^{p^{r-1}} x^{p^{2r-1}w_i})\Big)\cdot$$
$$\cdots\cdot\Big(\Theta(t_i x^{p^{(s-1)r}w_i})\cdots\Theta(t_i^{p^{r-1}} x^{p^{rs-1}w_i})\Big).$$

Θέτουμε τώρα

$$\mathrm{G}(X_0,\dots,X_n) \stackrel{\text{ορσ}}{=} \prod_{i=1}^{N} \Theta(t_i X^{w_i})\Theta(t_i^p X^{pw_i})\cdots\Theta(t_i^{p^{r-1}} X^{p^{r-1}w_i}),$$

συνεπώς
$$q^s N_s' = (q^s-1)^n + \sum_{\substack{x_0,x_1\dots,x_n\in\Omega_p\\ x_0^{q^s-1}=\cdots=x_n^{q^s-1}=1}} \mathrm{G}(x)\mathrm{G}(x^q)\mathrm{G}(x^{q^2})\cdots\mathrm{G}(x^{q^{s-1}})$$

Επειδή όμως $\Theta(t_i^{p^j} X^{p^j w_i}) \in R_0$ γιά κάθε $i=1,\dots,n$ και $j=1,\dots,r-1$ [77] και το R_0 είναι κλειστό ως προς τον πολλαπλασιασμό και την απεικόνιση $R \ni \mathrm{G} \mapsto G_q \in R$, έχουμε ότι $\mathrm{G}(X_0,\dots,X_n) \in R_0 \subset \Omega_p[[X_0,\dots,X_n]]$.

Από το λήμμα λοιπόν 7.1, σελ. 62, έχουμε ότι $q^s N_s' = (q^s-1)^n + (q^s-1)^{n+1}\mathrm{Tr}(\Psi^s)$ άρα

$$N_s' = \sum_{i=0}^{n}(-1)^i \binom{n}{i} q^{s(n-i-1)} + \sum_{i=0}^{n+1}\binom{n+1}{i} q^{s(n-i)}\mathrm{Tr}(\Psi^s),$$

και θέτοντας σύμφωνα με το λήμμα σελ. 56,

$$\Delta(T) \stackrel{\text{ορσ}}{=} \det(I-AT) = \exp\Big\{-\sum_{s=1}^{\infty}\mathrm{Tr}(\Psi^s)\frac{T^s}{s}\Big\},$$

[77] Βλ. παράρτημα

έχουμε τα εξής :

$$Z^{'}(H_f/\mathbb{F}_q;T) = \exp\Big\{\sum_{s=1}^{\infty} N_s^{'}\frac{T^s}{s}\Big\} =$$

$$\exp\Big\{\sum_{s=1}^{\infty}\Big(\sum_{i=0}^{n}(-1)^i\binom{n}{i}q^{s(n-i-1)} + \sum_{i=1}^{n+1}(-1)^i\binom{n+1}{i}q^{s(n-i)}\mathrm{Tr}(\Psi^s)\Big)\frac{T^s}{s}\Big\} =$$

$$\exp\Big\{\sum_{s=1}^{\infty}\Big(\sum_{i=0}^{n}(-1)^i\binom{n}{i}q^{s(n-i-1)}\frac{T^s}{s}+\sum_{i=0}^{n+1}(-1)^i\binom{n+1}{i}q^{s(n-i)}\mathrm{Tr}(\Psi^s)\frac{T^s}{s}\Big)\Big\} =$$

$$\exp\Big\{\sum_{i=0}^{n}\sum_{s=1}^{\infty}(-1)^i\binom{n}{i}q^{s(n-i-1)}\frac{T^s}{s}+\sum_{i=0}^{n+1}\sum_{s=1}^{\infty}(-1)^i\binom{n+1}{i}q^{s(n-i)}\mathrm{Tr}(\Psi^s)\frac{T^s}{s}\Big\} =$$

$$\prod_{i=0}^{n}\exp\Big\{\sum_{s=1}^{\infty}(-1)^i\binom{n}{i}q^{s(n-i-1)}\frac{T^s}{s}\Big\}$$

$$\times\prod_{i=0}^{n+1}\exp\Big\{\sum_{s=1}^{\infty}(-1)^i\binom{n+1}{i}q^{s(n-i)}\mathrm{Tr}(\Psi^s)\frac{T^s}{s}\Big\} =$$

$$\prod_{i=0}^{n}\Big(\exp\Big\{\sum_{s=1}^{\infty}q^{s(n-i-1)}\frac{T^s}{s}\Big\}\Big)^{(-1)^i\binom{n}{i}}$$

$$\times\prod_{i=0}^{n+1}\Big(\exp\Big\{\sum_{s=1}^{\infty}q^{s(n-i)}\mathrm{Tr}(\Psi^s)\frac{T^s}{s}\Big\}\Big)^{(-1)^i\binom{n+1}{i}} =$$

$$\prod_{i=0}^{n}\exp\Big\{-\sum_{s=1}^{\infty}(-1)^{s+1}\frac{(-q^{n-i-1})^s}{s}\Big\}^{(-1)^i\binom{n}{i}}$$

$$\times\prod_{i=0}^{n+1}\exp\Big\{-\sum_{s=1}^{\infty}\mathrm{Tr}(\Psi^s)\frac{(q^{n-i}T)^s}{s}\Big\}^{(-1)^{i+1}\binom{n+1}{i}} =$$

$$\prod_{i=0}^{n}\exp\{\log_p(1-q^{(n-i-1)T})\}^{(-1)^{i+1}\binom{n}{i}}\cdot\prod_{i=0}^{n+1}\Delta(q^{n-i}T)^{(-1)^{i+1}\binom{n+1}{i}} =$$

$$\prod_{i=0}^{n}(1-q^{n-i-1}T)^{(-1)^{i+1}\binom{n}{i}}\prod_{i=0}^{n+1}\Delta(q^{n-i}T)^{(-1)^{i+1}\binom{n+1}{i}}.$$

Λαμβάνοντας υπ'οψιν το γεγονός ότι, λόγω του λήμματος 7.3, γιά κάθε $a \in \Omega_p$, η $\Delta(aT)$ είναι μία δυναμοσειρά με άπειρη ακτίνα σύκλισης και σταθερό όρο μονάδα, παρατηρούμε ότι η τελευταία παράσταση είναι ένα κλάσμα, ο αριθμητής και ο παρονομαστής του οποίου είναι πεπερασμένα γινόμενα δυναμοσειρών με τις ίδιες ιδιότητες. Έπεται λοιπόν ότι η $Z^{'}(H_f/\mathbb{F}_q)$ είναι μερόμορφη.

Στην επόμενη ενότητα θα δείξουμε ότι η συνάρτηση ζήτα είναι ουσιαστικά ένα πηλίκο πολυωνύμων.

9 Το τελευταίο βήμα της απόδειξης.

Λήμμα : 9.1 *Έστω* $F(T) = \sum_{i=0}^{\infty} a_i T^i \in K[[T]]$*, όπου* K *ένα τυχαίο σώμα. Γιά κάθε* $m, s \geq 0$*, έστω* $A_{s,m}$ *ο πίνακας* $\{a_{s+i+j}\}_{0 \leq i,j \leq m}$:

$$\begin{pmatrix} a_s & a_{s+1} & a_{s+2} & \cdots & a_{s+m} \\ a_{s+1} & a_{s+2} & a_{s+3} & \cdots & a_{s+m+1} \\ a_{s+2} & a_{s+3} & a_{s+4} & \cdots & a_{s+m+2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{s+m} & a_{s+m+1} & a_{s+m+2} & \cdots & a_{s+2m} \end{pmatrix}$$

και έστω $N_{s,m} \overset{\text{ορσ}}{=} \det(A_{s,m})$.
Τότε $F(T) = \frac{P(T)}{Q(T)}$ όπου $P(T), Q(T) \in K[T]$ πολυώνυμα, αν και μόνο αν υπάρχουν ακέραιοι $m \geq 0$ και S τέτοιοι ώστε $N_{s,m} = 0$ όταν $s \geq S$.

Απόδειξη : ($\Longrightarrow$) Έστω ότι $F(T) = \frac{P(T)}{Q(T)}$ όπου $P(T), Q(T) \in K[T]$ πολυώνυμα. Έστω ακόμα $P(T) = \sum_{i=0}^{M} b_i T^i$ και $Q(T) = \sum_{i=0}^{N} c_i T_i$. Τότε, εξισώνοντας τους συντελεστές του T^i στη σχέση $F(T)Q(T) = P(T)$ γιά $i > \max(M, N)$ έχουμε : $\sum_{j=0}^{N} a_{i-N+j} c_{N-j} = 0$.
Έστω τώρα $S = \max(M - N + 1, 1)$ και $m \overset{\text{ορσ}}{=} N$.
Αν $s \geq S$, από την παραπάνω εξίσωση γιά $i = s + N, s + N + 1, \ldots, s + 2N$ έχουμε :

$$\begin{gathered} a_s c_N + a_{s+1} c_{N-1} + \ldots + a_{s+N} c_0 = 0 \\ a_{s+1} c_N + a_{s+2} c_{N-1} + \ldots + a_{s+N+1} c_0 = 0 \\ \vdots \\ a_{s+N} c_N + a_{s+N+1} c_{N-1} + \ldots + a_{s+2N} c_0 = 0. \end{gathered}$$

,ή αλλιώς

$$A_{s,N}\cdot\begin{pmatrix} c_N \\ c_{N-1} \\ \vdots \\ c_0 \end{pmatrix} = \mathbf{0}.$$

Όμως $(c_N,\ldots,c_0)\neq(0,\ldots,0)$, καθώς $Q(T)\neq 0$, άρα $N_{s,m}=N_{s,N}=0$ γιά $s\geq S$.

($\Longleftarrow$) Έστω m ο ελάχιστος φυσικός γιά τον οποίο υπάρχει ακέραιος S έτσι ώστε να ισχύει $N_{s,m}=0\ \forall s\geq S$. Τότε, θα δείξουμε πρώτα ότι $N_{s,m-1}\neq 0$ $\forall s\geq S$, και με βάση αυτό θα ολοκληρώσουμε την απόδειξη.
Ας υποθέσουμε λοιπόν ότι γιά κάποιο $s\geq S$ ισχύει $N_{s,m-1}=0$. Θα δείξουμε επαγωγικά ότι τότε $N_{s+j,m-1}=0$ γιά $j=1,2,\ldots$, οπότε θα έρθουμε σε αντίφαση με την επιλογή του m.

Λόγω της $N_{s,m-1}=0$, έπεται ότι υπάρχουν $b_0,\ldots,b_{m-1}\in\Omega_p$, με $(b_0,\ldots,b_{m-1})\neq(0,\ldots,0)$, τέτοια ώστε

$$b_0(a_s,a_{s+1},\ldots,a_{s+m-1})+b_1(a_{s+1},a_{s+2},\ldots,a_{s+m})+\ldots+\\ b_{m-1}(a_{s+m-1},a_{s+m},\ldots,a_{s+2m-2})=0.$$

Έστω j_0 το ελάχιστο $j\in\{0,\ldots,m-1\}$ με $b_j\neq 0$ και έστω

$$b=a_{s+m+j_0}-\tfrac{b_{j_0+1}}{b_{j_0}}a_{s+m+j_0+1}-\ldots-\tfrac{b_{m-1}}{b_{j_0}}a_{s+2m-1}\in\Omega_p.$$

$i)$ Αν $j_0>0$, τότε

$$N_{s,m}=\det\left(\begin{array}{cccccc|c} a_s & a_{s+1} & a_{s+2} & \cdots & a_{s+m-2} & & a_{s+m} \\ - & - & - & - & - & \neg & \\ a_{s+1} & a_{s+2} & a_{s+3} & \cdots & a_{s+m-1} & & a_{s+m+1} \\ \vdots & \vdots & \vdots & \cdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & 0 & & b \\ \vdots & \vdots & \vdots & \cdots & \vdots & & \vdots \\ a_{s+m} & a_{s+m+1} & a_{s+m+2} & \cdots & a_{s+2m-2} & & a_{s+2m} \end{array}\right),$$

,

όπου η γραμμή $(0,\ldots,0,b)$ είναι στη j_0+1 θέση.

Αυτό διότι, αν $j_0=m-1$, τότε η προτελευταία γραμμή του $A_{s,m}$ είναι $(0,\ldots,0,b)$, ενώ αν $j_0<m-1$ τότε, αντικαθιστώντας στον $A_{s,m}$ την $(j_0+1)-$οστή γραμμή με την

$$(a_{s+j_0},\dots a_{s+j_0+m})-\frac{b_{j_0+1}}{b_{j_0}}(a_{s+j_0+1},\dots,a_{s+j_0+m+1})-\dots-$$
$$\frac{b_{m-1}}{b_{j_0}}(a_{s+m-1},\dots,a_{s+2m-1})$$

έπεται το ζητούμενο. Η ορίζουσα του κάτω αριστερά υποπίνακα είναι ίση με $N_{s+1,m-1}=0$.

$ii)$ Αν $j_0=0$, τότε

$$N_{s,m}=\det\begin{pmatrix} 0 & | & 0 & \cdots & 0 & & b \\ - & - & - & - & - & \urcorner & \\ a_{s+1} & | & a_{s+2} & \cdots & & | & a_{s+m+1} \\ \vdots & | & \vdots & \cdots & & | & \vdots \\ \vdots & \vdots & \vdots & \cdots & \vdots & | & \vdots \\ & \llcorner & - & - & & \lrcorner & - \\ a_{s+m} & a_{s+m+1} & a_{s+m+2} & \cdots & a_{s+2m-2} & | & a_{s+2m} \end{pmatrix},$$

απ'οπου προκύπτει ότι $0=N_{s,m}=N_{s+1,m-1}b$.
α)Αν $b\neq 0$, τότε $N_{s+1,m-1}=0$.
β)Αν $b=0$, τότε, επειδή λόγω της συμμετρικότητας του $A_{s,m}$, η ορίζουσα του πάνω δεξιά υποπίνακα του $A_{s,m}$ είναι η $N_{s+1,m-1}$, πάλι έχουμε ότι $N_{s+1,m-1}=0$.
Σε κάθε περίπτωση λοιπόν έχουμε ότι $N_{s+1,m-1}=0$.

Δείξαμε ότι : $N_{s,m-1}=0\Rightarrow N_{s+1,m-1}=0$, οπότε, επαγωγικά, $N_{s+j,m-1}=0\ \forall j\geq 1$, κάτι πού αντιφάσκει με την επιλογή του m.
Συμπεραίνουμε λοιπόν ότι γιά κάθε $s\geq S$, έχουμε ότι $N_{s,m}=0$ και $N_{s,m-1}\neq 0$.
Θεωρούμε τον πίνακα

$$\begin{pmatrix} a_S & a_{S+1} & \cdots & a_{S+m-1} & a_{S+m} \\ a_{S+1} & a_{S+2} & \cdots & a_{S+m} & a_{S+m+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{S+m-2} & a_{S+m-1} & \cdots & a_{S+2m-3} & a_{S+2m-2} \\ a_{S+m-1} & a_{S+m} & \cdots & a_{S+2m-2} & a_{S+2m-1} \end{pmatrix}.$$

Καθώς $N_{S,m-1}\neq 0$, έπεται ότι η τάξη του πίνακα είναι m. Υπάρχει λοιπόν $(u_m,\dots,u_0)\neq(0,\dots,0)$ με

$$\begin{pmatrix} a_S & a_{S+1} & \cdots & a_{S+m-1} & a_{S+m} \\ a_{S+1} & a_{S+2} & \cdots & a_{S+m} & a_{S+m+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{S+m-2} & a_{S+m-1} & \cdots & a_{S+2m-3} & a_{S+2m-2} \\ a_{S+m-1} & a_{S+m} & \cdots & a_{S+2m-2} & a_{S+2m-1} \end{pmatrix} \begin{pmatrix} u_m \\ u_{m-1} \\ \vdots \\ u_0 \end{pmatrix} = \mathbf{0}$$

Επειδή τώρα $N_{S,m} = 0$, η επισύναψη στον παραπάνω πίνακα της γραμμής $(a_{S+m}, \ldots, a_{S+2m})$ δεν αυξάνει την τάξη του πίνακα, συνεπώς η γραμμή $(a_{S+m}, \ldots, a_{S+2m})$ είναι γραμμικός συνδιασμός των υπολείπων γραμμών. Έπεται ότι $a_{S+m}u_m + \ldots + a_{S+2m}u_0 = 0$.

Θεωρούμε τώρα τον πίνακα

$$\begin{pmatrix} a_{S+1} & a_{S+2} & \cdots & a_{S+m} & a_{S+m+1} \\ a_{S+2} & a_{S+3} & \cdots & a_{S+m+1} & a_{S+m+2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{S+m-1} & a_{S+m} & \cdots & a_{S+2m-2} & a_{S+2m-1} \\ a_{S+m} & a_{S+m+1} & \cdots & a_{S+2m-1} & a_{S+2m} \end{pmatrix}.$$

Καθώς $N_{S+1,m-1} \neq 0$, έπεται ότι η τάξη του πίνακα είναι m. Ακόμα

$$\begin{pmatrix} a_{S+1} & a_{S+2} & \cdots & a_{S+m} & a_{S+m+1} \\ a_{S+2} & a_{S+3} & \cdots & a_{S+m+1} & a_{S+m+2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{S+m-1} & a_{S+m} & \cdots & a_{S+2m-2} & a_{S+2m-1} \\ a_{S+m} & a_{S+m+1} & \cdots & a_{S+2m-1} & a_{S+2m} \end{pmatrix} \begin{pmatrix} u_m \\ u_{m-1} \\ \vdots \\ u_0 \end{pmatrix} = \mathbf{0}$$

Όμοια με προηγουμένως, επειδή $N_{S+1,m} = 0$, η επισύναψη στον παραπάνω πίνακα της γραμμής $(a_{S+m+1}, \ldots, a_{S+2m+1})$ δεν αυξάνει την τάξη του πίνακα, άρα $a_{S+m+1}u_m + \ldots + a_{S+2m+1}u_0 = 0$.

Επαγωγικά, με τον ίδιο συλλογισμό, βλέπει κανείς ότι $a_{S+k}u_m + \ldots + a_{S+m+k}u_0 = 0$ γιά κάθε $k \geq 0$, απ'οπου προκύπτει ότι το $\Big(\sum_{i=0}^{m} u_i X^i\Big)\Big(\sum_{i=0}^{\infty} a_i X^i\Big)$ είναι ένα πολυώνυμο βαθμού μικρότερου από $S + m$.

Στην ενότητα 8 είδαμε ότι η $Z(H_f/\mathbb{F}_q; T)$ είναι πηλίκο δύο δυναμοσειρών στο $\Omega_p[[T]]$ με άπειρη ακτίνα σύγκλισης και σταθερό όρο μονάδα. Έστω λοιπόν

$Z(H_f/\mathbb{F}_q;T) \overset{\text{ορσ}}{=} Z(T) = \frac{A(T)}{B(T)}$ όπου $A(T), B(T)$ όπως προναφέρθηκαν. Από το Πόρισμα 4.1 σελ. 46 γιά την $B(T)$, έχουμε ότι υπάρχει δυναμοσειρά $G(T)$ με άπειρη ακτίνα σύγκλισης που δε μηδενίζεται στο Ω_p και πολυώνυμο $P(T)$ για τα οποία ισχύει η σχέση $P(T) = B(T)G(T)$, ή αλλιώς $B(T) = \frac{P(T)}{G(T)}$. Έχουμε συνεπώς ότι $Z(T) = \frac{A(T)G(T)}{P(T)}$, ή, θέτοντας $F(T) \overset{\text{ορσ}}{=} A(T)G(T)$, $Z(T) = \frac{F(T)}{P(T)}$, όπου η $F(T)$ συγκλίνει γιά κάθε $t \in \Omega_p$, καθώς οι $A(T), G(T)$ συγκλίνουν γιά κάθε $t \in \Omega_p$.
Αφού έχουμε σύγκλιση σε όλο το Ω_p, μπορούμε να θεωρήσουμε ότι έχουμε σύγκλιση σε ένα δίσκο $D(R)$ ακτίνας $R \overset{\text{ορσ}}{=} q^{2n}$.[78] Έχουμε λοιπόν ότι $F(T) = P(T)Z(T)$ και έστω ότι $F(T) = \displaystyle\sum_{i=0}^{\infty} b_i T^i \in 1 + T\Omega_p[[T]]$, $P(T) = \displaystyle\sum_{i=0}^{e} c_i T^i \in 1 + \Omega_p[T]$ και $Z(T) = \displaystyle\sum_{i=0}^{\infty} a_i T^i \in 1 + T\mathbb{Z}[[T]]$. Από το λήμμα 5.4, σελ. 53, έχουμε ότι $|a_i|_\infty \le q^{in}$. Καθώς η $F(T)$ συγκλίνει στον $D(R)$, έχουμε ότι $|b_i|_p R^i \overset{i\to\infty}{\longrightarrow} 0$, άρα μπορούμε να βρούμε i_0 τ.ώ. αν $i \ge i_0$, τότε $|b_i|_p R^i \le 1$, ή $|b_i|_p \le R^{-i} = q^{-2ni}$. Επιλέγουμε τώρα και σταθεροποιούμε $m > 2e$.

Έστω $A_{s,m} = \{a_{s+i+j}\}_{0\le i,j\le m}$ όπως στο τελευταίο λήμμα και $N_{s,m} = \det(\mathrm{A_{s,m}})$. Θα δείξουμε ότι γιά μεγάλο s, έχουμε $N_{s,m} = 0$. Αν αυτό δειχθεί, τότε από το τελευταίο λήμμα και επειδή $Z(T) \in 1 + \mathbb{Z}[[T]] \subseteq 1 + \mathbb{Q}[[T]]$, θα έχουμε ότι η $Z(T)$ είναι ένα πηλίκο δύο πολυωνύμων με συντελεστές στο $\mathbb{Q}$.
Εξισώνοντας τους συντελεστές στη σχέση $F(T) = P(T)Z(T)$, έχουμε ότι γιά κάθε $j \ge 0$, $b_{j+e} = a_{j+e} + c_1 a_{j+e-1} + c_2 a_{j+e-2} + \ldots + c_e a_j$.

Θεωρούμε τον πίνακα $A'_{s,m}$ ο οποίος εχει προκύψει από τον $A_{s,m}$ κατόπιν αντικατάστασης της $(j+e)$-οστής στήλης του από την $c_0(j+e)$-οστή $+c_1(j+e-1)$-οστή $+\ldots+c_e(j+e-e)$-οστή όπου $j = 1, \ldots, m+1-e$. Έχουμε λοιπόν ότι $N_{s,m} = \det(\mathrm{A'_{s,m}}) =$

$$\det\begin{pmatrix} a_s & \cdots & a_{s+e-1} & b_{s+e} & b_{s+e+1} & \cdots & b_{s+m} \\ a_{s+1} & \cdots & a_{s+e} & b_{s+e+1} & b_{s+e+2} & \cdots & b_{s+m+1} \\ a_{s+2} & \cdots & a_{s+e+1} & b_{s+e+2} & b_{s+e+3} & \cdots & b_{s+m+2} \\ \vdots & \vdots & \vdots & \vdots & \vdots & & \\ a_{s+m-2} & \cdots & a_{s+e-1+m-2} & b_{s+e+m-2} & b_{s+e+m-1} & \cdots & b_{s+2m-2} \\ a_{s+m-1} & \cdots & a_{s+e-1+m-1} & b_{s+e+m-1} & b_{s+e+m} & \cdots & b_{s+2m-1} \\ a_{s+m} & \cdots & a_{s+e-1+m} & b_{s+e+m} & b_{s+e+m+1} & \cdots & b_{s+2m} \end{pmatrix} \overset{\text{ορσ}}{=} N'_{s,m}.$$

[78] Όπου n είναι το πλήθος των μεταβλητών του f.

Προκύπτουν τώρα οι εξής εκτιμήσεις :

$$|N_{s,m}|_p = |N^{'}_{s,m}|_p \leq {}^{79} (\max_{s+e \leq j \leq s+2m} |b_j|_p)^{m+1-e} \leq {}^{80} (\max_{j \geq s+e} |b_j|_p)^{m+1-e} <$$

$$R^{-s(m+1-e)} < q^{-ns(m+2)}$$

όταν $s \geq i_0$, [81] καθώς $R = q^{2n}$ και $m > 2e$.
Παράλληλα, επειδή $|a_i|_\infty \leq q^{in}$, έχουμε ότι

$$|N_{s,m}|_\infty \leq (m+1)! q^{n(s+2m)(m+1)} = (m+1)! q^{2nm(m+1)} q^{ns(m+1)}.$$

Προκύπτει συνεπώς ότι

$$|N_{s,m}|_p |Ns,m|_\infty < q^{-ns(m+2)}(m+1)! q^{2nm(m+1)} q^{ns(m+1)} = \frac{(m+1)! q^{2nm(m+1)}}{q^{ns}}$$

άρα μπορούμε να βρούμε $s_0 > i_0$ τ.ώ. γιά κάθε $s \geq s_0$ να ισχύει

$$|N_{s,m}|_p |Ns,m|_\infty < 1.$$

Όμως $N_{s,m} \in \mathbb{Z}$ και καθώς $n \in \mathbb{Z}$ και $|n|_\infty |n|_p < 1 \Rightarrow n = 0$,[82] έπεται ότι $N_{s,m} = 0$ γιά κάθε $s \geq s_0$.

Ενδεικτική της σημασίας του θεωρήματος του Dwork, είναι η παρακάτω εφαρμογή :

Έστω H_S μία (αφφινική ή προβολική) πολλαπλότητα και $Z(H_f/\mathbb{F}_q;T) = \exp(\sum_{s=1}^{\infty} N_s \frac{T^s}{s})$ η συνάρτηση ζήτα αυτής. Ισχύει ότι πεπερασμένοι μιγαδικοί αριθμοί καθορίζουν την ακολουθία $\{N_s\}_{s \geq 1}$.
Πράγματι, από το θεώρημα του Dwork έχουμε ότι

$$Z(H_f/\mathbb{F}_q;T) = \exp(\sum_{s=1}^{\infty} N_s \frac{T^s}{s}) = \frac{f}{g}$$

γιά κάποια $f, g \in 1 + X\mathbb{Z}[X]$. Άρα,

[79] Γιά κάθε i έχουμε $a_i \in \mathbb{Z}$, άρα $|a_i|_p \leq 1$

[80] Έχουμε θέσει $R = q^{2n} \geq 1$, άρα από τη σύγκλιση της $F(t)$ για $t \in w$ με $|t|_p = 1$ έχουμε ότι $|b_j|_p \xrightarrow{j \to \infty} 0$. Έχει νόημα λοιπόν το $\max_{j \geq e} |b_j|_p$ και μάλιστα $\max_{s+e \leq j \leq s+2m} |b_j|_p \leq \max_{j \geq e} |b_j|_p$.

[81] Γιά $j \geq s+e > s \geq i_0$ έχουμε $|b_j|_p < R^{-j} < R^{-s}$, άρα $\max_{j \geq s+e} |b_j|_p < R^{-s}$.

[82] Αν $0 \neq |n|_\infty = p^\kappa l$ όπου $1 \leq l < p$, τότε $|n|_\infty \geq p^\kappa$ άρα $|n|_\infty |n|_p \geq 1$.

$$\exp(\sum_{s=1}^{\infty} N_s \frac{T^s}{s}) = \frac{\prod_{i=1}^{m}(1 - a_i T)}{\prod_{i=1}^{n}(1 - b_i T)},$$

όπου τα a_i $i = 1, \ldots, m$ και b_i $i = 1, \ldots, n$ είναι τα αντίστροφα των μιγαδικών ριζών των f και g αντίστοιχα. Λογαριθμώντας τα δυο μέλη της παραπάνω ισότητας, λόγω των σχέσεων 6, 7, σελ. 28, έχουμε ότι

$$\sum_{s=1}^{\infty} N_s \frac{T^s}{s} = \sum_{s=1}^{\infty} (-1)^{s+1} (-\sum_{i=1}^{m} a_i^s + \sum_{i=1}^{n} b_i^s) \frac{T^s}{s},$$

συνεπώς

$$N_s = \sum_{i=1}^{m} (-a_i)^s - \sum_{i=1}^{n} (-b_i)^s$$

γιά κάθε $s \geq 1$. Βλέπουμε λοιπόν ότι, γιά κάθε $s \geq 1$, το N_s καθορίζεται από τα $a_1, \ldots, a_m, b_1, \ldots, b_n$.

10 Παράρτημα.

10.

$$\frac{F(X^p,Y^p)}{F^p(X,Y)} = F(X^p,Y^p)(F^p(X,Y))^{-1} = {}^{83}$$

$$((1+Y^p)^{X^p}(1+Y^{p^2})^{\frac{X^{p^2}-X^p}{p}}(1+Y^{p^3})^{\frac{X^{p^3}-X^{p^2}}{p^2}}\cdot\ldots)\cdot$$
$$((1+Y)^{pX}(1+Y^p)^{X^p-X}(1+Y^{p^2})^{\frac{X^{p^2}-X^p}{p}}\cdot\ldots)^{-1} =$$

$$((1+Y^p)^{X^p}\prod_{n=2}^{\infty}(1+Y^{p^n})^{\frac{X^{p^n}-X^{p^{n-1}}}{p^{n-1}}})((1+Y)^{pX}\prod_{n=1}^{\infty}(1+Y^{p^n})^{\frac{X^{p^n}-X^{p^{n-1}}}{p^{n-1}}})^{-1} \quad (22)$$

Όμως,

$$((1+Y)^{pX}\prod_{n=1}^{\infty}(1+Y^{p^n})^{\frac{X^{p^n}-X^{p^{n-1}}}{p^{n-1}}})^{-1} =$$
$$((1+Y)^{pX})^{-1}\prod_{n=1}^{\infty}((1+Y^{p^n})^{\frac{X^{p^n}-X^{p^{n-1}}}{p^{n-1}}})^{-1}$$

διότι : έχουμε

$$|(1+Y)^{pX}\prod_{n=1}^{\kappa}(1+Y^{p^n})^{\frac{X^{p^n}-X^{p^{n-1}}}{p^{n-1}}} -$$
$$(1+Y)^{pX}\prod_{n=1}^{\infty}(1+Y^{p^n})^{\frac{X^{p^n}-X^{p^{n-1}}}{p^{n-1}}}|_{X,Y} \overset{\kappa\to\infty}{\longrightarrow} 0^{84}.$$

Ακόμα, γιά κάθε $\kappa \geq 1$, το $(1+Y)^{pX}\prod_{n=1}^{\kappa}(1+Y^{p^n})^{\frac{X^{p^n}-X^{p^{n-1}}}{p^{n-1}}}$ είναι αντιστρέψιμο στοιχείο του $\mathbb{Q}_p[[X,Y]]$ καθώς έχει σταθερό όρο μονάδα. Από το λήμμα 1.6 σελ. 10 λοιπόν, και το $(1+Y)^{pX}\prod_{n=1}^{\infty}(1+Y^{p^n})^{\frac{X^{p^n}-X^{p^{n-1}}}{p^{n-1}}}$ είναι αντιστρέψιμο στοιχείο

[83] Απο το λήμμα 1.5 σελ. 8και τη σχέση 12 σελ. 28

του $\mathbb{Q}_p[[X,Y]]$ και επιπλέον έχουμε

$$|((1+Y)^{pX}\prod_{n=1}^{\kappa}(1+Y^{p^n})^{\frac{X^{p^n}-X^{p^{n-1}}}{p^{n-1}}})^{-1}- \\ ((1+Y)^{pX}\prod_{n=1}^{\infty}(1+Y^{p^n})^{\frac{X^{p^n}-X^{p^{n-1}}}{p^{n-1}}})^{-1}|_{X,Y} \stackrel{\kappa\to\infty}{\longrightarrow} 0.$$

Όμως γιά κάθε $\kappa \geq 1$,

$$((1+Y)^{pX}\prod_{n=1}^{\kappa}(1+Y^{p^n})^{\frac{X^{p^n}-X^{p^{n-1}}}{p^{n-1}}})^{-1} = \\ ((1+Y)^{pX})^{-1}\prod_{n=1}^{\kappa}((1+Y^{p^n})^{\frac{X^{p^n}-X^{p^{n-1}}}{p^{n-1}}})^{-1}$$

και ακόμα

$$|((1+Y)^{pX})^{-1}\prod_{n=1}^{\kappa}((1+Y^{p^n})^{\frac{X^{p^n}-X^{p^{n-1}}}{p^{n-1}}})^{-1}- \\ ((1+Y)^{pX})^{-1}\prod_{n=1}^{\infty}((1+Y^{p^n})^{\frac{X^{p^n}-X^{p^{n-1}}}{p^{n-1}}})^{-1}|_{X,Y} \stackrel{\kappa\to\infty}{\longrightarrow} 0$$

διότι

$$\mathrm{ord}(((1+Y^{p^n})^{\frac{X^{p^n}-X^{p^{n-1}}}{p^{n-1}}})-1) = \mathrm{ord}(((1+Y^{p^n})^{\frac{X^{p^n}-X^{p^{n-1}}}{p^{n-1}}})^{-1}-1) \stackrel{n\to\infty}{\longrightarrow} \infty.$$

Συνεπώς $((1+Y)^{pX}\prod_{n=1}^{\infty}(1+Y^{p^n})^{\frac{X^{p^n}-X^{p^{n-1}}}{p^{n-1}}})^{-1} = ((1+Y)^{pX})^{-1}\prod_{n=1}^{\infty}((1+Y^{p^n})^{\frac{X^{p^n}-X^{p^{n-1}}}{p^{n-1}}})^{-1}$. Συνεχίζοντας λοιπόν την 22 σελ. 83, έχουμε ότι

$$(22) = ((1+Y^p)^{X^p}\prod_{n=2}^{\infty}(1+Y^{p^n})^{\frac{X^{p^n}-X^{p^{n-1}}}{p^{n-1}}}) \\ \times((1+Y)^{pX})^{-1}\prod_{n=1}^{\infty}((1+Y^{p^n})^{\frac{X^{p^n}-X^{p^{n-1}}}{p^{n-1}}})^{-1} =_{85} \frac{(1+Y^p)^X}{(1+Y)^{pX}}.$$

60. $\mathrm{G}\circ\mathrm{T}_q = \mathrm{T}_q\circ\mathrm{G}_q = \Psi_{q,G_q}$.

Απόδειξη : Έστω $u \in U$. Τότε

$$\mathrm{G}(T_q(X^u)) = \begin{cases} \mathrm{G}(X^{\frac{u}{q}}), & \text{αν } q|u \\ \mathrm{G}(0), & \text{αλλιώς} \end{cases} = \begin{cases} \sum_{w\in U} g_w X^{w+\frac{u}{q}}, & \text{αν } q|u \\ 0, & \text{αλλιώς} \end{cases}$$

$$\mathrm{T}_q(\mathrm{G}_q(X^u)) = \mathrm{T}_q(\sum_{w\in U} g_w X^{qw+u}) =$$

$$\sum_{w\in U} g_{qw} X^{qw+u} = \begin{cases} \sum_{w\in U} g_w X^{w+\frac{u}{q}}, & \text{αν } q|u \\ 0, & \text{αλλιώς} \end{cases}.$$

61. Γιά κάθε $n \in \mathbb{N}$ $(\mathrm{G}\cdot\mathrm{G}_q\cdot\ldots\cdot\mathrm{G}_{q^n})_q \circ \mathrm{G} = \mathrm{G}\cdot\mathrm{G}_q\cdot\ldots\cdot\mathrm{G}_{q^{n+1}}$.

Απόδειξη : Έστω $r \in R$ και $\kappa \in \mathbb{N}$. Τότε

$$((\mathrm{G}\cdot\mathrm{G}_q\cdot\ldots\cdot\mathrm{G}_{q^\kappa})_q \circ \mathrm{G})(r) = (\mathrm{G}\cdot\mathrm{G}_q\cdot\ldots\cdot\mathrm{G}_{q^\kappa})_q(\mathrm{G}r) \overset{86}{=}$$
$$(\mathrm{G}_q\cdot\mathrm{G}_{q^2}\cdot\ldots\cdot\mathrm{G}_{q^{\kappa+1}})(\mathrm{G}r) = \mathrm{G}\cdot\mathrm{G}_q\cdot\ldots\cdot\mathrm{G}_{q^{\kappa+1}}(r).$$

62. Έστω $\mathrm{G} = \sum_{w\in U} g_w X^w, r = \sum_{u\in U} a_u X^u \in R_0$. υπάρχουν λοιπόν $M, N > 0$ τ.ώ. $\mathrm{ord}(g_w) \geq M|w| \;\; \forall\, w \in U$ και $\mathrm{ord}(a_u) \geq N|u| \;\; \forall\, u \in U$. Έστω ακόμα $\mathrm{G}r = \sum_{v\in U} \beta_v X^v$ όπου $\beta_v = \sum_{\substack{w,u\in U \text{ με} \\ w_i+u_i=v_i \;\; \forall\, i=1,\ldots,n}} g_w a_u$. Θέτοντας $K = min\{M, N\}$, γιά κάθε $v \in U$ έχουμε : $\mathrm{ord}(\beta_v) = \mathrm{ord}\Big(\sum_{\substack{w,u\in U \text{ με} \\ w_i+u_i=v_i \;\; \forall\, i=1,\ldots,n}} g_w a_u\Big) \geq \max_{\substack{w,u\in U \text{ με} \\ w_i+u_i=v_i \;\; \forall\, i=1,\ldots,n}} \{\mathrm{ord}(g_w) + \mathrm{ord}(a_u)\} \geq K|w| + K|u| = K|v|$.

63. Έστω $\mathrm{G}(X) = \sum_{w\in U} g_w X^w \in R_0$. Άρα υπάρχει $M > 0$ τ.ώ. $\mathrm{ord}(g_w) \geq M|w| \;\; \forall\, w \in U$. Τότε $\mathrm{G}_q(X) = \sum_{w\in U} g_w X^{wq} = \sum_{w\in U} a_w X^w$ όπου

$$a_w = \begin{cases} 0, & \text{αν } q \not| w \\ g_{\frac{w}{q}}, & \text{αν } q|w. \end{cases}$$

Θέτοντας τώρα $K = \frac{M}{q}$, έχουμε :

$$\mathrm{ord}(a_w) = \begin{cases} \infty \geq K|w|, & \text{αν } q \not| w \\ \mathrm{ord}(g_{\frac{w}{q}}) \geq M|\frac{w}{q}| = K|w|, & \text{αν } q|w. \end{cases}$$

65. Γιά κάθε θετικούς ακέραιους n, α, ισχύει ότι :

$$\sum_{\zeta\in\Omega_p \text{ με } \zeta^n=1} \zeta^\alpha = \begin{cases} n, & \text{αν } n|\alpha \\ 0, & \text{αλλιώς} \end{cases} .$$

Απόδειξη : • Αν $n|\alpha$, δηλαδή $\alpha = n\kappa$, τότε θα έχουμε : $\displaystyle\sum_{\zeta\in\Omega_p \text{ με } \zeta^n=1} \zeta^\alpha = \sum_{\zeta\in\Omega_p \text{ με } \zeta^n=1} \zeta^{n\kappa} = \sum_{\zeta\in\Omega_p \text{ με } \zeta^n=1} 1 = n.$

• Αν $n \not| \alpha$, τότε

-Αν $n > \alpha$, τότε $n = \alpha\kappa+\lambda$ με $0 \le \lambda < \alpha$, άρα θέλουμε $\displaystyle\sum_{\zeta\in\Omega_p \text{ με } \zeta^n=1} \zeta^\alpha = 0$

-Αν $n < \alpha$, τότε $\alpha = n\kappa+\lambda$ με $0 < \lambda < \alpha$, άρα θέλουμε $\displaystyle\sum_{\zeta\in\Omega_p \text{ με } \zeta^n=1} \zeta^\alpha = \sum_{\zeta\in\Omega_p \text{ με } \zeta^n=1} \zeta^{n\kappa}\zeta^\lambda = \sum_{\zeta\in\Omega_p \text{ με } \zeta^n=1} \zeta^\lambda = 0$

Αρκεί λοιπόν να δείξουμε ότι αν α είναι θετικός ακέραιος με $\alpha < n$, τότε $\displaystyle\sum_{\zeta\in\Omega_p \text{ με } \zeta^n=1} \zeta^\alpha = 0$

Έστω $A \overset{\text{ορσ}}{=} \{\zeta_0^0 = 1, \zeta_0^1, \ldots, \zeta_0^{n-1}\}$ οι n-οστές ρίζες της μονάδας.

-Έστω $(\alpha, n) = 1$. Τότε, αν είχα $\zeta_i^\alpha = \zeta_j^\alpha$ γιά κάποια $\zeta_i, \zeta_j \in A$ και i, j με $i > j$, τότε, αν $\zeta_i = \zeta_0^i$ και $\zeta_j = \zeta_0^j$, θα είχα $\zeta_0^{\alpha(i-j)} = 1$ άρα $n|\alpha(i-j)$, και καθώς $(n, \alpha) = 1$ θα πρέπει $n|i-j$, άτοπο αφού $i, j \in \{0, 1, \ldots n-1\}$.

Στην περίπτωση λοιπόν αυτή, τα $\zeta_0^{0\alpha}, \zeta_0^{1\alpha}, \ldots, \zeta_0^{(n-1)\alpha}$ είναι μία αναδιάταξη των $\zeta_0^0, \zeta_0^1, \ldots, \zeta_0^{n-1}$, άρα $\displaystyle\sum_{\zeta\in\Omega_p \text{ με } \zeta^n=1} \zeta^\alpha = 0.$

-Έστω $(\alpha, n) > 1$. Τότε $\displaystyle\sum_{\zeta\in\Omega_p \text{ με } \zeta^n=1} \zeta^\alpha = 1 + \zeta_0^\alpha + \zeta_0^{2\alpha} + \ldots + \zeta_0^{(n-1)\alpha} = 1 + (\zeta_0^\alpha) + (\zeta_0^\alpha)^2 + \ldots + (\zeta_0^\alpha)^{n-1}.$

Έστω $\kappa = \operatorname{ord}(\zeta_0^\alpha)$ και $\{1, \zeta_0^\alpha, \ldots, \zeta_0^{\kappa\alpha}\}$ η ομάδα που παράγει η ζ_0^α. Αφου $\kappa|n$, έστω ότι δηλαδή $n = \kappa d$, θα έχουμε ότι

$$1 + (\zeta_0^\alpha) + (\zeta_0^\alpha)^2 + \ldots + (\zeta_0^\alpha)^{n-1} =$$

$$\underbrace{(1 + \zeta_0^\alpha + \ldots + \zeta_0^{\alpha(\kappa-1)}) + \ldots + (1 + \zeta_0^\alpha + \ldots + \zeta_0^{\alpha(\kappa-1)})}_{d} = 0,$$

αφού $1 + \zeta_0^\alpha + \ldots + \zeta_0^{\alpha(\kappa-1)} = 0.$

69. Ισχύει το εξής

Θεώρημα : Ένας πίνακας A είναι τριγωνίσιμος αν και μόνο αν το χαρακτηριστικό του πολυώνυμο είναι γινόμενο πρωτοβαθμίων παραγόντων.

Απόδειξη : Βλέπε Στυλ. Ανδρεαδάκη Γραμμική Άλγεβρα θεώρημα 6.5.1 σελ.209.

Άμεσο πόρισμα του παραπάνω θεωρήματος είναι ότι κάθε πίνακας με στοιχεία από ένα αλγεβρικά κλειστό σώμα είναι τριγωνίσιμος.

75. Έστω επέκταση $\mathbb{F}_q \ \mathbb{F}_p$ και $\varepsilon \in \Omega_p$ πρωταρχική p-οστή ρίζα του 1. Τότε ισχύει ότι $\displaystyle\sum_{x\in\mathbb{F}_q} \varepsilon^{\mathrm{Tr}_{\mathbb{F}_q \ \mathbb{F}_p} x} = 0$.

Απόδειξη : Αφού η επέκταση $\mathbb{F}_q\backslash\mathbb{F}_p$ είναι διαχωρίσιμη, έχουμε ότι η απεικόνιση $\mathrm{Tr}_{\mathbb{F}_q\backslash\mathbb{F}_p} : \mathbb{F}_q \longrightarrow \mathbb{F}_p$ είναι διάφορη της μηδενικής. Υπάρχει λοιπόν $x_0 \in \mathbb{F}_q$ με $\mathrm{Tr}_{\mathbb{F}_q \ \mathbb{F}_p} x_0 \neq 0$. Έχουμε λοιπόν : $\displaystyle\sum_{x\in\mathbb{F}_q} \varepsilon^{\mathrm{Tr}_{\mathbb{F}_q\backslash\mathbb{F}_p} x} = \sum_{x+x_0\in\mathbb{F}_q} \varepsilon^{\mathrm{Tr}_{\mathbb{F}_q\backslash\mathbb{F}_p}(x+x_0)} = \varepsilon^{\mathrm{Tr}_{\mathbb{F}_q\backslash\mathbb{F}_p} x_0} \sum_{x\in\mathbb{F}_q} \varepsilon^{\mathrm{Tr}_{\mathbb{F}_q\backslash\mathbb{F}_p} x}$. Θέτοντας $\Sigma = \displaystyle\sum_{x\in\mathbb{F}_q} \varepsilon^{\mathrm{Tr}_{\mathbb{F}_q\backslash\mathbb{F}_p} x}$, έχουμε ότι $\Sigma = \varepsilon^{\mathrm{Tr}_{\mathbb{F}_q\backslash\mathbb{F}_p}(x_0)}\Sigma$ και επειδή $\varepsilon^{\mathrm{Tr}_{\mathbb{F}_q\backslash\mathbb{F}_p}(x_0)} \neq 1$, έχουμε ότι $\Sigma = 0$.

77. Έστω $X^w = X_1^{w_1} \cdots X_n^{w_n}$ και $b \in D(1)$. Τότε $\Theta(bX^w) \in R_0$.

Απόδειξη : Αφού $\Theta(\mathrm{T}) = \displaystyle\sum_{\kappa=1}^{\infty} a_\kappa \mathrm{T}^\kappa$, [87] θα έχουμε ότι $\Theta(bX^w) = \displaystyle\sum_{\kappa=0}^{\infty} a_\kappa b^\kappa X^{w\kappa} = \sum_{u\in U} s_u X^u$, όπου

$$s_u = \begin{cases} 0, & \text{αν } u \neq \lambda w \text{ γιά } \quad \text{κάθε } \lambda \in \mathbb{N}_0 \\ a_\kappa b^\kappa, & \text{αν } u = \kappa w \text{ γιά } \quad \text{κάποιο } \kappa \in \mathbb{N}_0 \ . \end{cases}$$

Θέτοντας τώρα $M = \frac{1}{(p-1)|w|}$, έχουμε :

$$\mathrm{ord}(s_u) = \begin{cases} \infty > \frac{1}{(p-1)|w|}|u| = M|u| & \text{αν } u \neq \lambda w \text{ γιά } \quad \text{κάθε } \lambda \in \mathbb{N}_0 \\ \mathrm{ord}(a_\kappa) + \kappa \mathrm{ord} b \geq^{88} \frac{\kappa}{(p-1)|w|}|w| = M|u|, & \text{αν } u = \kappa w \text{ γιά } \quad \text{κάποιο } \kappa \in \mathbb{N}_0 \ . \end{cases}$$

[87] Βλ. σελίδα 59

Αναφορές

[Ko] N. Koblitz, *p-adic Numbers, p-adic Analysis, and Zeta Functions*, Springer Graduate Text in Mathematics 58, 1977

[Gou] Fernando Q. Gouvêa, *p-adic Numbers*, Springer-Verlag, 1993

[BS] Z. I. Borevich, I. R. Shafarevich *Number Theory*, Academic Press, 1966

[Ca] J. W. S. Cassels *Local Fields*, Cambridge University Press, 1986

[Ro] A. M. Robert *A Course in p-adic Analysis*, Springer Graduate Text in Mathematics 198, 2000