Η Υποθεση του Riemann

Πτυχιακη Εργασια

Νικολεντζος Πολυχρονης
Α.Μ.: 311/2003066

Εισηγητης: Κοντογεωργης Αριστειδης

Τμημα Μαθηματικων
Πανεπιστημιο Αιγαιου
Καρλοβασι, 2008

Εξεταστικη Επιτροπη:

Ανούσης Μιχαήλ

Κοντογεώργης Αριστείδης

Φελουζής Ευάγγελος

Πρόλογος

Στην πτυχιακή αυτή εργασία θα ασχοληθούμε με ένα από τα σπουδαίοτερα προβλήματα της Θεωρίας Αριθμών την υπόθεση του Riemann για τη ζ - συνάρτηση.

Αρχικά θα ορίσουμε τη ζ - συνάρτηση σαν μια σειρά Dirichlet και θα δούμε τα χωρία σύγκλισής της. Η ζ - συνάρτηση συγκλίνει στο ημιεπίπεδο του μιγαδικού επιπέδου που ορίζεται από την $\mathrm{Re(z)} \geq 1$. Η συναρτησιακή εξίσωση μας δίνει την δυνατότητα να ορίσουμε την ζ-συνάρτηση ως μια μερόμορφη συνάρτηση σε όλο το μιγαδικό επίπεδο εκτός από τον πόλο στο $s = 1$. Περιγράφουμε τα αναλυτικά εργαλεία που χρειαζόμαστε για να σκιαγραφήσουμε την αποδείξη της συναρτησιακής της εξίσωσης. Από την συναρτησιακή εξίσωση υπολογίζουμε τις τετριμμένες ρίζες της ζ - συνάρτησης και διατυπώνουμε την υπόθεση του Riemann για τις μη τετριμμένες ρίζες της. Η απόδειξη της υπόθεσης Riemann είναι ένα ανοιχτό πρόβλημα, από τα σημαντικότερα για την θεωρία αριθμών και τα μαθηματικά γενικότερα.

Θα μπορούσε να πει κανείς ότι διαισθητικά η ζ-συνάρτηση περιγράφει την κατανομή των πρώτων του δακτυλίου των ακεραίων $\mathbb{Z}$ του σώματος των ρητών αριθμών. Υπάρχουν γόνιμες γενικεύσεις της ζ-συνάρτησης για αλγεβρικά σώματα αριθμών και πολλές ιδιότητες ενός σώματος αριθμών αποτυπώνονται στην ζήτα συνάρτηση του.

Από την άλλη μεριά τα σώματα $\mathbb{Q}$ και $\mathbb{F}_p(t)$ παρουσιάζουν πολλές ομοιότητες. Οι δακτύλιοι των ακεραίων τους $\mathbb{Z}$, $\mathbb{F}_p[t]$ είναι για παράδειγμα και οι δύο μονοδιάστατοι δακτύλιοι του Dedekind. Οι αλγεβρικές επεκτάσεις του σώματος $\mathbb{F}_p(t)$ αντιστοιχούν σε σώματα συναρτήσεων αλγεβρικών καμπυλών και τα ονομάζουμε *αλγεβρικά σώματα συναρτήσεων μίας μεταβλητής. Η θέαση των σωμάτων αυτών ως σώματα συναρτήσεων καμπυλών προσθέτει στο οπλοστάσιο μας ένα πλήθος γεωμετρικών εργαλείων.*

Στην πτυχιακή αυτή εργασία προσπαθούμε να δόσουμε μία γενίκευση της ζ-συνάρτησης. Οδηγούμαστε και πάλι σε μία μερόμορφη συνάρτηση στο μιγαδικό επίπεδο, η οποία περιέχει όλη την πληροφορία για το πλήθος των σημείων της αντίστοιχης καμπύλης πάνω από κάθε επέκταση $\mathbb{F}_{p^r}$ του $\mathbb{F}_p$. Το ενδιαφέρον σχετικά με την ζ-συνάρτηση ενός σώματος συναρτήσεων είναι ότι αθροίζεται σε μία ρήτη συνάρτηση στο $\mathbb{C}(t)$. Τοπολογικές και γεωμετρικές ιδιότητες της ζ-συνάρητησης όπως για παράδειγμα το γένος της καμπύλης εμφανίζονται στην ρητή γραφή της ζ-συνάρτησης. Το κυριότερο όμως χαρακτηριστικό της ζ-συνάρτησης είναι ότι οι ρίζες της ικανοποιούν την υπόθεση Riemann.

Πρώτος ο A. Weil παρατήρησε ότι τα σημεία μίας καμπύλης πάνω από το $\mathbb{F}_{p^r}$ είναι τα σταθερά σημεία του ομομορφισμού του Frobenious $x \mapsto x^{p^r}$ και επιρεασμένος από τα θεωρήματα σταθερού σημείου της αλγεβρικής τοπολογίας κατάφερε να δώσει μία «απόδειξη», υπό την προϋπόθεση ότι μία «κατάλληλη» συνομολογιακή θεωρία για αλγεβρικές καμπύλες υπήρχε. Την θεωρία αυτή την κατασκεύασε ο A. Grothendick και η χρήση αυτής της θεωρίας οδήγησε τον P. Deligne στην απόδειξη της εικασίας του Riemann για τις ζ-συναρτήσεις αλγεβρικών πολλαπλοτήτων.

Εμείς θα περιοριστούμε σε αλγεβρικές καμπύλες και στα σώματα συναρτήσεων τους και θα παρουσιάσουμε μία βατή απόδειξη της εικασίας του Riemann η οποία οφείλεται στον Bombieri.

Αφού ορίσουμε τα εργαλεία και τις έννοιες που θα χρειαστούμε όπως του αλγεβρικού σώματος συναρτήσεων, των θέσεων και των διαιρετών και την σύνδεσή τους με την γεωμετρία θα ορίσουμε την ζ-συνάρτηση ενός αλγεβρικού σώματος συναρτήσεων και θα υπολογίσουμε την ρητή έκφραση με την βοήθεια του θεωρήματος των Riemann-Roch. Τέλος θα περιγράψουμε την απόδειξη της εικασίας του Riemann και το φράγμα των Hasse-Weil

Περιεχόμενα

ΚΕΦΑΛΑΙΟ 1

Οι συναρτήσεις Γάμμα και Ζήτα και οι L-σειρές

1.1 Εισαγωγή

Στο κεφάλαιο αυτό σκοπός μας είναι να μελετήσουμε τη ζήτα συνάρτηση του ***Riemann*** *ως μια σειρά* ***Dirichlet*** *και να μελετήσουμε την* ***συναρτησιακή της εξίσωση****.*

Το 1737 *ο* ***Euler*** *έδωσε μια εναλλακτική απόδειξη του θεωρήματος του* ***Ευκλείδη*** *για την ύπαρξη άπειρων πρώτων αριθμών, αποδεικνύοντας ότι η σειρά* $\sum_{p\in\mathbb{P}} p^{-1}$ *αποκλίνει, δηλαδή,*

$$\sum_{p\in\mathbb{P}} p^{-1} = \infty$$

$\mathbb{P}$ *το σύνολο των πρώτων αριθμών*

Αυτό το συμπέρανε από το γεγονός ότι η συνάρτηση

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \overset{\mathbb{R}\ni s>1}{=} \infty, \text{ όταν } s \to 1.$$

(Την απόδειξη ότι η απειρία των πρώτων αριθμών σχετίζεται με την απόκλιση της ζ *- συνάρτησης του Euer θα την αποδείξουμε στο τέλος αυτής της ενότητας.)*

Ο ***Riemann****, μελετώντας την* ζ *- συνάρτηση του Euler, θεώρησε την μεταβλητή* s *να είναι ένας μιγαδικός αριθμός της μορφής* $s = \sigma + it$*, όπου* σ *και* t *είναι πραγματικοί αριθμοί. Την σπουδαιότητα αυτής της θεώρησης θα την δούμε παρακάτω.*

1.2 Σειρές Dirichlet

Πριν αρχίσουμε να μιλάμε για τις σειρές Dirichlet θα πούμε δυο λόγια για τη σύγκλιση σειρών και γινομένων.

Ορισμός 1.1 (Σύγκλιση σειρών) *Έστω* $\{a_n\}_{n=1}^{\infty},\ n \in \mathbb{N}$ *μία ακολουθία πραγματικών αριθμών. Θα λέμε ότι η σειρά* $\sum_{n=1}^{\infty} a_n$ ***συγκλίνει*** *στον πραγματικό αριθμό* ℓ *και θα γράφουμε* $\sum_{n=1}^{\infty} a_n = \ell$*, αν και μόνον αν η ακολουθία των μερικών αθροισμάτων* $\sigma_n = a_1 + a_2 + \cdots + a_n,\ n \in \mathbb{N}$ *συγκλίνει στο* ℓ *δηλαδή* $\lim_{n\to\infty} \sigma_n = \ell$*.*

Σημείωση 1.2 *Από τον προηγούμενο ορισμό αν* $\ell = +\infty$ *θα λέμε ότι η σειρά* $\sum_{n=1}^{\infty} a_n$ ***απειρίζεται θετικά****, ενώ αν* $\ell = -\infty$ *θα λέμε ότι η σειρά* $\sum_{n=1}^{\infty} a_n$ ***απειρίζεται αρνητικά****. Γενικά αν η σειρά απειρίζεται είτε θετικά είτε αρνητικά θα λέμε ότι σειρά* ***αποκλίνει****.*

Ορισμός 1.3 (Απόλυτη σύγκλιση σειρών) *Θα λέμε ότι η σειρά* $\sum_{n=1}^{\infty} a_n$ ***συγκλίνει απόλυτα*** *αν και μόνον αν η σειρά* $\sum_{n=1}^{\infty} |a_n|$ ***συγκλίνει****.*

Σημείωση 1.4 *Η απόλυτη σύγκλιση μιας σειράς συνεπάγεται την απλή σύγκλιση της, δηλαδή*

$$\sum_{n=1}^{\infty} |a_n| < +\infty \Rightarrow \sum_{n=1}^{\infty} a_n < +\infty.$$

Ορισμός 1.5 (Σύγκλιση άπειρου γινομένου) *Έστω* $\{z_n\}_{n=1}^{\infty}$ *μία ακολουθία μη μηδενικών μιγαδικών αριθμών. Θα λέμε ότι το άπερο γινόμενο* $\prod_{n=1}^{\infty} z_n$ *συγκλίνει σ' ένα μη μηδενικό αριθμό* ℓ*, αν η ακολουθία των μερικών γινομένων* $P_N = z_1 \cdot z_2 \cdots z_N$ *συγκλίνει στο* ℓ *δηλαδή* $\lim_{N\to\infty} P_N = \ell$*.*

Σημείωση 1.6 *Από τον προηγούμενο ορισμό αν* $\ell = 0$ *τότε λέμε ότι το άπειρο γινόμενο αποκλίνει στο* 0*.*

Θεώρημα 1.7 (Dirichlet) *Αν* $k > 0$ *και* $(h, k) = 1$ *τότε υπάρχουν άπειροι πρώτοι στην αριθμητική πρόοδο* $nk + h,\ n = 0, 1, 2, 3, \ldots$*.*

Η απόδειξη αυτού του θεωρήματος (παραπέμπουμε στο βιβλίο [TOMA]) βασίζεται στις L - σειρές Dirichlet, που θα μιλήσουμε γι' αυτές λίγο παρακάτω.

Ορισμός 1.8 (Χαρακτήρας Dirichlet) *Έστω* $k \in \mathbb{N} \setminus \{0\}$ *και η πεπερασμένη ομάδα* $\mathbb{Z}_k^* = \{n \pmod k : \mu\kappa\delta\,(n, k) = 1\}$*. Κάθε ομομορφισμός ομάδων*

$$\chi : \mathbb{Z}_k^* \longrightarrow \mathbb{C}^*$$

θα λέγεται χαρακτήρας Dirichlet $\bmod k$*.*

Σχόλιο 1.9 *Από τον προηγούμενο ορισμό έχουμε ότι ο χ ορίζεται μόνο στα n για τα οποία μκδ$(n,k)=1$. Επεκτείνουμε λοιπόν τον ορισμό ως εξής*

$$\chi(n)=\begin{cases} n \pmod k, & \text{αν μκδ}(n,k)=1 \\ 0, & \text{αν μκδ}(n,k)>1 \end{cases}$$

και θα τον ονομάζπυμε και πάλι χαρακτήρα Dirichlet.

Ώστε χαρακτήρας Dirichlet να είναι μία συνάρτηση $\chi:\mathbb{Z}\to\mathbb{C}$ με τις ακόλουθες ιδιότητες:

i. *Υπάρχει θετικός ακέραιος k τέτοιος ώστε $\chi(n)=\chi(n+k)$ για όλους τους ακεραίους n.*

ii. *$\chi(n)=0$ για κάθε n με μκδ$(n,k)>1$.*

iii. *$\chi(mn)=\chi(m)\chi(n)$ για όλους τους ακεραίους m και n.*

iv. *$\chi(1)=1$.*

Ορισμός 1.10 *Μια **σειρά Dirichlet** είναι μία σειρά της μορφής*

$$\sum_{n=1}^{\infty} z_n e^{-\lambda_n s}$$

όπου $\{\lambda_n\}$ είναι ακολουθία πραγματικών αριθμών με $\lambda_1<\lambda_2<\cdots<\lambda_n\to\infty$, z_n αυθαίρετοι μιγαδικοί αριθμοί και $s=\sigma+it\in\mathbb{C}$

Παράδειγμα 1.11 *Έστω $\lambda_n=\log n$ η σείρα Dirichlet γράφεται ως*

$$\sum_{n=1}^{\infty}\frac{z_n}{n^s}\overset{z_n=f(n)}{=}\sum_{n=1}^{\infty}\frac{f(n)}{n^s}$$

όπου $f(n)$, αριθμητική συνάρτηση.
*Τη σειρά αυτή θα τη λέμε **συνήθη σειρά Dirichlet**.*

Ορισμός 1.12 *Έστω $k\in\mathbb{N}$ και χ είναι ένας χαρακτήρας Dirichlet $\bmod k$. Η L-σειρά Dirichlet ορίζεται ως εξής:*

$$L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}$$

Αφού $|\chi(n)|=1$ για κάθε φυσικό αριθμό n, έπεται ότι $\left|\frac{\chi(n)}{n^s}\right|\le\frac{1}{n^\sigma}$, άρα η $L(s/x)$ συγκλίνει απόλυτα για $\sigma>1$.

Θεώρημα 1.13 *Έστω ότι η σειρά $\sum_{n=1}^{\infty}|f(n)n^{-s}|$ δεν συγκλίνει για όλα τα s ούτε αποκλίνει για όλα τα s. Τότε υπάρχει ένας πραγματικός αριθμός σ_a, που λέγεται τετμημένη απόλυτης σύγκλισης, τέτοιος ώστε η σιερά $\sum_{n=1}^{\infty}f(n)n^{-s}$ να συγκλίνει απόλυτα για $\sigma>\sigma_a$, ενώ για $\sigma<\sigma_a$ η σειρά να μην συγκλίνει απόλυτα.*

Απόδειξη: *Έστω D το σύνολο των πραγματικών σ, για τους οποίους η σειρά*

$$\sum_{n=1}^{\infty} |f(n)n^{-s}|$$

αποκλίνει. Το $D \neq \emptyset$, διότι η σειρά δε συγκλίνει για όλους τους s, ενώ το D είναι άνω φραγμένο, διότι η σειρά δεν αποκλίνει για όλα τα s. Επομένως το D έχει ένα ελάχιστο άνω φράγμα, που το ονομάζουμε σ_a. Αν $\sigma < \sigma_a$, τότε $\sigma \in D$, διότι διαφορετικά, το σ θα ήταν άνω φράγμα για το D, μικρότερο από το ελάχιστο άνω φράγμα. Αν $\sigma > \sigma_a$, τότε $\sigma \notin D$, διότι το σ_a είναι άνω φράγμα για το D. □

Παράδειγμα 1.14 Η συνάρτηση ζήτα του Riemann.
Η σειρά Dirichlet $\sum_{n=1}^{\infty} n^{-s}$ συγκλίνει απόλυτα για $\sigma > 1$. Όταν $s = 1$, η σειρά αποκλίνει, οπότε $\sigma_a = 1$. Το άθροισμα αυτής της σειράς συμβολίζεται με $\zeta(s)$ και λέγεται συνάρτηση ζήτα του Riemann.

Σημείωση 1.15 *Αρχικά η συνάρτηση ζήτα του Riemann ορίζεται για $\sigma > 1$, κάνοντας χρήση της συναρτησιακής εξίσωσης, που θα μελετήσουμε παρακάτω, θα την ορίσουμε σε όλο το $\mathbb{C} \setminus \{1\}$.*

Στη συνέχεια θα ορίσουμε την έννοια της ***πολλαπλασιαστικής συνάρτησης*** *και αποδείξουμε το θεώρημα που συνδέει μια άπειρη, συγκλίνουσα απόλυτα σειρά με το γινόμενο Euler. Αρχικά ας δούμε πως η σύγκλιση μιας μιγαδικής σειράς συνδέεται με τη σύγκλιση ενός* ***άπειρου γινομένου μιγαδικών όρων****.*

Πρόταση 1.16 *Αν $z_n \neq -1$, $n = 1, 2, \ldots$, το $\prod_{n=1}^{\infty}(1 + z_n)$ συγκλίνει* ***αν και μόνον αν*** *η σειρά $\sum_{n=1}^{\infty} \log(1 + z_n)$ συγκλίνει (με $\log z$ συμβολίζουμε τον κύριο κλάδο του αλγορίθμου, δηλαδή $-\pi < \operatorname{Im} \log z = \arg z \leq \pi$).*

Απόδειξη: *Θέτουμε $S_K = \sum_{n=1}^{K} \log(1 + z_n)$. Τότε $P_K = e^{S_K}$ και , αν $S_K \to S$, έχουμε $P_K \to P = e^S$. Αντίστροφα, ας υποθέσουμε ότι $P_K \to P \neq 0$. Τότε κάποιος κλάδος του λογαρίθμου (τον οποίο θα συμβολίζουμε με $\log^*$) είναι συνεχής στο P και $\log^* P_K \to \log^* P$ όταν $K \to \infty$. Ορίζουμε επαγωγικά ακεραίους b_n έτσι ώστε*

$$\sum_{n=1}^{K} \big(\log(1 + z_n) + 2\pi b_n \big) = \log^* P_K.$$

Αφού η $\log^* P_K$ συγκλίνει, η σειρά

$$\sum_{n=1}^{K} \big(\log(1 + z_n) + 2\pi i b_n \big)$$

συγκλίνει. Επομένως, $\log(1 + z_n) + 2\pi i b_n \to 0$ όταν $n \to \infty$. Αφού $z_n \to 0$ και $\log$ είναι ένας κύριος κλάδος του λογαρίθμου, έπεται ότι $b_n = 0$, αν το n είναι αρκετά μεγάλο. Συνεπώς, η σειρά $\sum_{n=1}^{\infty} \log(1 + z_n)$ συγκλίνει. □

Πρόταση 1.17 *Αν η σειρά $\sum_{n=1}^{\infty}|z_n|$ συγκλίνει, τότε το $\prod_{n=1}^{\infty}(1+z_n)$ συγκλίνει απόλυτα.*

Απόδειξη: *Υποθέτουμε ότι η $\sum_{n=1}^{\infty}|z_n|$ συγκλίνει σ' έναν αριθμό K, τέτοιον ώστε για $n>K$ να ισχύει $|z_n|<\frac{1}{2}$. Τότε, αν $n>K$,*

$$|\log(1+z_n)| = \left|z_n - \frac{{z_n}^2}{2} + \frac{{z_n}^3}{3} - \cdots\right| \leq |z_n|\left(1+\frac{1}{2}+\frac{1}{4}+\cdots\right) \leq 2\,|z_n|\,.$$

Επομένως, η σειρά $\sum_{n=K+1}^{\infty}\log(1+z_n)$ συγκλίνει και, από την προηγούμενη πρόταση, συγκλίνει και το απειρογινόμενο $\prod_{n=1}^{\infty}(1+z_n)$. □

Ορισμός 1.18 *Λέμε ότι το άπειρο γινόμενο*

$$\prod_{n=1}^{\infty}(1+z_n)$$

συγκλίνει απόλυτα, αν το άπειρο γινόμενο

$$\prod_{n=1}^{\infty}(1+|z_n|)$$

συγκλίνει.

Ορισμός 1.19 *Η συνάρτηση $f:\mathbb{N}\to\mathbb{C}$ θα λέγεται* ***πολλαπλασιαστική*** *συνάρτηση όταν*

$$f(mn)=f(m)f(n)$$

για όλους τους $m,n\in\mathbb{N}$ με $(m,n)=1$ και υπάρχει τουλάχιστον ένας $n_0\in\mathbb{N}$ τέτοιος ώστε $f(n_0)\neq 0$. Επιπλέον θα λέγεται ***πλήρως πολλαπλασιαστική*** *συνάρτηση όταν απαλείψουμε τον περιορισμό $(m,n)=1$.*

Παράδειγμα 1.20 *Ο χαρακτήρας Dirichlet είναι μία πλήρως πολλαπλασιαστική συνάρτηση.*

Θεώρημα 1.21 (Γινόμενο Euler) *Αν f* ***πολλαπλασιατική*** *και $\sum_{n=1}^{\infty}f(n)$* ***απολύτως συγκλίνουσα*** *τότε*

$$\sum_{n=1}^{\infty}f(n)=\prod_{p\in\mathbb{P}}\left\{1+f(p)+f(p^2)+\cdots\right\}$$

και το απειρογινόμενο συγκλίνει απολύτως. Αν f ***πλήρως πολλαπλασιαστική*** *τότε*

$$\sum_{n=1}^{\infty}f(n)=\prod_{p\in\mathbb{P}}\frac{1}{1-f(p)}.$$

Απόδειξη: *Αρχικά ορίζουμε*

$$P(x) := \prod_{p \leq x} \{1 + f(p) + f(p^2) + \cdots\}$$

Το $P(x)$ είναι πεπερασμένο γινόμενο απόλυτα συγκλινουσών σειρών, συνεπώς μπορούμε να πολλαπλασιάσουμε ή να αλλάξουμε τη σειρά των όρων, χωρίς να αλλάξει το άθροισμα. Θα έχουμε δηλαδή γινόμενα της μορφής

$$f(p_1^{a_1}) f(p_2^{a_2}) \cdots f(p_n^{a_n}) = f(p_1^{a_1} p_1^{a_1} \cdots p_n^{a_1})$$

Από το θεμελιώδες θεώρημα της αριθμητικής:

> *Κάθε φυσικός αριθμός $n > 1$ αναπαρίσταται σε γινόμενο πρώτων αριθμών. Η αναπαράσταση αυτή είναι μοναδική αν αγνοήσουμε τη διάταξη των παραγόντων του γινομένου.*

έχουμε ότι:

$$P(x) = \sum_{n \in A} f(n)$$

όπου $A = \{n \in \mathbb{N} \mid$ οι πρώτοι παράγοντες του n είναι όλοι $\leq x\}$. Επομένως

$$\sum_{n=1}^{\infty} f(n) - P(x) = \sum_{n \in B} f(n)$$

όπου $B = \{n \in \mathbb{N} \mid \exists p \in \mathbb{P},\ p|n,$ τέτοιος ώστε $p > x\}$. Άρα

$$\left| \sum_{n=1}^{\infty} f(n) - P(x) \right| \leq \sum_{n=1}^{\infty} |f(n)| \leq \sum_{n > x} |f(n)|$$

Τώρα αφού $\sum_{n=1}^{\infty} |f(x)|$ συγκλίνει, έπεται ότι για $x \to \infty$ το $\sum_{n>x}^{\infty} |f(x)| \to 0$. Επίσης από την πρόταση 1.17 γνωρίζουμε ότι:

$$\prod (1 + z_n) \text{ συγκλίνει απόλυτα } \iff \sum |z_n| \text{ συγκλίνει.}$$

Επίσης έχουμε ότι

$$\sum_{p \leq x} |f(p) + f(p^2) + \cdots| \leq \sum_{p \leq x} \left(|f(p)| + |f(p^2)| + \cdots \right) \leq \sum_{n=2}^{\infty} |f(n)|.$$

Αφού όλα τα μερικά αθροίσματα είναι πεπερασμένα, η σειρά θετικών όρων

$$\sum_{p \in \mathbb{P}} |f(p) + f(p^2) + \cdots|$$

συγκλίνει*, οπότε και το αντίστοιχο άπειρο γινόμενο συγκλίνει απόλυτα. Τώρα αν η f είναι πλήρως πολλαπλασιαστική τότε $f(p^n) = f(p)^n$ για κάθε πρώτο p και έχουμε συγκλίνουσες γεωμετρικές σειρές με αθροίσμα $\frac{1}{1-f(p)}$.*
Άρα αποδείξαμε ότι

$$\sum_{n=1}^{\infty} f(n) = \prod_{p \in \mathbb{P}} \frac{1}{1 - f(p)}.$$

□

Παράδειγμα 1.22 *Η* ***σειρά Dirichlet*** *μπορεί να εκφραστεί σαν* ***γινόμενο Euler***

$$\sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_{p\in\mathbb{P}} \frac{1}{1-f(p)p^{-s}};$$

Απόδειξη: *Από προηγούμενο θεώρημα η σειρά Dirichlet* ***συγκλίνει απόλυτα*** *για* $\sigma > \sigma_a \in \mathbb{R}$.
Θέτω $g(n) = \frac{f(n)}{n^s}$, *η οποία είναι μια πολλαπλασιαστική συνάρτηση διότι* f ***πολλαπλασιαστική*** $\Rightarrow$ $g(mn) = \frac{f(mn)}{(mn)^s} = \frac{f(m)}{m^s}\frac{f(n)}{n^s} = g(m)g(n)$ *για όλους τους* $m, n \in \mathbb{N}$ *με* $(m,n) = 1$ *και υπάρχει τουλάχιστον ένας* $n_0 \in \mathbb{N}$ *τέτοιος ώστε* $g(n_0) \neq 0$. *Επομένως έχουμε από το προηγούμενο θεώρημα για την* $g(n)$ *ότι*

$$\begin{aligned} \sum_{n=1}^{\infty} g(n) &= \prod_{p\in\mathbb{P}} \left\{1 + g(p) + g(p^2) + \cdots\right\} \Rightarrow \\ \sum_{n=1}^{\infty} \frac{f(n)}{n^s} &= \prod_{p\in\mathbb{P}} \left\{1 + \frac{f(p)}{p^s} + \frac{f(p^2)}{p^{2s}} + \cdots\right\} \end{aligned}$$

Αν f ***πλήρως πολλαπλασιαστική*** *συνάρτηση* $\Rightarrow$ g ***πλήρως πολλαπλασιαστική*** *συνάρτηση. Επομένως από το προηγούμενο θεώρημα για τη* $g(n)$ *έχουμε*

$$\sum_{n=1}^{\infty} g(n) = \prod_{p\in\mathbb{P}} \frac{1}{1-g(p)} \Rightarrow \sum_{n=1}^{\infty} \frac{f(n)}{n^s} = \prod_{p\in\mathbb{P}} \frac{1}{1-f(p)p^{-s}}$$

□

Παράδειγμα 1.23 *Η* $\zeta(s)$ *συνάρτηση του* ***Riemann*** *μπορεί να εκφραστεί σαν* ***γινόμενο Euler***

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p\in\mathbb{P}} \frac{1}{1-p^{-s}}$$

Απόδειξη: *Από προηγούμενο παράδειγμα η* $\zeta(s)$ ***συγκλίνει απόλυτα*** *για* $\sigma > 1$.
Θέτω $g(n) = \frac{1}{n^s}$, *η οποία είναι* ***πολλαπλασιαστική*** *και* ***πλήρως πολλαπλασιαστική*** *(προφανές).*

Επομένως

$$\sum_{n=1}^{\infty} g(n) = \prod_{p\in\mathbb{P}} \frac{1}{1-g(p)} \Rightarrow \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p\in\mathbb{P}} \frac{1}{1-p^{-s}}.$$

□

Τώρα, μπορούμε να απόδειξουμε την απειρία των πρώτων αριθμών.

Απόδειξη: *Γνωρίζουμε ότι η σειρά* $\sum_{n=1}^{\infty} \frac{1}{n}$ *αποκλίνει και συγκεκριμένα απειρίζεται θετικά. Άρα από το θεώρημα 1.21 προκύπτει ότι για* $f(n) = \frac{1}{n}$ *έχουμε:*

$$\sum_{n=1}^{\infty} \frac{1}{n} = \prod_{p\in\mathbb{P}} \frac{1}{1-p^{-1}}$$

αφού το άθροισμα απειρίζεται θετικά και το άπειρο γινόμενο θα απειρίζεται, επομένως $\prod_{p\in\mathbb{P}}\left(1-\frac{1}{p}\right)$ *θα αποκλίνει στο 0, δηλαδή η κολουθία των μερικών γινομένων θα συγκλίνει στο 0, αλλά από την πρόταση 1.17 αφού το γινόμενο* $\prod_{p\in\mathbb{P}}\left(1-\frac{1}{p}\right)$ *αποκλίνει στο 0 άρα και η σειρά* $\sum_{p\in\mathbb{P}}\left|\frac{1}{p}\right|$ *αποκλίνει. Τελικά*

$$\sum_{p\in\mathbb{P}}\frac{1}{p}=+\infty.$$

□

1.3 Η Γάμμα συνάρτηση του Euler

Για το υπόλοιπο του κεφαλαίου θα χρειαστούμε κάποιες από τις ιδιότητες της Γ-συνάρτησης, έτσι στην ενότητα αυτή θα τις παραθέσουμε παραθέσουμε αν και δεν θα μας χρειαστούν όλες. Αρχικά θα ορίσουμε την Γ-συνάρτηση.

Ορισμός 1.24 (Γ-συνάρτηση) *Η Γ-συνάρτηση ορίζεται να είναι το γενικευμένο ολοκλήρωμα*

$$\Gamma(s)=\int_0^\infty e^{-t}t^s\,\frac{dt}{t}$$

για $Re(s)>0$.

Ιδιοτητες:

1. $\Gamma(1)=1$
2. $\Gamma(s+1)=s\Gamma(s)$
3. $\Gamma(s)\Gamma(1-s)=\frac{\pi}{\sin(\pi s)}\ \forall\, s\in\mathbb{C}\setminus\mathbb{Z}$.
4. $\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s+1}{2}\right)=\sqrt{\pi}2^{1-s}\Gamma(s)\ \forall\, s\in\mathbb{C}\setminus\{-n\mid n\in\mathbb{N}^*\}$.
5. $\Gamma(s+1)=s!$ *για* $s\in\mathbb{N}$

Για τις αποδείξεις αυτών των ιδιοτήτων παραπέμπουμε στο βιβλίο [ΓΙΑΝΑΝ].

1.4 Η συναρτησική εξίσωση της $\zeta(s)$

Σ' αυτή την ενότητα, όπως αναφέρει και ο τίτλος, θα αποδείξουμε την συναρτησιακή εξίσωση της ζ-συνάρτησης, που απεδείχθει από τον Riemann στο άρθρο του το 1857. *Η συναρτησιακή εξίσωση εκφράζει το* $\zeta(s)$ *ως συνάρτηση του* $\zeta(1-s)$. *Έτσι με τον τρόπο αυτό μπορούμε να υπολογίσουμε τη ζ-συνάρτηση και για αρνητικά* s. *Για παράδειγμα:* $\zeta(-2),\zeta(-4),\ldots$ *που αποτελούν τις τετριμμένες ρίζες της ζ - συνάρτησης.*

Πριν προχωρίσουμε στην απόδειξη θα αναφέρουμε κάποιες προτάσεις και ορισμούς που θα χρειαστούμε στη συνέχεια.

Ορισμός 1.25 (Μετασχηματισμός Mellin) *Ο μετασχηματισμός Mellin μιας συνάρτησης f είναι*

$$\{\mathcal{M}f\}(s) = \phi(s) = \int_0^\infty f(t)t^s \frac{dt}{t}.$$

Παρατήρηση 1.26 *Ειδικότερα ο μετασχηματισμός Mellin είναι ο μετασχηματισμός που σχετίζει τη συνηθισμένη σειρά Dirichlet $f(s) = \sum_{n=1}^\infty a_n n^{-s}$ με τη δυναμοσειρά με τους ίδιους συντελεστές $F(s) = \sum_{n=1}^\infty a_n s^n$ ως εξής:*

$$f(s) = \frac{1}{\Gamma(s)} \int_0^\infty F(e^{-t})t^{s-1}\, dt.$$

Ορισμός 1.27 *Ορίζουμε τη θήτα συνάρτηση ως εξής*

$$\Theta(t) := \sum_{n=-\infty}^{+\infty} e^{-\pi t n^2} \qquad\qquad (t > 0).$$

Πρόταση 1.28 *Η θήτα συνάρτηση $\Theta(t)$ επαληθεύει την παρακάτω συναρτησιακή εξίσωση*

$$\Theta(t) = \frac{1}{\sqrt{t}}\Theta\left(\frac{1}{t}\right).$$

Για την απόδειξη παραπέμπουμε στο βιβλίο [ΓΙΑΝΑΝ].

Πρόταση 1.29 *Για $t \to 0^+$ έχουμε:*

$$\left|\Theta(t) - t^{-\frac{1}{2}}\right| < e^{-c/t}$$

όπου c θετική σταθερά.

Για την απόδειξη παραπέμπουμε στο βιβλίο [ΓΙΑΝΑΝ].

Ορισμός 1.30 *Μία συνάρτηση λέγεται **αναλυτική** σ' ένα σημείο z αν είναι παραγωγίσιμη σε μία περιοχή του z. Ομοίως λέγεται **αναλυτική** σ' ένα σύνολο S αν είναι παραγωγίσιμη σε όλα τα σημεία ενός ανοικτού συνόλου που περιέχει το S.*

Ορισμός 1.31 *Έστω $f(z) = A(z)/B(z)$ με A, B να είναι αναλυτικές στο z_0 με $A(z_0) \neq 0$ και $B(z_0) = 0$, τότε λέμε ότι η f έχει πόλο στο z_0.*

Ορισμός 1.32 *Έστω $f(z) = A(z)/B(z)$ και*

$$f(z) = \sum_{-\infty}^{\infty} C_k(z - z_0)^k$$

σε μια τρυπημένη περιοχή του z_0, ο $\mathrm{Res}(f; z_0)$ λέγεται υπόλοιπο της f στο z_0. Αν η $f(z)$ έχει απλό πόλο στο z_0 τότε

$$\mathrm{Res}(f; z_0) = \lim_{z\to z_0} (z - z_0)f(z) = \frac{A(z_0)}{B'(z_0)}.$$

Ορισμός 1.33 (Μερόμορφη συνάρτηση) *Μερόμορφη λέμε μια μιγαδική συνάρτηση, η οποία στο $\mathbb{C}$ εκτός από πόλους δεν έχει άλλα ανώμαλα σημεία. Καθε μερόμορφη συνάρτηση μπορεί να γραφεί ως πηλίκο δύο ακέραιων συναρτήσεων (ακέραια λέγεται η συνάρτηση που είναι ορισμένη και αναλυτική στο $\mathbb{C}$).*

Πρόταση 1.34 *Μία μιγαδική συνάρτηση $f = u + iv$ είναι* ***παραγωγίσιμη*** *στο z αν ικανοποιείται η Εξίσωση Cauchy - Riemann*

$$f_y = if_x$$

$$\left(f_x = \lim_{h\to 0} \frac{f(x+h,y) - f(x,y)}{h} \ \textit{και}\ f_y = \lim_{h\to 0} \frac{f(x,y+h) - f(x,y)}{h}\right)$$

ή ισοδύναμα

$$u_x = v_y \ \textit{και}\ u_y = -v_x.$$

Θεώρημα 1.35 *Η ζήτα συνάρτηση του Riemann η οποία ορίζεται, κατ' αρχήν, για $\mathrm{Re}(s) > 1$ επεκτείνεται αναλυτικά σ' όλο το μιγαδικό s-επίπεδο, εκτός από μοναδικό απλό πόλο στη θέση $s = 1$ με ολοκληρωτικό υπόλοιπο ίσο προς 1. Αν $\Lambda(s) := \pi^{-s/2}\Gamma\left(\frac{s}{2}\right)\zeta(s)$ τότε η $\Lambda(s)$ παραμένει αναλλοίωτη αν*

$$s \mapsto 1 - s \qquad\qquad \Lambda(s) = \Lambda(1-s)$$

δηλαδή η $\zeta(s)$ επαληθεύει τη ***συναρτησιακή εξίσωση***

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) = \pi^{-\frac{1-s}{2}}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s).$$

Απόδειξη: *Για να καταλήξουμε στο ζητούμενο θα χρησιμοποιήσουμε τον μετασχηματισμό Mellin, που αναπτύξαμε παραπάνω*

$$\int_0^\infty \Theta(t)t^s\,\frac{dt}{t}.$$

Όπως ορίσαμε προηγούμενα

$$\Theta(t) = \sum_{n=-\infty}^{\infty} e^{-\pi t n^2}$$

συνεπώς για μεγάλο t και $n \neq 0$ όλοι οι όροι φθίνουν στο 0, ενώ για $n = 0$ η $\Theta(t)$ τείνει στο 1. Από την άλλη μεριά για πολύ μικρό t και κοντά στο 0 η πρόταση 1.29 λέει ότι η $\Theta(t)$ τείνει στο $t^{-1/2}$. Επειδή όμως θέλουμε ο μετασχηματισμός μας να συγκλίνει και στα δύο άκρα θα πρέπει να προσθέσουμε διαφορετικούς όρους, επιπλέον θα πρέπει να θέσουμε $s = s/2$ γιατί διαφορετικά θα πάρουμε την τιμή $\zeta(2s)$ αντι για $\zeta(s)$ που θέλουμε.

Ορίζουμε λοιπόν

$$\phi(s) := \int_1^\infty t^{s/2}\big(\Theta(t) - 1\big)\,\frac{dt}{t} + \int_0^1 t^{s/2}\left(\Theta(t) - \frac{1}{\sqrt{t}}\right)\,\frac{dt}{t}.$$

Τώρα θα ελέγξουμε αν οι ποσότητες $\Theta(t)-1$ *και* $\Theta(t)-\frac{1}{\sqrt{t}}$ *συγκλίνουν για κάθε* s. *Αρχικά η ποσότητα*

$$\Theta(t)-1=\sum_{n=-\infty}^{\infty}e^{-\pi tn^2}-1=2\sum_{n=1}^{\infty}e^{-\pi tn^2}\overset{t\to\infty}{\longrightarrow}0\;\forall\, s\in\mathbb{C}$$

αλλά και η ποσότητα $\Theta(t)-\frac{1}{\sqrt{t}}$ *από την πρόταση (1.29) συγκλίνει για κάθε* s.

Αφού η $\Theta(t)$ *όταν* $t\to 0$ *φράσεται από την* $t^{-\frac{1}{2}}$, *στο διάστημα* $(0,1]$ *μπορούμε να πάρουμε* s *τέτοιο ώστε* $Re(s)>1$, *συνεπώς το ολοκλήρωμα*

$$\int_0^1 t^{s/2}\left(\Theta(t)-\frac{1}{\sqrt{t}}\right)\frac{dt}{t}$$

είναι

$$\begin{aligned}\int_0^1 t^{\frac{s}{2}}\Theta(t)\,\frac{dt}{t}-\int_0^1 t^{\frac{s-1}{2}}\,\frac{dt}{t} &= \int_0^1 t^{\frac{s}{2}}\Theta(t)\,\frac{dt}{t}-\frac{2}{s-1}t^{\frac{2}{s-1}}\Big|_0^1\\ &= \int_0^1 t^{\frac{s}{2}}\Theta(t)\,\frac{dt}{t}-\frac{2}{s-1}.\end{aligned}$$

Επομένως για $s\in\mathbb{C}$ *με* $Re(s)>1$ *έχουμε*

$$\begin{aligned}\phi(s) &= 2\sum_{n=1}^{\infty}\int_1^{\infty}e^{-\pi tn^2}t^{\frac{s}{2}}\,\frac{dt}{t}+\left(\int_0^1 t^{\frac{s}{2}}\,\frac{dt}{t}+2\sum_{n=1}^{\infty}\int_0^1 e^{-\pi tn^2}t^{\frac{s}{2}}\,\frac{dt}{t}-\frac{2}{s-1}\right)\\ &= 2\sum_{n=1}^{\infty}\int_0^{\infty}e^{-\pi tn^2}t^{\frac{s}{2}}\,\frac{dt}{t}+\frac{2}{s}t^{\frac{2}{s}}\Big|_0^1-\frac{2}{s-1}\\ &= 2\sum_{n=1}^{\infty}\int_0^{\infty}e^{-\pi tn^2}t^{\frac{s}{2}}\,\frac{dt}{t}+\frac{2}{s}-\frac{2}{s-1}.\end{aligned}$$

Τώρα με τη χρήση του μετασχηματισμού Mellin

$$\int_0^{\infty}t^{s-1}e^{-nt}\,dt=n^{-s}\Gamma(s)$$

μπορούμε να θέσουμε $c=n$, *για κάθε σταθερά* $c>0$ *και να πάρουμε*

$$\int_0^{\infty}t^{s}e^{-ct}\,\frac{dt}{t}=c^{-s}\Gamma(s). \tag{1.1}$$

Αν θέσουμε $c=\pi n^2$ *και* $s\mapsto s/2$ *και πολλαπλασιάσουμε την* $\phi(s)$ *που υπολογίσαμε παραπάνω με 1/2 και αντικαταστήσουμε τον μετασχηματισμό Mellin της σχέσης (1.1) παίρνουμε*

$$\begin{aligned}\frac{1}{2}\phi(s) &= \sum_{n=1}^{\infty}(\pi n^2)^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)+\frac{1}{s}+\frac{1}{1-s}\\ &= \pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s)+\frac{1}{s}+\frac{1}{1-s}.\end{aligned}$$

Όπως δείξαμε τα ολοκληρώματα που ορίζουν την $\phi(s)$ συγκλίνουν για κάθε s, συνεπώς η $\phi(s)$ είναι μία ***ακέραια*** *συνάρτηση του s. Επομένως, υπάρχει μερόμορφη συνάρτηση του s σε όλο το μιγαδικό επίπεδο, η*

$$\frac{\pi^{\frac{s}{2}}}{\Gamma\left(\frac{s}{2}\right)}\left(\frac{1}{2}\phi(s)-\frac{1}{s}+\frac{1}{1-s}\right)=\zeta(s)$$

η οποία είναι η $\zeta(s)$ για $Re(s)>1$. Επειδή $\pi^{s/2}$, $1/\big(\Gamma(s/2)\big)$ και $\phi(s)$ είναι όλες ακέραιες συναρτήσεις, έπεται ότι οι μόνοι πιθανοί πόλοι είναι για $s=0$ και $s=1$. Αλλά κοντά στο $s=0$ μπορούμε να αντικαταστήσουμε το $s\Gamma(s/2)$ του παρονομαστή με

$$2\left(\frac{s}{2}\right)\Gamma\left(\frac{s}{2}\right)=2\Gamma\left(\frac{s}{2}+1\right)\neq 0 \quad \textit{καθώς } s\to 0$$

Σημείωση 1.36 *Η ανωτέρω σχέση προκύπτει με τη βοήθεια της ιδιότητας 2 της Γ συνάρτησης, δηλαδή*

$$\Gamma(s+1)=s\Gamma(s)\overset{s\mapsto\frac{s}{2}}{\Longrightarrow}\Gamma\left(\frac{s}{2}+1\right)=\left(\frac{s}{2}\right)\Gamma\left(\frac{s}{2}\right).$$

Άρα έχουμε μοναδικό πόλο για $s=1$ του οποίου το ολοκληρωτικό υπόλοιπο είναι

$$\lim_{s\to 1}(s-1)\frac{\pi^{\frac{s}{2}}}{\Gamma(\frac{s}{2})}\left(\frac{1}{2}\phi(s)-\frac{1}{s}+\frac{1}{s-1}\right)=\frac{\pi^{\frac{1}{2}}}{\Gamma\left(\frac{1}{2}\right)} \qquad (*)$$

Από την ιδιότητα 4 της Γ έχουμε ότι

$$\begin{aligned}\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{s+1}{2}\right) &= \sqrt{\pi}2^{1-s}\Gamma(s) \qquad (\textit{για } s=1)\\ \Gamma\left(\frac{1}{2}\right)\Gamma\left(\frac{1+1}{2}\right) &= \sqrt{\pi}2^{1-1}\Gamma(1) \qquad \big(\Gamma(1)=1\big)\\ \Gamma\left(\frac{1}{2}\right) &= \pi^{\frac{1}{2}}\end{aligned}$$

Άρα τελικά

$$(*)\Rightarrow\frac{\pi^{\frac{1}{2}}}{\Gamma\left(\frac{1}{2}\right)}=\frac{\pi^{\frac{1}{2}}}{\pi^{\frac{1}{2}}}=1.$$

Μένει λοιπόν να δείξουμε την συναρτησιακή εξίσωση.

Έχουμε

$$\Lambda(s)=\frac{1}{2}\phi(s)-\frac{1}{s}-\frac{1}{s-1}. \qquad (1.2)$$

Επειδή η $s\mapsto 1-s$ αφήνει αναλοίωτο το $1/s+1/(s-1)$ αρκεί $\phi(s)=\phi(1-s)$.

Τώρα χρειαζόμαστε την συναρτησιακή εξίσωση της θήτα συνάρτησης (πρόταση 1.28)

$$\Theta(t)=\frac{1}{\sqrt{t}}\Theta\left(\frac{1}{t}\right).$$

Αν στον ορισμό της $\phi(s)$ αντικαταστήσουμε το t με $\frac{1}{t}$ παίρνουμε:

$$\phi(s)=\int_0^1 t^{-\frac{s}{2}}\left[\Theta\left(\frac{1}{t}\right)-1\right]\frac{dt}{t}+\int_1^\infty t^{-\frac{s}{2}}\left[\Theta\left(\frac{1}{t}\right)-\sqrt{t}\right]\frac{dt}{t} \qquad (1.3)$$

οπότε η πρόταση 1.29 μας δίνει

$$\begin{aligned}(1.3) &= \int_0^1 t^{-\frac{s}{2}}\left(\sqrt{t}\Theta(t)-1\right)\frac{dt}{t}+\int_1^\infty t^{-\frac{s}{2}}\left(\sqrt{t}\Theta(t)-\sqrt{t}\right)\frac{dt}{t}\\ &= \int_0^1 t^{\frac{1-s}{2}}\left(\Theta(t)-\frac{1}{\sqrt{t}}\right)\frac{dt}{t}+\int_1^\infty t^{\frac{1-s}{2}}\left(\Theta(t)-1\right)\frac{dt}{t}\\ &= \phi(1-s).\end{aligned}$$

Αποδείξαμε λοιπόν αυτό που ζητούσαμε $\phi(s)=\phi(1-s)$ και επομένως $\Lambda(s)=\Lambda(1-s)$. Καταλήξαμε τελικά τη συναρτησιακή εξίσωση της ζ - συνάρτησης. □

Παρατήρηση 1.37 *Η πληροφορία ότι το s είναι ένας μιγαδικός αριθμός είναι πολύ συμαυτική. Αρχικά η ζ - συνάρτηση ορίζεται για $\mathrm{Re}(s)>1$, δηλαδή σε ανοικτό και συνεκτικό χωρίο. Επιπλέον, από την συναρτησιακή εξίσωση επεκτείνεται στο ημιεπίπεδο με $\mathrm{Re}(s)<0$. Άρα από την μιγαδική ανάλυση και λόγω αναλυτικής συνέχισης η επέκταση αυτή είναι μοναδική.*

Στη συνέχεια θα μορφοποιήσουμε την συναρτησιακή εξίσωση ώστε να μπορέσουμε να βρούμε τις τετριμμένες ρίζες της συνάρτησης ζ του Riemann.

Υπολογισμός των τετριμμένων ριζών της ζ-συνάρτησης.

$$\begin{aligned}\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s) &= \pi^{-\frac{1-s}{2}}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s)\Rightarrow\\ \zeta(s) &= \pi^{s-\frac{1}{2}}\frac{\Gamma\left(\frac{1-s}{2}\right)}{\Gamma\left(\frac{s}{2}\right)}\zeta(1-s) \qquad (1.4)\end{aligned}$$

Πρώτα θα απλοποιήσουμε την ποσότητα

$$\frac{\Gamma\left(\frac{1-s}{2}\right)}{\Gamma\left(\frac{s}{2}\right)}.$$

Από την ιδιότητα 3 της Γ-συνάρτησης εύκολα υπολογίζουμε ότι:

$$\Gamma\left(\frac{s}{2}\right)=\frac{\pi}{\Gamma\left(1-\frac{s}{2}\right)\sin\pi\frac{s}{2}}$$

και αν αντικαταστήσουμε το προηγούμενο στην ποσότητα $\frac{\Gamma\left(\frac{1-s}{2}\right)}{\Gamma\left(\frac{s}{2}\right)}$ θα έχουμε

$$\frac{\Gamma\left(\frac{1-s}{2}\right)\Gamma\left(1-\frac{s}{2}\right)\sin\left(\pi\frac{s}{2}\right)}{\pi}.$$

Θέτουμε $s=1-s$ (ο μετασχηματιμός είναι καλός αφού είναι αντιστρέψιμος), επομένως η ποσότητα $\Gamma\left(\frac{1-s}{2}\right)\Gamma\left(1-\frac{s}{2}\right)$ γίνεται $\Gamma\left(\frac{s}{2}\right)\Gamma\left(\frac{1+s}{2}\right)$ η οποία από την ιδιότητα 4 της Γ-συνάρτησης για ισούται με

$$\sqrt{\pi}2^{1-s}\Gamma(s).$$

και αντιστρέφοντας τον μετασχηματισμό έχουμε

$$\frac{\Gamma\left(\frac{1-s}{2}\right)}{\Gamma\left(\frac{s}{2}\right)}=\pi^{-1/2}2^s\Gamma(1-s)\sin\left(\pi\frac{s}{2}\right)$$

αντικαθιστούμε στην συναρτησιακή εξίσωση και παίρνουμε

$$\zeta(s) = \pi^{s-1} 2^s \Gamma(1-s) \sin\left(\pi \frac{s}{2}\right) \zeta(1-s)$$

Οι τετριμμένες ρίζες της συναρτησιακής εξίσωσης είναι οι ρίζες του ημιτόνου που βρίσκεται μέσα στην συναρτησική εξίσωση, δηλαδή

$$\sin\left(\pi \frac{s}{2}\right) = 0 \Rightarrow \sin\left(\pi \frac{s}{2}\right) = \sin 0 \Rightarrow s = \begin{cases} 4m \\ 4m+2 \end{cases} \quad m \in \mathbb{Z}^*$$

Μπορούμε να γενικεύσουμε τις ρίζες της συναρτησιακής εξίσωσης και θα έχουμε $s = 2k,\ k \in \mathbb{Z}^*$. *Όμως για τις θετικές τιμές του* k *θα πάρουμε τις τιμές της* ζ*-συνάρτησης* $\zeta(2), \zeta(4), \ldots$ *οι οποίες δεν είναι μηδέν. Συνεπώς οι τετριμμένες ρίζες της* ζ*-συνάρτησης ορίζονται για τις αρνητικές τιμές του* k. *Άρα οι τετριμμένες ρίζες της* ζ*-συνάρτησης είναι*

$$s = -2k,\ k \in \mathbb{N}^*.$$

Σημείωση 1.38 *Θα πρεπει* $s \neq 1$, *αφού για* $s = 1$ *η* $\zeta(s)$ *δεν συγκλίνει και επιπλέον τις τιμές* $s = -k$ *στις οποίες η* Γ*-συνάρτηση έχει πόλους τάξης 1.*

Στο σημείο αυτό μπορούμε να ορίσουμε την εικασία του Riemann.

> ***Η εικασία του Riemman***
> ***Οι μη τετριμμένες ρίζες της ζ-συνάρτησης έχουν πραγματικό μέρος*** $\mathbf{1/2}$.

Παράδειγμα 1.39 *Από τον προηγούμενο υπολογισμό για το* s *διαλέγουμε* $k = 1$ *και* $k = 2$ *έτσι έχουμε* $s = -2$ *και* $s = -4$ *άρα* $\zeta(-2) = 0$ *και* $\zeta(-4) = 0$.

Παράδειγμα 1.40

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$$

(Ένας τρόπος να υπολογίσουμε την $\zeta(2)$ *είναι να υπολογίσουμε το πλήρες σύστημα Fourier της συνάρτησης* $f(x) = x,\ x \in [-1, 1]$*).*

ΚΕΦΑΛΑΙΟ 2

Αλγεβρικά σώματα συναρτήσεων

2.1 Θέσεις

Σημείωση 2.1 (Ορισμός)

i. *Αν η* $\varphi : R \to R'$ *είναι ομομορφισμός και* $1-1$ *λέγεται* ***μονομορφισμός***.

ii. *Αν η* $\varphi : R \to R'$ *είναι ομομορφισμός και επί λέγεται* ***επιμορφισμός***.

iii. *Αν η* $\varphi : R \to R'$ *είναι ομομορφισμός και* $1-1$ *και επί λέγεται* ***ισομορφισμός***.

Ορισμός 2.2 *Έστω* F *ένα σώμα και* K *υπόσωμα του* F.

i. *Το* F/K *λέγεται επέκταση σώματος. Θεωρώντας το* F *ως έναν διανυσματικό χώρο πάνω από το* K*, η διάστασή του ονομάζεται βαθμός του* F/K *και συμβολίζεται με* $[F : K]$.

ii. *Το* F/K *λέγεται πεπρασμενη επέκταση αν* $[F : K] = n < \infty$*. Τότε υπάρχει μία βάση* $\{a_1, \ldots, a_n\}$ *του* F/K*, δηλαδή κάθε* $\gamma \in F$ *γράφεται με μοναδικό τρόπο στη μορφή*

$$\gamma = \sum_{i=1}^{n} c_i a_i \ \text{ με } \ c_i \in K.$$

Αν F/K *και* M/F *είναι πεπερασμένες επεκτάσεις, τότε και το* M/K *είναι πεπερασμένη επέκταση και ισχύει*

$$[M : K] = [M : F] \cdot [F : K].$$

iii. *Ένα στοιχείο $a \in F$ καλείται* ***αλγεβρικό πάνω από το K*** *αν υπάρχει* ***μη μηδενικό*** *πολυώνυμο $f(x) \in K[x]$ ($K[x]$: ο δακτύλιος πολυωνύμων του x με συντελεστές από το K) έτσι ώστε $f(a) = 0$. Αν δεν υπάρχει πολυώνυμο που να ικανοποιεί τις παραπάνω προϋποθέσεις τότε το στοιχείο a* ***δεν*** *είναι αλγεβρικό πάνω από το K, το a τότε καλείται* ***υπερβατικό πάνω από το K****.*

iv. *Η επέκταση σώματος F/K λέγεται* ***αλγεβρική επέκταση*** *αν* ***όλα*** *τα στοιχεία $a \in F$ είναι αλγεβρικά πάνω από το K.*

Σχόλια 2.3

i. *Έστω $\gamma_1, \ldots, \gamma_r \in F$. Το μικρότερο υπόσωμα του F το οποίο περιέχει το K και όλα τα στοιχεία $\gamma_1, \ldots, \gamma_r$ το συμβολίζουμε με $K(\gamma_1, \ldots, \gamma_r)$. Η επέκταση $K(\gamma_1, \ldots, \gamma_r)/K$ είναι πεπερασμένη αν-ν* ***όλα*** *τα γ_i, $i = 1, \ldots, r$ είναι* ***αλγεβρικά πάνω από το K****.*

ii. *Ειδικότερα το $a \in F$ είναι αλγεβρικό πάνω από το K αν και μόνο αν $[K(a) : K] < \infty$.*

Παράδειγματα 2.4

i. *Το $\mathbb{Q}(\sqrt{2})$ είναι μια πεπερασμένη επέκταση του $\mathbb{Q}$, με $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. Το $\sqrt{2}$ είναι αλγεβρικό πάνω του $\mathbb{Q}$, εφόσον υπάρχει μη μηδενικό πολυώνυμο $f(x) = x^2 - 2 \in \mathbb{Q}[x]$, του οποίου ο $\sqrt{2}$ είναι ρίζα.*

ii. *Ομοίως το $\mathbb{C}$ είναι μια πεπερασμένη επέκταση του $\mathbb{R}$, με $[\mathbb{C} : \mathbb{R}] = 2$. Το i είναι αλγεβρικό πάνω από το $\mathbb{Q}$, αφού είναι ρίζα του $(x^2 + 1) \in \mathbb{R}[x]$.*

iii. *Οι αριθμοί π και e είναι υπερβατικοί πάνω από το $\mathbb{Q}$. Όμως οι π και e είναι αλγεβρικοί πάνω από το $\mathbb{R}$ ως ρίζες των $(x - \pi) \in \mathbb{R}[x]$ και $(x - e) \in \mathbb{R}[x]$ αντίστοιχα.*

Στο σημείο αυτό θα πρέπει να αναφέρουμε την αιτιολόγηση της έκφρασης ***«πάνω από»*** *που θα χρησιμοποιούμε συχνά στη συνέχεια του κεφαλαίου.*

Σχόλιο 2.5 *Έστω K είναι ένα σώμα. Όταν μιλάμε για μια επέκταση ενός σώματος, για παράδειγμα F, πάνω από το K μπορούμε να δούμε το F σαν ένα διανυσματικό χώρο πάνω από το K όπου η πρόσθεση διανυσμάτων ταυτίζεται με τη συνήθη πρόσθεση του σώματος F και ο βαθμωτός πολλαπλασιαμός ενός στοιχείου του F με ένα στοιχείο του K ταυτίζεται με τον συνήθη πολλαπλασιασμό στο F.*

Ένα απλό παράδειγμα είναι το εξής

Παράδειγμα 2.6 *Για κάθε σώμα K μπορούμε να δούμε του $K[x]$ ως διανυσματικό χώρο πάνω από το K, στον οποίο η πρόσθεση διανυσμάτων ταυτίζεται με τη συνήθη πρόσθεση πολυωνύμων του $K[x]$ και το βαθμωτό γινόμενο ενός στοιχείου του $K[x]$ με ένα στοιχείο του K ταυτίζεται με το γινόμενο στον $K[x]$.*

Ορισμός 2.7 (Αλγεβρικό σώμα συναρτήσεων) *Ένα **αλγεβρικό σώμα συναρτήσεων** F/K μίας μεταβλητής πάνω από το K είναι μία επέκταση σώματος $F(\supseteq K)$ έτσι ώστε F να είναι μία πεπερασμένη αλγεβρική επέκταση του $K(x)$ για κάποια $x \in F$ τα οποία είναι υπερβατικά πάνω από το K. Για συντομία το F/K το λέμε **σώμα συναρτήσεων**.*

Για εκείνα τα στοιχεία του F που είναι υπερβατικά πάνω από το K ισχύει η ακόλουθη πρόταση.

Πρόταση 2.8 *Ένα στοιχείο $z \in F$ είναι υπερβατικό πάνω από το K αν και μόνο αν $[F : K(z)] < \infty$.*

Απόδειξη : $(\Longrightarrow)$

Ένα $z \in F$ λέμε ότι είναι υπερβατικό πάνω από το K, αν δεν υπάρχει ανάγωγο πολυώνυμο ελαχίστου με συντελεστές από το K που να έχει ως ρίζα το z, δηλαδή

$$\begin{array}{ll} F & \\ \Big| & \text{πεπερασμένη} \\ K(z) & \\ \Big| & \text{άπειρη} \\ K & \end{array}$$

επομένως $[F : K(z)] < \infty$.
$(\Longleftarrow)$

Αν $[F : K(z)] < \infty$ και z αλγεβρικό τότε $[K(z) : K] < \infty$. Επομένως $[F : K] = [F : K(z)] \cdot [K(z) : K] < \infty$. Άτοπο, άρα z υπερβατικό πάνω από το K. $\square$

Ορισμός 2.9 *Το σύνολο*

$$\widetilde{K} := \{z \in F : z \text{ είναι αλγεβρικό πάνω από το } K\}$$

λέγεται σώμα των σταθερών του F/K.

Παρατηρήσεις 2.10

i. *Το $\widetilde{K}$ είναι υπόσωμα του F.*
   Πράγματι, αν a, β αλγεβρικά στοιχεία του F, αρκεί να δείξουμε ότι $a + \beta, a \cdot \beta, -a$ και a^{-1} (με $a \neq 0$) είναι επίσης αλγεβρικά. Αφού a είναι αλγεβρικό ισχύει $[K(a) : K] < \infty$. Επιπλέον το β είναι αλγεβρικό πάνω από το K άρα είναι και αλγεβρικό πάνω απο το σώμα $K(a)$. Άρα το σώμα $K(a, \beta)$ είναι μία πεπερασμένη επέκταση του $K(a)$, δηλαδή $[K(a, \beta) : K(a)] < \infty$. Επειδή $K \subset K(a)$, το $[K(a, \beta) : K]$ είναι επίσης πεπερασμένο. Άρα κάθε στοιχείο του $K(a, \beta)$ είναι αλγεβρικό πάνω από το K. Τα στοιχεία $a + \beta, a \cdot \beta, -a$ και a^{-1} βρίσκονται όλα στο $K(a, \beta)$. Άρα είναι αλγεβρικά.

ii. *Ισχύει ότι* $K \subseteq \widetilde{K} \subset F$ *και ότι το* $F/\widetilde{K}$ *είναι σώμα συναρτήσεων πάνω από το* $\widetilde{K}$.

iii. *Το* K *θα λέγεται αλγεβρικά κλειστό στο* F *(δηλαδή κάθε μη σταθερό πολυώνυμο στον* $K[x]$ *έχει μία ρίζα στο* K*) αν* $\widetilde{K} = K$.

Παράδειγματα 2.11 *Το απλούστερο παράδειγμα ενός αλγεβρικού σώματος συναρτήσεων είναι το σώμα των ρητών συναρτήσεων.*

Το F/K *ονομάζεται* ***ρητό*** *αν* $F = K(x)$ *για κάποιο* $x \in F$ *υπερβατικό πάνω από το* K.

Κάθε στοιχείο $z(\neq 0) \in K(x)$ *γράφεται με μοναδικό τρόπο*

$$z = a \cdot \prod_i p_i(x)_i^n \tag{2.1}$$

όπου $a(\neq 0) \in K$, *τα* $p_i(x) \in K[x]$ *έχουν μεγιστοβάθμιο συντελεστή μονάδα (μονικά πολυώνυμα) και είναι ανάγωγα,* $n_i \in \mathbb{Z}$.

Σχόλια 2.12

i. *Ένα αυθαίρετο σώμα συναρτήσεων* F/K *(το οποίο δεν είναι απαραίτητα ρητό) συχνά αναπαρίσταται ως μία απλή αλγεβρική επέκταση σώματος, του σώματος των ρητών συναρτήσεων* $K(x)$*, δηλαδή* $F = K(x, y)$*, όπου* $\varphi(y) = 0$ *για κάποια ανάγωγα πολυώνυμα* $\varphi(t) \in K(x)[t]$.

ii. *Αν* F/K ***δεν*** *είναι ρητό σώμα συναρτήσεων, δεν είναι σαφές αν κάθε μη μηδενικό στοιχείο* $z \in F$ *δέχεται ανάλυση ανάλογης της (2.1). Πράγματι δεν είναι ξεκάθαρο τι εννοούμε όταν λέμε ανάγωγο στοιχείο του* F. *Ένα άλλο πρόβλημα σχετικά με την (2.1) είναι το ακόλουθο:*
Πρόβλημα: *Δίνονται τα στοιχεία* $a_1, \ldots, a_n \in K$. *Να βρείτε όλες τις ρητές συναρτήσεις* $f(x) \in K(x)$ *με προκαθορισμένη τάξη ριζών (ή πόλων) στα* $a_1, \ldots, a_n$.
Για να απαντήσουμε σε τέτοια προβλήματα εισάγουμε τις έννοιες των ***δακτυλίων εκτίμησης*** *και των* ***θέσεων***.

Ορισμός 2.13 (Δακτύλιος εκτίμησης) *Ένας* ***δακτύλιος εκτίμησης*** *ενός σώματος συναρτήσεων* F/K *είναι ένας δακτύλιος* $\mathcal{O} \subseteq F$ *με τις ακόλουθες ιδιότητες:*

i. $K \subset \mathcal{O} \subset F$ *και*

ii. *Για κάθε* $z \in F$ *το* $z \in \mathcal{O}$ *ή* $z^{-1} \in \mathcal{O}$.

Παρατηρήσεις 2.14 *Στην περίπτωση του σώματος των ρητών συναρτήσεων* $K(x)$ *δοθέντος ενός ανάγωγου πολυωνύμου* $p(x) \in K[x]$ *θεωρούμε το σύνολο*

$$\mathcal{O}_{p(x)} := \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x] \text{ και } p(x) \not| g(x) \right\}.$$

Επομένως,

i. *το $\mathcal{O}_{p(x)}$ είναι ένας δακτύλιος εκτιμήσεων του $K(x)/K$*

Απόδειξη: *Πράγματι $\mathcal{O}_{p(x)} \subset K(x)$ και για κάθε $z \in K(x)$ το $z \in \mathcal{O}_{p(x)}$ ή $z^{-1} \in \mathcal{O}_{p(x)}$. Κάθε $z \in K(x)$ είναι της μορφής $f(x)/g(x)$ όπου $f(x), g(x) \in K[x]$ και $p(x)$ ανάγωγο πολυώνυμο του $K[x]$ τότε $p(x) \not| f(x)$.* □

ii. *αν $q(x)$ είναι ένα άλλο ανάγωγο πολυώνυμο, τότε $\mathcal{O}_{p(x)} \neq \mathcal{O}_{q(x)}$.*

Πρόταση 2.15 *Έστω $\mathcal{O}$ ένας δακτύλιος εκτίμησης του σώματος συναρτήσεων F/K. Τότε*

i. *ο $\mathcal{O}$ είναι ένας τοπικός δακτύλιος, δηλαδή ο $\mathcal{O}$ έχει μοναδικό μέγιστο ιδεώδες $P := \mathcal{O} \setminus \mathcal{O}^*$ όπου το σύνολο*

$$\mathcal{O}^* = \left\{ z \in \mathcal{O} : \text{ υπάρχει } w \in \mathcal{O} \text{ με } zw = 1 \right\}$$

είναι η ομάδα των μονάδων του $\mathcal{O}$,

ii. *για $x(\neq 0) \in F$, το $x \in P$ αν-ν $x^{-1} \notin \mathcal{O}$ και*

iii. *για το σώμα $\widetilde{K}$ των σταθερών του F/K έχουμε ότι $\widetilde{K} \subseteq \mathcal{O}$ και $\widetilde{K} \cap P = \{0\}$.*

Απόδειξη:

i. *Θα δείξουμε ότι το $P = \mathcal{O} \setminus \mathcal{O}^*$ είναι ιδεώδες του $\mathcal{O}$.*

(α') *Το $0 \in P$.*

(β') *Έστω ότι $x \in P$ και $z \in \mathcal{O}$. Τότε $xz \notin \mathcal{O}^*$ γιατί αλλιώς το x θα μπορούσε να είναι μονάδα. Πράγματι αν $z \in \mathcal{O}$ τότε $xz = u \in \mathcal{O}^*$ οπότε $xu^{-1} = z^{-1}$ άρα z είναι μονάδα οπότε και x μονάδα. Επομένως $xz \in P$.*

(γ') *Έστω ότι $x, y \in P$. Χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι $x/y \in \mathcal{O}$. Τότε $1 + x/y \in \mathcal{O}$ και $x + y = y(1 + x/y) \in P$ από το β'.*

Άρα το P είναι ιδεώδες του $\mathcal{O}$. Ως γνήσιο ιδεώδες του $\mathcal{O}$ δεν μπορεί να περιέχει μονάδα οπότε είναι το μοναδιαίο μέγιστο ιδεώδες.

ii. *Έχουμε ότι $x \in F$ άρα*

$$x \in \mathcal{O} \text{ ή } x^{-1} \in \mathcal{O} \tag{2.2}$$

και $x \in P$ άρα

$$x \in \mathcal{O} \text{ και } x \notin \mathcal{O}^*. \tag{2.3}$$

Από τις (2.2) και (2.3) συνεπάγεται και αντιστρόφως ότι $x^{-1} \notin \mathcal{O}$.

iii. Έστω ότι $z \in \widetilde{K}$. Υποθέτουμε ότι $z \notin \mathcal{O}$. Τότε $z^{-1} \in \mathcal{O}$, εφόσον $\mathcal{O}$ είναι δακτύλιος εκτίμησης. Από την άλλη, αφού z^{-1} είναι αλγεβρικό πάνω από το K, υπάρχουν στοιχεία $a_1, \ldots, a_r \in K$ με

$$\begin{aligned} a_r(z^{-1})^r + \cdots + a_1 z^{-1} + 1 &= 0 \\ \text{ή} & \\ z^{-1}\big(a_r(z^{-1})^{r-1} + \cdots + a_1\big) &= -1 \end{aligned}$$

Επομένως

$$z = -\big(a_r(z^{-1})^{r-1} + \cdots + a_1\big) \in K[z^{-1}] \subseteq \mathcal{O}.$$

Έτσι $z \in \mathcal{O}$. Η ισχύς της $\widetilde{K} \cap P = \{0\}$ είναι προφανής. □

Θεώρημα 2.16 *Έστω $\mathcal{O}$ ένας δακτύλιος εκτίμησης του σώματος συναρτήσεων F/K και P είναι το μοναδικό του μέγιστο ιδεώδες. Τότε:*

i. Το P είναι κύριο ιδεώδες.

ii. Αν $P = t\mathcal{O}$, τότε κάθε $z(\neq 0) \in F$ έχει μοναδική αναπαράσταση, της μορφής

$$z = t^n u$$

για κάποια $n \in \mathbb{Z},\ u \in \mathcal{O}^*$.

iii. Έστω ότι το $\mathcal{O}$ είναι περιοχή κυρίων ιδεωδών. Ακριβώς, αν $P = t\mathcal{O}$ και $I(\neq \{0\}) \subseteq \mathcal{O}$ είναι ιδεώδες, τότε $I = t^n\mathcal{O}$ για κάποια $n \in \mathbb{N}$.

Σημείωση 2.17 (Ορισμός) *Ένας δακτύλιος με τις παραπάνω ιδιότητες καλείται **διακριτός δακτύλιος εκτίμησης**.*

Λήμμα 2.18 *Έστω $\mathcal{O}$ είναι ένας δακτύλιος εκτίμησης ενός αλγερικού σώματος συναρτήσεων F/K, P το μέγιστο ιδεώδες του και $x(\neq 0) \in P$. Έστω $x_1, x_2, \ldots, x_n \in P$ έτσι ώστε $x_1 = x$ και $x_i \in x_{i+1}P$ για $i = 1, \ldots, n-1$. Τότε έχουμε $n \leq [F : K(x)] < \infty$.*

Απόδειξη: *Το ότι $[F : K(x)] < \infty$ προκύπτει από τις προτάσεις 2.8 και 2.15. Έτσι μένει να δείξουμε ότι τα $x_1, \ldots, x_n$ είναι γραμμικώς ανεξάρτητα πάνω από το $K(x)$. Για το λόγο αυτό υποθέτουμε ότι υπάρχει ένας μη τετριμμένος γραμμικός συνδιασμός*

$$\sum_{i=1}^{n} \varphi_i x_i = 0 \text{ με } \varphi_i \in K(x).$$

Μπορούμε να υποθέσουμε ότι όλα τα φ_i είναι πολυώνυμα του x και ότι το x δεν τα διαιρεί όλα. Θέτουμε $a_i := \varphi_i(0)$ ως τον σταθερό όρο του φ_i και ορίζουμε $j \in \{1, \ldots, n\}$ με την υπόθεση $a_j \neq 0$ αλλά $a_i = 0$ για όλα τα $i > j$. Έχουμε λοιπόν

$$-\varphi_j x_j = \sum_{i \neq j} \varphi_i x_i \tag{2.4}$$

με $\varphi_i \in \mathcal{O}$ για $i = 1, \ldots, n$ (εφόσου $x = x_1 \in P$), $x_i \in x_j P$ για $i < j$ και $\phi_i = xg_i$ για $i > j$, όπου g_i τα πολυώνυμα του x. Διαιρώντας την (2.4) με x_j προκύπτει

$$-\varphi_j = \sum_{i<j} \varphi_i \cdot \frac{x_i}{x_j} + \sum_{i>j} \frac{x}{x_j} \cdot g_i x_i.$$

τα αθροίσματα του δευτέρου μέλους ανήκουν στο P, επομένως $\varphi_j \in P$. Από την άλλη $\varphi_j = a_j + xg_j$ με $g_j \in K[x] \subseteq \mathcal{O}$ και $x \in P$, έτσι ώστε $a_j = \varphi_j - xg_j \in P \cap K$. Άτοπο, γιατί $a_j \neq 0$. Άρα τα $x_1, \ldots, x_n$ είναι γραμμικώς ανεξάρτητα πάνω από το $K(x)$. □

Απόδειξη: *(Θεωρήματος 2.16)*

i. *Υποθέτουμε ότι το P δεν είναι κύριο ιδεώδες. Έστω επίσης ένα στοιχείο $x_1 (\neq 0) \in P$. Αφού $P \neq x_1\mathcal{O}$, υπάρχει $q_2 \in P \setminus x_1\mathcal{O}$. Τότε $x_2 x_2^{-1} \notin \mathcal{O}$, οπότε $x_2^{-1} x_1 \in P$ από την πρόταση 2.15.ii. Έτσι $x_1 \in x_2 P$. Με επαγωγή παίρνουμε μία άπειρη ακολουθία $x_1, x_2, x_3, \ldots$ στο P, τέτοια ώστε $x_i \in x_{i+1} P$ για κάθε $i \geq 1$.* Ατοπο, *από το λήμμα 2.18. Άρα το P είναι κύριο ιδεώδες του $\mathcal{O}$.*

ii. *Έστω ότι $z \in F$. Τότε $z \in \mathcal{O}$ ή $z^{-1} \in \mathcal{O}$, οπότε μπορούμε να υποθέσουμε ότι $z \in \mathcal{O}$. Αν $z \in \mathcal{O}^*$ τότε $z = t^0 z$. Άρα ισχύει. Αν $z \in P$ υπάρχει ένα μέγιστο $m \geq 1$ με $z \in t^m \mathcal{O}$, εφόσον το μήκος της ακολουθίας*

$$x_1 = z, x_2 = t^{m-1}, x_3 = t^{m-2}, \ldots, x_m = t$$

φράσεται λόγω του λήμματος 2.18. Γράφουμε $z = t^m u$ με $u \in \mathcal{O}$. Τότε το u πρέπει να είναι μονάδα του $\mathcal{O}$ (αλλιώς $u \in P = t\mathcal{O}$ και έτσι $u = tw$ με $w \in \mathcal{O}$ και $z = t^{m+1} w \in t^{m+1}\mathcal{O}$. Ατοπο, *γιατί το m είναι μέγιστο μ¨ αυτή την ιδιότητα). Άρα $z = t^m u$ με $m \in \mathbb{Z}$ και $u \in \mathcal{O}^*$.*

Μοναδικότητα: *Αν $z = t^m u = t^s v$ όπου $u, v \in \mathcal{O}^*$ και $m \leq s$, τότε $u = t^{s-m} v$ οπότε $s = m$ και $u = v$.*

iii. *Έστω ότι το $I (\neq \{0\}) \subseteq \mathcal{O}$ είναι ένα ιδεώδες. Το σύνολο*

$$A := \{r \in \mathbb{N} : t^r \in I\}$$

δεν είναι κενό $\big($αν $x (\neq 0) \in I$ τότε $x = t^r u$ με $u \in \mathcal{O}$ και $t^r = xu^{-1} \in I\big)$. Θέτουμε $n := \min(A)$. Απαιτούμε $I = t^n \mathcal{O}$. $t^n \mathcal{O} \subseteq I$ ισχύει, εφ¨ όσον $t^n \in I$. Έστω $y \in I$ με $y \neq 0$. Έχουμε $y = t^s w$ με $w \in \mathcal{O}^*$ και $s \geq 0$. Έτσι $t^s \in I$ και $s \geq n$. Επομένως $y = t^n t^{s-n} w \in t^n \mathcal{O}$. Άρα $I \subseteq t^n \mathcal{O}$. Άρα $I = t^n \mathcal{O}$. □

Ορισμός 2.19

i. *Μία **θέση** P του σώματος συναρτήσεων F/K είναι το μέγιστο ιδεώδες κάποιου δακτυλίου εκτίμησης $\mathcal{O}$ του F/K. Κάθε στοιχείο $t \in P$ έτσι ώστε $P = t\mathcal{O}$ ονομάζεται **πρώτο στοιχείο για το P**.*

ii. $\mathbb{P}_F := \{P : P \text{ είναι μία θέση του } F/K\}$

Αν $\mathcal{O}$ είναι ένας δακτύλιος εκτίμησης του F/K και το P το μέγιστο ιδεώδες του, τότε το $\mathcal{O}$ ορίζεται μοναδικά από το P, δηλαδή

$$\mathcal{O} = \{z \in F : z^{-1} \notin P\}$$

(πρόταση 2.15). Επομένως το $\mathcal{O}_P(:= \mathcal{O})$ ονομάζεται δακτύλιος εκτίμησης της θέσης P.

Ορισμός 2.20 *Μία διακριτή εκτίμηση του F/K είναι μία συνάρτηση $\upsilon : F \to \mathbb{Z} \cup \{\infty\}$ με τις ακόλουθες ιδιότητες:*

1. $\upsilon(x) = \infty \Leftrightarrow x = 0$.
2. $\upsilon(xy) = \upsilon(x) + \upsilon(y),\ \forall\, x, y \in F$.
3. $\upsilon(x + y) \geq \min\{\upsilon(x), \upsilon(y)\},\ \forall\, x, y \in F$.
4. *Υπάρχει ένα στοιχείο $z \in F$ με $\upsilon(z) = 1$ και*
5. $\upsilon(a) = 0,\ \forall\, a(\neq 0) \in K$.

Το σύμολο ∞ εκφράζει τα στοιχεία που δεν ανήκουν στο $\mathbb{Z}$ έτσι ώστε $\infty + \infty = \infty + n = n + \infty = \infty$ και $\infty > m$ για όλα τα $m, n \in \mathbb{Z}$.

Από τις ιδιότητες (2) και (4) του ορισμού 2.20 προκύπτει αμέσως ότι η $\upsilon : F \to \mathbb{Z} \cup \{\infty\}$ είναι 1-1 και επί.

Λήμμα 2.21 (Ισχυρή Τριγωνική Ανισότητα) *Έστω υ μία διακριτή εκτίμηση του F/K και $x, y \in F$ με $\upsilon(x) \neq \upsilon(y)$. Τότε*

$$\upsilon(x + y) = \min\{\upsilon(x), \upsilon(y)\}.$$

Απόδειξη: *Παρατηρούμε ότι*

$$\upsilon(ay) = \upsilon(a) + \upsilon(y) = 0 + \upsilon(y) = \upsilon(y)$$

για $a(\neq 0) \in K$ (Ιδιότητες (2) και (5) του ορισμού 2.20). Ειδικότερα

$$\upsilon(-y) = \upsilon(-1 \cdot y) = \upsilon(-1) + \upsilon(y) = 0 + \upsilon(y) = \upsilon(y).$$

Εφόσον $\upsilon(x) \neq \upsilon(y)$ μπορούμε να υποθέσουμε $\upsilon(x) > \upsilon(y)$. Υποθέτουμε ότι $\upsilon(x + y) \neq \min\{\upsilon(x), \upsilon(y)\}$ και έτσι $\upsilon(x + y) > \upsilon(y)$ από την ιδιότητα (3) του ορισμού 2.20. Οπότε έχουμε $\upsilon(x) = \upsilon\big((x+y)-y\big) \geq \min\{\upsilon(x+y), \upsilon(y)\} > \upsilon(x)$. Ατοπο! *Άρα $\upsilon(x + y) = \min\{\upsilon(x), \upsilon(y)\}$.* □

Ορισμός 2.22 *Σε κάθε θέση $P \in \mathbb{P}_F$ αντιστοιχίζουμε μία συνάρτηση $\upsilon_p : F \to \mathbb{Z} \cup \{\infty\}$ (η οποία μπορεί να αποδειχθεί ότι είναι μία διακριτή εκτίμηση του F/K). Διαλέγουμε ένα πρώτο στοιχείο t για το P. Τότε κάθε $z(\neq 0) \in F$ έχει μοναδική αναπαράσταση $z = t^n u$ με $u \in \mathcal{O}_P^*$ και $n \in \mathbb{Z}$. Ορίζουμε $\upsilon_P(z) := n$ και $\upsilon_P(0) := \infty$.*

Παρατήρηση 2.23 *Ο προηγούμενος ορισμός εξαρτάται μόνο από το P και όχι από την επιλογή του t. Αν t' (τυχαίο στοιχείο) είναι ένα άλλο πρώτο στοιχείο για το P τότε $P = t\mathcal{O} = t'\mathcal{O}$. Έτσι $t = t'w$ για κάποια $w \in \mathcal{O}_P^*$. Επομένως $t^n u = (t'^n w^n)u = t'^n(w^n u)$ με $w^n u \in \mathcal{O}_P^*$.*

Θεώρημα 2.24 *Έστω F/K ένα σώμα συναρτήσεων. Τότε*

i. Για κάθε θέση $P \in \mathbb{P}_F$, η συνάρτηση υ_p που ορίστηκε πιο πάνω είναι μία διακριτή εκτίμηση του F/K. Επιπλέον έχουμε

$$\mathcal{O}_P = \{z \in F : \upsilon_P(z) \geq 0\} \tag{2.5}$$

$$\mathcal{O}_P^* = \{z \in F : \upsilon_P(z) = 0\} \tag{2.6}$$

$$P = \{z \in F : \upsilon_P(z) > 0\} \tag{2.7}$$

Τέλος ένα στοιχείο $x \in F$ είναι ένα πρώτο στοιχείο για το P αν και μόνο αν $\upsilon_P(x) = 1$.

ii. ***Αντιστρόφως.*** *Υποθέτουμε ότι υ είναι μία διακριτή εκτίμηση του F/K. Τότε το σύνολο*

$$P := \{z \in F : \upsilon(z) > 0\}$$

είναι μία θέση του F/K και το

$$\mathcal{O}_P = \{z \in F : \upsilon(z) \geq 0\}$$

είναι ο αντίστοιχος δακτύλιος εκτίμησης.

iii. Κάθε δακτύλιος εκτίμησης $\mathcal{O}$ του F/K είναι ένας μέγιστος, γνήσιος υποδακτύλιος του F.

Απόδειξη :

i. Η υ_P έχει τις ιδιότητες (1), (2), (4) και (5) του ορισμού 2.20. Θ¨ αποδείξουμε ότι ισχύει και η (3). Έστω ότι $x, y \in F$ με $\upsilon_P(x) = n$ και $\upsilon_P(y) = m$. Μπορούμε να υποθέσουμε ότι $n \leq m < \infty$. Έτσι $x = t^n u_1$ και $y = t^m u_2$ με $u_1, u_2 \in \mathcal{O}_P^*$. Τότε

$$x + y = t^n u_1 + t^m u_2 = t^n(u_1 + t^{m-n} u_2) = t^n z$$

με $z \in \mathcal{O}_P$. Αν $z = 0$ έχουμε

$$\upsilon_P(x + y) = \infty > \min\{n, m\}$$

αλλιώς $z = t^k \cdot u$ *με* $k \geq 0$ *και* $u \in \mathcal{O}_P^*$. *Επομένως*

$$\upsilon_P(x+y) = \upsilon_P(t^{n+k}u) = n+k \geq n = \min\{\upsilon_P(x), \upsilon_P(y)\}.$$

Άρα υ_P *είναι μία διακριτή εκτίμηση του* F/K. *Τέλος αν* $x \in F$ *είναι ένα πρώτο στοιχείο για το* $P \Leftrightarrow x = x^1 u$ *με* $u \in \mathcal{O}_P^* \Leftrightarrow \upsilon_P(x) = 1$.

ii. Πράγματι, το $\mathcal{O}_P$ *είναι δακτύλιος εκτίμησης αφού αν* $z \in F$ *τότε* $\upsilon(z) \geq 0$ *οπότε* $z \in \mathcal{O}_P$ *ή* $\upsilon(z) < 0$ *οπότε* $\upsilon(z^{-1}) = -\upsilon(z) > 0$ *και* $z^{-1} \in \mathcal{O}_P$. *Οι μονάδες του* $\mathcal{O}_P$ *είναι τα* $z \in F$ *ώστε* $\upsilon(z) = 0$ *και το μέγιστο ιδεώδες αποτελείται από αυτά που έχουν θετική εκτίμηση.*

iii. Έστω $\mathcal{O}$ *ένας δακτύλιος εκτίμησης του* F/K, P *το μέγιστο του ιδεώδες,* υ_P *η διακριτή εκτίμηση που αντιστοιχεί στο* P *και* $z \in F \setminus \mathcal{O}$. *Θέλουμε να δείξουμε ότι* $F = [z]$. *Έστω ένα αυθαίρετο στοιχείο* $y \in F$ *τότε* $\upsilon_P(yz^{-k}) \geq 0$ *για αρκετά μεγάλο* $k \geq 0$ $\left(\upsilon_P(z^{-1}) > 0\right)$ *εφόσον* $z \notin \mathcal{O}$. *Συνεπώς* $w := yz^{-k} \in \mathcal{O}$ *και* $y = wz^k \in \mathcal{O}[z]$. *Άρα* $F \subseteq \mathcal{O}[z]$ *και επειδή* $\mathcal{O}[z] \subseteq F$ *έχουμε* $F = \mathcal{O}[z]$. □

Έστω P *μία θέση του* F/K *και* $\mathcal{O}_P$ *ο δακτύλιος εκτίμησης της. Εφόσον* P *είναι ένα μέγιστο ιδεώδες, ο δακτύλιος κλάσης υπολοίπων* $\mathcal{O}_P/P$ *είναι σώμα. Για* $x \in \mathcal{O}_P$ *ορίζουμε* $x(P) \in \mathcal{O}_P/P$ *να είναι η κλάση των υπολοίπων του* $x \,\mathrm{modulo} P$, *για* $x \in F \setminus \mathcal{O}_P$ *θέτουμε* $x(P) := \infty$ *(το σύμβολο* ∞ *δεν έχει έννοια με τον ορισμό 2.20).*

Από την πρόταση 2.15 ξέρουμε ότι $K \subseteq \mathcal{O}_P$ *και* $K \cap P = \{0\}$. *Έτσι η απεικόνιση* $\mathcal{O}_P \to \mathcal{O}_P/P$ *δημουργεί μία κανονική* ***εμφύτευση*** *του* K *στο* $\mathcal{O}_P/P$. *Στο εξής θα θεωρούμε το* K *πάντα ως υπόσωμα του* $\mathcal{O}_P/P$ *μέσω αυτής της εμφύτευσης. Αυτό εφαρμόζεται και για το* $\widetilde{K}$ *αντί για το* K. *Έτσι μπορούμε να θεωρούμε το* $\widetilde{K}$ *ως υπόσωμα του* $\mathcal{O}_P/P$.

Σημείωση 2.25 (Ορισμός: Εμφύτευση σωμάτων) *Έστω* F, F' *δύο σώματα, θα λέμε ότι το* F *εμφυτεύεται στο* F' *και θα γράφουμε* $F \hookrightarrow F'$ *αν υπάρχει* $\phi : F \to F'$ *η οποία να είναι ομομορφισμός.*

Ορισμός 2.26 *Έστω* $P \in \mathbb{P}_F$.

i. $F_P := \mathcal{O}_P/P$ *είναι ένα σώμα κλάσης υπολοίπων του* P. *Η απεικόνιση* $x \mapsto x(P)$ *από το* F *στο* $F_P \cup \{\infty\}$ *ονομάζεται απεικόνιση κλάσης υπολοίπων με εκτίμηση στο* P. *Μερικές φορές θα χρησιμοποιήσουμε επίσης τον συμβολισμό* $x + P := x(P)$ *για* $x \in \mathcal{O}_P$.

ii. $\deg P := [F_P : K]$ *ονομάζεται* ***βαθμός*** *του* P.

Παρατήρηση 2.27 *Ο βαθμός μιας θέσης είναι* ***πάντα πεπερασμένος.***

Πρόταση 2.28 *Αν P είναι μία θέση του F/K και $x(\neq 0) \in P$ τότε $\deg P \leq [F : K(x)] < \infty$.*

Απόδειξη: *$[F : K(x)] < \infty$ ισχύει από την πρόταση 2.8. Οπότε μένει να δείξουμε ότι για οποιαδήποτε στοιχεία $z_1, \ldots, z_n \in \mathcal{O}_P$ των οποίων οι κλάσεις υπολοίπων $z_1(P), \ldots, z_n(P) \in F_P$ είναι γραμμικά ανεξάρτητες πάνω από το K, είναι και γραμμικά ανεξάρτητες πάνω από το $K(x)$.*
Υποθέτουμε ότι υπάρχει ένας μη τετριμμένος γραμμικός συνδυασμός

$$\sum_{i=1}^{n} \varphi_i z_i = 0 \tag{2.8}$$

με $\varphi_i \in K(x)$. Χωρίς βλάβη της γενικότητας θεωρούμε ότι τα φ_i είναι πολυώνυμα του x και δεν είναι όλα διαιρετά από το x δηλαδή $\varphi_i = a_i + xg_i$ με $a_i \in K$, $g_i \in K[x]$ όχι όλα τα $a_i = 0$. Εφόσου $x \in P$ και $g_i \in \mathcal{O}_P$, $\varphi_i(P) = a_i(P) = a_i$. Εφαρμόζοντας την απεικόνιση κλάσης υπολοίπων στην (2.8) έχουμε

$$0 = 0(P) = \sum_{i=1}^{n} \varphi_i(P) z_i(P) = \sum_{i=1}^{n} a_i z_i(P) \tag{2.9}$$

Ατοπο, *γιατί τα $z_i(P), \ldots, z_n(P)$ είναι γραμμικά ανεξάρτητα πάνω από το K.* □

Πόρισμα 2.29 *Το σώμα $\widetilde{K}$ των σταθερών του F/K είναι μία πεπερασμένη επέκταση του K.*

Απόδειξη: *Το $P_F \neq \emptyset$ (αποδεικνύεται παρακάτω). Επιλέγουμε κάποια $P \in \mathbb{P}_F$. Εφόσου $\widetilde{K}$ έχει εμφυτευθεί στο F_P μέσω της απεικόνισης κλάσης υπολοίπων $\mathcal{O}_P \to F_P$, έπεται ότι*

$$[\widetilde{K} : K] \leq [F_P : K] < \infty. \tag{2.10}$$

□

Σχόλιο 2.30 *Για την περίπτωση που $\deg P = 1$ έχουμε $F_P = K$ και η απεικόνιση κλάσης υπολοίπων απεικονίζει το F στο $K \cup \{\infty\}$. Ειδικότερα αν K είναι ένα αλγεβρικά κλειστό σώμα, κάθε θέση έχει βαθμό 1, οπότε μπορούμε να διαβάσουμε ένα στοιχείο $z \in F$ ως μία συνάρτηση*

$$z : \begin{cases} \mathbb{P}_F \to K \cup \{\infty\} \\ P \to z(P) \end{cases}. \tag{2.11}$$

*Για το λόγο αυτό το F/K λέγεται **σώμα συναρτήσεων**. Τα στοιχεία του K που ερμηνεύονται ως συναρτήσεις με την έννοια της (2.11) είναι σταθερές συναρτήσεις γι' αυτό το λόγο το K ονομάζεται **σώμα σταθερών του F**.*

Ορισμός 2.31 *Έστω $z \in F$ και $P \in \mathbb{P}_F$. Λέμε ότι:*

- *το P είναι* ***ρίζα*** *του $z \Leftrightarrow v_P(z) > 0$.*
- *το P είναι* ***πόλος*** *του $z \Leftrightarrow v_P(z) < 0$.*

Αν $v_P(z) = m > 0,\ P$ είναι ***ρίζα*** *του z τάξης m. Αν $v_P(z) = -m < 0,\ P$ είναι* ***πόλος*** *του z τάξης m.*

Θεώρημα 2.32 *Έστω F/K ένα σώμα συναρτήσεων και R ένας υποδακτύλιος του F με $K \subseteq R \subseteq F$. Έστω ότι $\{0\} \neq I \subsetneq R$ ένα γνήσιο ιδεώδες του R. Τότε υπάρχει μία θέση $P \in \mathbb{P}_F$ τέτοια ώστε $I \subseteq P$ και $R \subseteq \mathcal{O}_P$.*

Πριν προχωρίσουμε στην απόδειξη του θεωρήματος θα παραθέσουμε το λήμμα του Zorn, που θα χρειστούμε στη συνέχεια.

Λήμμα 2.33 (Zorn) *Αν S είναι ένα μερικά διατεταγμένο σύνολο τέτοιο ώστε κάθε αλυσίδα στο S να έχει ένα άνω φράγμα στο S, τότε το S έχει τουλάχιστον ένα μέγιστο στοιχείο.*

Σημείωση 2.34 *Ένα υποσύνολο T ενός μερικά διατεταγμένου συνόλου S λέγεται* ***αλυσίδα*** *αν οποιαδήποτε δύο στοιχεία a και b του S είναι συγκρίσιμα.*

Ένα στοιχείο $u \in S$ λέγεται άνω φράγμα ενός υποσυνόλου A ενός μερικά διατεταγμένου συνόλου S αν $a \leq u,\ \forall\, a \in A$.

Ένα στοιχείο m ενός μερικά διατεταγμένου συνόλου S λέγεται μεγιστικό αν δεν υπάρχει $s \in S$ τέτοιο ώστε $m < s$.

Απόδειξη: (Θεωρήματος)
Θεωρούμε το σύνολο

$$\mathcal{F} := \{S : S \text{ είναι υποδακτύλιος του } F \text{ με } R \subseteq S \text{ και } IS \neq S\} \tag{2.12}$$

(εξ' ορισμού, IS είναι το σύνολο όλων των πεπερασμένων αθροισμάτων $\sum a_\nu s_\nu$ με $a_\nu \in I,\ s_\nu \in S$. IS είναι ένα ιδεώδες του S). $R \in \mathcal{F}$ άρα $\mathcal{F} \neq \emptyset$ και $\mathcal{F}$ είναι επαγωγικώς διατεταγμένο. Πράγματι, αν $\mathcal{H} \subseteq \mathcal{F}$ είναι ολικώς διατεταγμένο υποσύνολο του $\mathcal{F}$ τότε $T := \bigcup\{S : S \in \mathcal{H}\}$ είναι υποδακακτύλιος του F με $R \subseteq T$. Έχουμε να αποδείξουμε ότι $IT \neq T$. Υποθέτουμε ότι αυτό δεν ισχύει, τότε $1 = \sum_{\nu=1}^{n} a_\nu s_\nu$ με $a_\nu \in I, s_\nu \in T$. Εφόσον $\mathcal{H}$ είναι ολικά διατεταγμένο υπάρχει ένα $S_0 \in \mathcal{H}$ τέτοιο ώστε $s_1, \ldots, s_n \in S_0$, έτσι

$$1 = \sum_{\nu=1}^{n} a_\nu s_\nu \in IS_0. \tag{2.13}$$

Ατοπο, *άρα $IT \neq T$.*
Από το λήμμα του Zorn (βλ. ανωτέτρω) το $\mathcal{F}$ περιέχει ένα μέγιστο στοιχείο, δηλαδή ένας δακτύλιος $\mathcal{O} \subseteq F$ τέτοιος ώστε $R \subseteq \mathcal{O} \subseteq F,\ I\mathcal{O} \neq \mathcal{O}$ και $\mathcal{O}$ μέγιστο με αυτές τις ιδιότητες.

Θα δείξουμε τώρα ότι το $\mathcal{O}$ είναι δακτύλιος εκτίμησης του F/K. Εφόσον $I \neq \{0\}$ και $I\mathcal{O} \neq \mathcal{O}$ έχουμε $\mathcal{O} \subsetneqq F$ και $I \subseteq \mathcal{O} \setminus \mathcal{O}^*$. Υποθέτουμε ότι υπάρχει ένα στοιχείο $z \in F$ με $z \notin \mathcal{O}$ και $z^{-1} \notin \mathcal{O}$. Τότε $I\mathcal{O}[z] = \mathcal{O}[z]$ και $I\mathcal{O}[z^{-1}] = \mathcal{O}[z^{-1}]$ και μπορούμε να βρούμε $a_0, \ldots, a_n, b_0, \ldots, b_n \in I\mathcal{O}$ με

$$1 = a_0 + a_1 z + \cdots + a_n z^n \qquad \text{και} \tag{2.14}$$

$$1 = b_0 + b_1 z^{-1} + \cdots + b_m z^{-m} \tag{2.15}$$

με $n \geq 1$ και $m \geq 1$. Μπορούμε να υποθέσουμε ότι m , n έχουν επιλεχθεί να είναι τα μικρότερα δυνατά και $m \leq n$. Πολλαπλασιάζοντας την (2.14) με $1 - b_0$ και την (2.15) με $a_n z^n$ παίρνουμε

$$1 - b_0 = (1 - b_0)a_0 + (1 - b_0)a_1 z + \cdots + (1 - b_0)a_n z^n \quad \text{και} \tag{2.16}$$

$$0 = (b_0 - 1)a_n z^n + b_1 a_n z^{n-1} + \cdots + b_m a_n z^{n-m}. \tag{2.17}$$

Στη συνέχεια προσθέτουμε κατά μέλη τις (2.16) και (2.17) και έχουμε

$$1 = c_0 + c_1 z + \cdots + c_{n-1} z^{n-1} \tag{2.18}$$

με συντελεστές $c_i \in I\mathcal{O}$. Ατοπο *λόγω του ελαχίστου του n στην (2.14). Άρα $z \in \mathcal{O}$ ή $z^{-1} \in \mathcal{O}$ οπότε $\mathcal{O}$ είναι* ***δακτύλιος εκτίμησης*** *του F/K.* □

Πόρισμα 2.35 *Έστω F/K σώμα συναρτήσεων, $z \in F$ υπερβατικό πάνω από το K. Τότε z έχει* ***μία τουλάχιστον ρίζα και έναν τουλάχιστον πόλο****. Ειδικότερα $\mathbb{P}_F \neq \emptyset$.*

Απόδειξη: *Θεωρούμε του δακτύλιο $R = K[z]$ και το ιδεώδες $I = zK[z]$. Από το θεώρημα 2.32 υπάρχει μία θέση $P \in \mathbb{P}_F$ με $z \in P$, οπότε P είναι μία* ***ρίζα*** *του z. Ομοίως z^{-1} έχει μία ρίζα $Q \in \mathbb{P}_F$, τότε Q είναι ένας* ***πόλος*** *του z.* □

2.2 Το Σώμα των ρητών συναρτήσεων

Για να κατανοήσουμε τις προηγούμενες έννοιες της προηγούμενης παραγράφου θα τις μελετήσουμε στην περίπτωση ***του σώματος των ρητών συναρτήσεων*** *$F = K(x)$, όπου x είναι υπερβατικό πάνω από το K. Για πολυώνυμο $p(x) \in K(x)$, ανάγωγο με μεγιστοβάθμιο συντελεστή 1 (μονικό πολυώνυμο) θεωρούμε τον δακτύλιο εκτίμησης*

$$\mathcal{O}_{p(x)} := \left\{ \frac{f(x)}{g(x)} : f(x)\,,\, g(x) \in K[x], p(x) \nmid g(x) \right\} \tag{2.19}$$

του $K(x)/K$ με μέγιστο ιδεώδες

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)} : f(x)\,,\, g(x) \in K[x],\ p(x) \mid f(x),\ p(x) \nmid g(x) \right\}. \tag{2.20}$$

Στην ειδική περίπτωση που το $p(x)$ είναι γραμμικό, δηλαδή $g(x) = x - a$ με $a \in K$ γράφουμε συντόμως

$$P_a := P_{x-a} \in \mathbb{P}_{K(x)}. \tag{2.21}$$

Υπάρχει ένας άλλος δακτύλιος εκτίμησης του $K(x)/K$, δηλαδή

$$\mathcal{O}_\infty := \left\{ \frac{f(x)}{g(x)} : f(x)\,,\, g(x) \in K[x],\ \deg f(x) \le \deg g(x) \right\}. \tag{2.22}$$

με μέγιστο ιδεώδες

$$P_\infty := \left\{ \frac{f(x)}{g(x)} : f(x)\,,\, g(x) \in K[x],\ \deg f(x) < \deg g(x) \right\}. \tag{2.23}$$

αυτό ονομάζεται άπειρη θέση του $K(x)$.

Παρατήρηση 2.36 *Οι χαρακτηριμοί που αναφέραμε παραπάνω εξαρτώνται από την ειδική επιλογή του γεννήτορα x του $K(x)/K$.*

Παράδειγμα 2.37 *$K(x) = K(1/x)$ και η άπειρη θέση με εκτίμηση στο $1/x$ είναι η θέση P_0 με εκτίμηση στο x.*

Πρόταση 2.38 *Έστω $F = K(x)$ το σώμα των ρητών συναρτήσεων.*

i. Έστω $P = P_{p(x)} \in \mathbb{P}_{K(x)}$ η θέση που ορίστηκε στην σχέση (2.20) όπου $p(x) \in K[x]$ είναι ένα ανάγωγο πολυώνυμο. Τότε $p(x)$ είναι ένα πρώτο στοιχείο του για το P, και η αντίστοιχη διακριτή εκτίμηση υ_P μπορεί να περιγραφεί ως εξής:

Αν $z \in K(x)\backslash\{0\}$ γράφεται στη μορφή $z = p(x)^n \left(\frac{f(x)}{g(x)}\right)$ με $n \in \mathbb{Z}$, $f(x)\,,\, g(x) \in K[x]$, $p(x) \nmid f(x)$ και $p(x) \nmid g(x)$ τότε $\upsilon_P(z) = n$.

Το σώμα κλάσης υπολοίπων $K(x)_P = \mathcal{O}_P/P$ είναι ισομορφικό με το $K[x]/\big(p(x)\big)$. Ο ισομορφισμός είναι

$$\phi : \begin{cases} K[x]/\big(p(x)\big) & \to & K(x)_P \\ f(x) \bmod p(x) & \mapsto & f(x)(P) \end{cases}.$$

Συνεπώς, $\deg P = \deg p(x)$.

ii. Στην ειδική περίπτωση που $p(x) = x - a$ με $a \in K$, ο βαθμός του $P = P_a$ είναι 1 και η απεικόνιση κλάσης υπολοίπων δίνεται από

$$z(P) = z(a) \quad \textit{για} \quad z \in K(x), \tag{2.24}$$

όπου $z(a)$ ορίζεται ως εξής:$z = f(x)/g(x)$ με σχετικά πρώτα πολυώνυμα $f(x)\,,\, g(x) \in K[x]$. Τότε

$$z(a) = \begin{cases} f(a)/g(a) & \textit{αν} \quad g(a) \neq 0 \\ \infty & \textit{αν} \quad g(a) = 0 \end{cases}.$$

iii. Τέλος, έστω $P = P_\infty$ είναι η άπειρη θέση του $K(x)/K$ που ορίστηκε στη σχέση (2.23). Τότε $\deg P_\infty = 1$. Ένα πρώτο στοιχείο για την P_∞ είναι το $t = 1/x$. Η αντίστοιχη δακριτή εκτίμηση δίνεται από τη σχέση

$$\upsilon_\infty\left(\frac{f(x)}{g(x)}\right) = \deg g(x) - \deg f(x) \tag{2.25}$$

όπου $f(x)\,,\, g(x) \in K[x]$. Η απεικόνιση κλάσης υπολοίπων που αντιστοιχεί στην P_∞ ορίζεται από την $z(P_\infty) = z(\infty)$ για $z \in K(x)$ όπου $z(\infty)$ ορίζεται ως εξής:

$$\text{Αν } \; z = \frac{a_n x^n + \cdots + a_0}{b_m x^m + \cdots + b_0} \;\; \text{με } \; a_n, b_m \neq 0, \tag{2.26}$$

τότε

$$z(\infty) = \begin{cases} \frac{a_n}{b_m} & \text{αν } n = m \\ 0 & \text{αν } n < m \\ \infty & \text{αν } n > m \end{cases} .$$

iv. K είναι το πλήρες σώμα σταθερών του $K(x)/K$.

Απόδειξη :

i. Έστω $P = P_\infty$, $p(x) \in K[x]$ ανάγωγο πολυώνυμο. Το ιδεώδες $P_{p(x)} \subseteq \mathcal{O}_{p(x)}$ παράγεται από το $p(x)$ οπότε το $p(x)$ είναι ένα πρώτο στοιχείο για το P. Για ν' αποδείξουμε ότι $K(x)_P$ είναι ισόμορφο με το $K[x]/\big(p(x)\big)$ θεωρούμε τον ***ομομορφισμό***

$$\varphi : \begin{cases} K[x]/\big(p(x)\big) & \to & K(x)_P \\ f(x) & \mapsto & f(x)(P) \end{cases} .$$

Ο πυρήνας της φ είναι το ιδεώδες που παράγεται από το $p(x)$. Επιπλέον η φ είναι $1-1$ και επί. Αν $z \in \mathcal{O}_{p(x)}$, μπορούμε να γράψουμε

$$z = \frac{u(x)}{\upsilon(x)} \;\; \text{με } \; u(x), \upsilon(x) \in K[x] \tag{2.27}$$

έτσι ώστε $p(x) \nmid \upsilon(x)$. Έτσι υπάρχουν $a(x), b(x) \in K[x]$ με

$$a(x)p(x) + b(x)\upsilon(x) = 1, \tag{2.28}$$

επομένως

$$\begin{aligned} z = 1z &= \Big(a(x)p(x) + b(x)\upsilon(x)\Big)\frac{u(x)}{\upsilon(x)} \\ &= \frac{a(x)u(x)}{\upsilon(x)}p(x) + b(x)u(x) \end{aligned} \tag{2.29}$$

και $z(P) = \big(b(x)u(x)\big)(P)$ είναι στην εικόνα της φ. Άρα η φ δημιουργεί έναν ισομορφισμό $\phi : K[x]/\big(p(x)\big) \to K(x)_p$.

ii. *Τώρα $P = P_a$ με $a \in K$. Αν $f(x) \in K[x]$ τότε $(x-a) \mid \big(f(x) - f(a)\big)$, όπου*

$$f(x)(P) = \big(f(x) - f(a)\big)(P) + f(a)(P) = f(a). \tag{2.30}$$

'Ενα αυθαίρετο στοιχείο $z \in \mathcal{O}_P$ μπορεί να γραφεί $z = f(x)/g(x)$ με $f(x), g(x) \in K[x]$ και $(x-a) \nmid g(x)$, επομένως $g(x)(P) = g(a) \neq 0$ και

$$z(P) = \frac{f(x)(P)}{g(x)(P)} = \frac{f(a)}{g(a)} = z(a). \tag{2.31}$$

iii. *Θα δείξουμε ότι $1/x$ είναι ένα πρώτο στοιχείο για το P_∞. Θεωρούμε κάποιο στοιχείο $z = \frac{f(x)}{g(x)} \in P_\infty$ έτσι ώστε $\deg f < \deg g$. Τότε $z = \frac{1}{x}\frac{xf}{g}$ με $\deg(xf) \leq \deg g$ οπότε $z \in \big(\frac{1}{x}\big)\mathcal{O}_\infty$ απ' όπου έπεται ότι $\frac{1}{x}$ είναι ένα πρώτο στοιχείο για το P_∞.*

iv. *Επιλέγουμε μια θέση P του $K(x)/K$ βαθμού 1 (π.χ.: $P = P_a$ με $a \in K$). Το σώμα $\widetilde{K}$ των σταθερών του $K(x)$ εμφυτεύεται στο σώμα κλάσης υπολοίπων $K(x)_P$, οπότε $K \subseteq \widetilde{K} \subseteq K(x)_P = K$.* □

Θεώρημα 2.39 *Δεν υπάρχουν άλλες θέσεις για το σώμα των ρητών συναρτήσεων $K(x)/K$ εκτός από τις θέσεις $P_{p(x)}$ και P_∞ που ορίστηκαν από τις σχέσεις (2.20) και (2.23).*

Απόδειξη: *Είναι αρκετό να δείξουμε το ακόλουθο:*

Δίνεται μία θέση $P \in \mathbb{P}_{K(x)}$, $P \neq P_\infty$, τότε υπάρχει ένα ανάγωγο πολυώνυμο $p(x) \in K[x]$ έτσι ώστε $\mathcal{O}_{p(x)} = \mathcal{O}_P$.

Πρώτη Περίπτωση:
Υποθέτουμε ότι $x \in \mathcal{O}_P$. Τότε $K[x] \subseteq \mathcal{O}_P$. Θέτουμε $I := K[x] \cap P$ αυτό είναι ένα ιδεώδες του $K[x]$ και μάλιστα πρώτο ιδεώδες. Η απεικόνιση κλάσης υπολοίπων δημιουργεί μία εμφύτευση

$$K[x]/I \hookrightarrow K(x)_P \tag{2.32}$$

συνεπώς $I \neq \{0\}$ από την πρόταση 2.28 έπεται ότι υπάρχει ένα ανάγωγο πολυώνυμο με μεγιστοβάθμιο συντελεστή 1 (μοναδικά ορισμένο) $p(x) \in K[x]$ έτσι ώστε $I = K(x) \cap P = p(x)K[x]$. Κάθε $g(x) \in K[x]$ με $p(x) \nmid g(x)$ δεν ανήκει στο I, έτσι $g(x) \notin P$ και $1/g(x) \in \mathcal{O}_P$ από την πρόταση 2.15. Συμπεραίνουμε λοιπόν ότι

$$\mathcal{O}_{p(x)} := \left\{ \frac{f(x)}{g(x)} : f(x)\,,\, g(x) \in K[x],\ p(x) \nmid g(x) \right\} \subseteq \mathcal{O}_P. \tag{2.33}$$

Ως δακτύλιοι εκτίμησης είναι μέγιστοι γνήσιοι υποδακτύλιοι του $K[x]$ (Θεώρημα 2.24) έχουμε $\mathcal{O}_P = \mathcal{O}_{p(x)}$.

Δεύτερη Περίπτωση:
Τώρα $x \notin \mathcal{O}_P$. Συμπεραίνουμε ότι

$$K[x^{-1}] \subseteq \mathcal{O}_P, \qquad x^{-1} \in P \cap K[x^{-1}] \tag{2.34}$$

και

$$P \cap K[x^{-1}] = x^{-1}K[x^{-1}]. \tag{2.35}$$

Όπως στην πρώτη περίπτωση,

$$\mathcal{O}_{p(x)} \supseteq \left\{ \frac{f(x^{-1})}{g(x^{-1})} : f(x^{-1})\,,\, g(x^{-1}) \in K[x^{-1}],\ f(x^{-1}) \nmid g(x^{-1}) \right\} =$$
$$\left\{ \frac{a_0 + a_1x^{-1} + \cdots + a_nx^{-n}}{b_0 + b_1x^{-1} + \cdots + b_mx^{-m}} :\ b_0 \neq 0 \right\} =$$

$$\left\{ \frac{a_0x^{m+n} + a_1x^{m+n-1} + \cdots + a_nx^m}{b_0x^{m+n} + b_1x^{m+n-1} + \cdots + b_mx^n} :\ b_0 \neq 0 \right\} =$$
$$\left\{ \frac{u(x)}{v(x)} :\ u(x)\,,\, v(x) \in K[x],\ \deg u(x) \leq \deg v(x) \right\} = \mathcal{O}_\infty.$$

Έτσι $\mathcal{O}_P = \mathcal{O}_\infty$ *και* $P = P_\infty$. □

Πόρισμα 2.40 *Οι θέσεις του* $K(x)/K$ *βαθμού 1 είναι σε* $1-1$ *αντιστοιχία με το* $K \cup \{\infty\}$.

Σχόλιο 2.41 *Στο προηγούμενο πόρισμα όταν λέμε* $\{\infty\}$ *θεωρούμε το* ∞ *σαν σημείο.*

2.3 Διαιρέτες

Από εδώ και στο εξής το F/K *θα θεωρείται ως ένα αλγεβρικό σώμα συναρτήσεων μίας μεταβλητής έτσι ώστε το* K *να είναι το πλήρες σώμα των σταθερών του* F/K.

Ορισμός 2.42 *Η ελεύθερη αβελιανή ομάδα η οποία παράγεται από τις θέσεις του* F/K *συμβολίζεται με* $\mathcal{D}_F$ *και λέγεται* ***ομάδα των διαιρετών του*** $\boldsymbol{F/K}$. *Τα στοιχεία του* $\mathcal{D}_F$ *λέγονται* ***διαιρέτες*** *του* F/K.

Με άλλα λόγια ένας διαιρέτης είναι ένα τυπικό άθροισμα της μορφής

$$D = \sum_{P \in \mathbb{P}_F} n_P P \ \text{ με } n_P \in \mathbb{Z} \text{ σχεδόν όλα ίσα με } 0.$$

Ορισμός 2.43 *Ο* ***φορέας*** *του* D *ορίζεται ως εξής*

$$\operatorname{supp} D := \{P \in \mathbb{P}_F : n_P \neq 0\}.$$

Πολλές φορές είναι βολικό να γράφουμε

$$D = \sum_{P \in S} n_P P,$$

όπου το $S \subseteq \mathbb{P}_F$ *είναι ένα πεπερασμένο σύνολο με* $\operatorname{supp} D \subseteq S$.

Ορισμός 2.44

i. *Ένας διαιρέτης της μορφής $D = P$ με $P \in \mathbb{P}_F$ ονομάζεται* ***πρώτος διαιρέτης***.

ii. *Δύο διαιρέτες $D = \sum n_P P$ και $D' = \sum n'_P P$ προσθέτονται με τον εξής τρόπο*

$$D + D' = \sum_{P \in \mathbb{P}_F} (n_P + n'_P)P.$$

iii. *Το* ***μηδενικό στοιχείο*** *της ομάδας των διαιρετών $\mathcal{D}_F$ είναι ο διαιρέτης*

$$0 := \sum_{P \in \mathbb{P}_F} r_P P \text{ με όλα τα } r_P = 0.$$

iv. *Για $Q \in \mathbb{P}_F$ και $D = \sum n_P P \in \mathcal{D}_F$ ορίζουμε*

$$\upsilon_Q(D) := n_Q.$$

Επομένως

$$\operatorname{supp} D := \{P \in \mathbb{P}_F : \upsilon_P(D) \neq 0\}$$

και

$$D = \sum_{P \in \operatorname{supp} D} \upsilon(D) \cdot P.$$

v. *Μία* ***μερική διάταξη*** *στο $\mathcal{D}_F$ ορίζεται ως εξής*

$$D_1 \leq D_2 \iff \upsilon(D_1) \leq \upsilon(D_2),\ \forall\, P \in \mathbb{P}_F.$$

vi. *Ένας διαιρέτης $D \geq 0$ καλείται* ***θετικός*** *(effective).*

vii. *Ο βαθμός ενός διαιρέτη ορίζεται μέσω της σχέσης*

$$\deg D := \sum_{P \in \mathbb{P}_F} \upsilon_P(D) \cdot \deg P$$

η οποία παράγει τον ακόλουθο ομομορφισμό

$$\deg : \mathcal{D}_F \to \mathbb{Z}.$$

Ορισμός 2.45 *Έστω $0 \neq x \in F$. Ας συμβολίσουμε με $\mathcal{Z}$ το σύνολο των* ***ριζών*** *και με $\mathcal{N}$ το σύνολο των* ***πόλων*** *του x στο $\mathbb{P}_F$. Τότε ορίζουμε*

i. *του* ***μηδενικό διαιρέτη*** *του x μέσω της σχέσης*

$$(x)_0 := \sum_{P \in \mathcal{Z}} \upsilon_P(x)P, \tag{2.36}$$

ii. *του* ***πόλο διαιρέτη*** *του x μέσω της*

$$(x)_\infty := \sum_{P \in \mathcal{N}} \big(-\upsilon(x)\big)P, \tag{2.37}$$

iii. τον ***κύριο διαιρέτη*** *του x μέσω της*

$$(x) := (x)_0 - (x)_\infty. \tag{2.38}$$

Προφανώς

$$(x)_0 \geq 0,\ (x)_\infty \geq 0,\ (x) = \sum_{P\in\mathbb{P}_F} v(x)P. \tag{2.39}$$

Τα στοιχεία του $x(\neq 0) \in F$ τα οποία είναι σταθερά χαρακτηρίζονται ως εξής

$$x \in F \Rightarrow (x) = 0.$$

Παράδειγμα 2.46 *Να βρεθούν οι divisors και ο βαθμός τους, της συνάρτησης*

$$\frac{(x-5)(x-6)}{3x^7}.$$

Απόδειξη:

$$\begin{aligned} v_{(x=5)}\left(\tfrac{(x-5)(x-6)}{3x^7}\right) &= 1\\ v_{(x=6)}\left(\tfrac{(x-5)(x-6)}{3x^7}\right) &= 1\\ v_{(x=0)}\left(\tfrac{(x-5)(x-6)}{3x^7}\right) &= -7 \end{aligned}$$

$$\begin{aligned} v_\infty\left(\tfrac{(x-5)(x-6)}{3x^7}\right) &= v_\infty\big((x-5)(x-6)\big) + v_\infty(3x^7)\\ &= v_\infty(x-5) + v_\infty(x-6) + v_\infty(3x^7)\\ &= 2 - 7 = -5 \end{aligned}$$

$$(F) = 1\cdot P_{(x=5)} + 1\cdot P_{(x=6)} - 7\cdot P_{(x=0)} + 5\cdot P_{x=\infty}$$

$$\textit{Άρα}\ \ \deg(F) = 0.$$

□

Ορισμός 2.47 *Το σύνολο*

$$P_F := \big\{(x) : x(\neq 0) \in F\big\}$$

ονομάζεται ***ομάδα κυρίων διαιρετών του F/K***.

Πρόταση 2.48 *Η ομάδα κυρίων διαιρετών του F/K είναι μία υποομάδα του $\mathcal{D}_F$ εφόσον για $0 \neq x, y \in F$ ισχύει ότι*

$$(x\cdot y) = (x) + (y).$$

Απόδειξη:

$$\begin{aligned} (x\cdot y) &= \textstyle\sum_{P\in\mathbb{P}_F} v_P(xy)P &&=\\ &= \textstyle\sum_{P\in\mathbb{P}_F} \big(v_P(x) + v_P(y)\big)P &&=\\ &= \textstyle\sum_{P\in\mathbb{P}_F} v_P(x)P + \sum_{P\in\mathbb{P}_F} v_P(y)P &&=\\ &= (x) + (y). \end{aligned}$$

□

Ορισμός 2.49 *Η ομάδα πηλίκο $\mathcal{C}_F := \mathcal{D}_F/\mathcal{P}_F$ ονομάζεται* ***ομάδα κλάσης διαιρετών****. Για ένα διαιρέτη $D \in \mathcal{D}_F$, το αντίστοιχο στοιχείο στην ομάδα πηλίκο $\mathcal{C}_F$ συμβολίζεται με $[D]$, ο διαιρέτης κλάσης του D.*

Ορισμός 2.50 *Δύο διαιρέτες $D, D' \in \mathcal{D}_F$ είναι ισοδύναμοι (συμβ. $D \sim D'$) αν $[D] = [D']$, δηλαδή $D = D' + (x)$ για κάποια $x \in F \setminus \{0\}$.*

Σημείωση 2.51 *Η σχέση $\sim$ του προηγούμενου ορισμού είναι σχέση ισοδυναμίας αφού ισχύουν τα ακόλουθα*

- $\triangle$ *$[D] = [D']$ άρα $D \sim D'$ προφανώς ισχύει η* ***ανακλαστική*** *ιδιότητα.*
- $\triangle$ *Αν $D \sim D'$ τότε $[D] = [D'] \Rightarrow [D'] = [D]$, επομένως $D' \sim D$. Άρα ισχύει η* ***συμμετρική*** *ιδιότητα.*
- $\triangle$ *Αν $D \sim D'$ και $D' \sim D''$ τότε $[D] = [D']$ και $[D'] = [D''] \Rightarrow [D] = [D'']$, επομένως $D \sim D''$. Άρα ισχύει η* ***μεταβατική*** *ιδιότητα.*

Ορισμός 2.52 *Για έναν διαιρέτη $A \in \mathcal{D}_F$ θέτουμε*

$$\mathcal{L}(A) := \{x \in F : (x) \geq -A\} \cup \{0\}.$$

Παρατήρηση 2.53 *Ο προηγούμενος ορισμός μας λέει ότι αν*

$$A = \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j \quad n_i, m_j > 0$$

τότε το $\mathcal{L}(A)$ περιέχει όλα τα στοιχεία $x \in F$ έτσι ώστε

i. *το x έχει ρίζες τάξης μεγαλύτερης ή ίσης του m_j στα Q_j για $j = 1, 2, \ldots, s$ και*

ii. *το x μπορεί να έχει πόλους μόνο στις θέσεις $P_1, P_2, \ldots, P_r$ με την τάξη πόλου στα P_i να φράσεται από τα n_i $(i = 1, 2, \ldots, r)$.*

Σχόλια 2.54 *Έστω ότι $A \in \mathcal{D}_F$. Τότε*

i. *το $x \in \mathcal{L}(A)$ αν και μόνο αν $\upsilon_P(x) \geq -\upsilon_P(A)$ για όλα τα $P \in \mathbb{P}_F$*

ii. *το $\mathcal{L}(A) \neq \{0\}$ αν και μόνο αν υπάρχει ένας διαιρέτης $A \sim A'$ με $A' \geq 0$.*

Απόδειξη:

i. *Εφόσον $x \in \mathcal{L}(A) \Leftrightarrow x \in F$ όπου*

$$\begin{array}{rcccl} (x) \geq -A & \Leftrightarrow & \sum \upsilon_P(x)P & \geq & -\sum \upsilon_P(A)P \\ & \Leftrightarrow & \upsilon_P(x) & \geq & -\upsilon_P(A). \end{array}$$

ii. *(⟹)*
Αν $\mathcal{L}(A) \neq \{0\}$ *τότε υπάρχει* $x \in \mathcal{L}(A)$ *με* $(x) \geq -A$. *Άρα* $A' = (x)+A \geq 0$.
(⟸)
Αν $A \sim A'$ *τότε υπάρχει διαιρέτης* $x \in F\backslash\{0\}$ *έτσι ώστε* $A' = (x) + A \geq 0$.
Άρα $x \in \mathcal{L}(A)$ *αφού* $(x) \geq -A$.
□

Λήμμα 2.55 *Έστω ότι* $A \in \mathcal{D}_F$. *Τότε έχουμε ότι*

i. *Το* $\mathcal{L}(A)$ *είναι διανυσματικός χώρος πάνω από το* K.

ii. *Αν* A' *είναι ένας διαιρέτης ισοδύναμος του* A *τότε* $\mathcal{L}(A) \simeq \mathcal{L}(A')$ *(ισόμορφοι ως διανυσματικοί χώροι πάνω από το* K*).*

Απόδειξη :

i. *Έστω ότι* $x, y \in \mathcal{L}(A)$ *και* $a \in K$. *Τότε για κάθε* $P \in \mathbb{P}_F$ *θα είναι*

$$\upsilon_P(x+y) \geq \min\left\{\upsilon_P(x), \upsilon_P(y)\right\} \geq -\upsilon_P(A)$$

(μέσω του σχολίου 2.54.i) και

$$\upsilon_P(ax) = \upsilon_P(a) + \upsilon_P(x) = 0 + \upsilon_P(x) \geq -\upsilon_P(A)$$

(επίσης μέσω του σχολίου 2.54.i). Άρα $x+y$ *και* ax *ανήκουν στο* $\mathcal{L}(A)$. *Επομένως το* $\mathcal{L}(A)$ *είναι ένας διανυσμαικός χώρος.*

ii. *Αν* $A \sim A'$ *τότε* $A = A' + (z)$ *με* $z \in F\backslash\{0\}$. *Θεωρούμε την απεικόνιση*

$$\varphi : \left\{ \begin{array}{ccc} \mathcal{L}(A) & \to & F \\ x & \mapsto & xz \end{array} \right.$$

και έστω ότι $x, y \in \mathcal{L}(A)$ *και* $a \in K$. *Τότε*

$$\varphi(x+y) = (x+y)z = xz + yz = \varphi(x) + \varphi(y)$$

και

$$\varphi(ax) = (ax)z = a(xz) = a\,\varphi(x)$$

Άρα η φ *είναι* K*-γραμμική και η εικόνα της περιέχεται στο* $\mathcal{L}(A')$. *Ομοίως η απεικόνιση*

$$\varphi' : \left\{ \begin{array}{ccc} \mathcal{L}(A') & \to & F \\ x & \mapsto & xz^{-1} \end{array} \right.$$

είναι K*-γραμμική από το* $\mathcal{L}(A')$ *στο* $\mathcal{L}(A)$. *Οι απεικονίσεις* φ *και* φ' *είναι η μία αντίστροφη της άλλης, άρα η* φ *είναι ισομορφισμός μεταξύ των* $\mathcal{L}(A)$ *και* $\mathcal{L}(A')$.
□

Ορισμός 2.56 *Για έναν διαιρέτη $A \in \mathcal{D}_F$, ο ακέραιος $\dim A := \dim \mathcal{L}(A)$ καλείται η διάσταση του διαιρέτη A.*

Πρόταση 2.57 *Ισοδύναμοι διαιρέτες έχουν τον ίδιο βαθμό και την ίδια διάσταση, έστω $A' \sim A$ με $A, A' \in D_F$ ισχύει $\deg A = \deg A'$ και $\dim A = \dim A'$.*

Απόδειξη: *Έχουμε $A' \sim A \Rightarrow A = A + (x)$ $\big((x)$ κύριος διαιρέτης$\big)$ επομένως $\deg A' = \deg\big(A + (x)\big) = \deg A + \deg(x) = \deg A$. Τώρα για τη διάσταση ισχύει ότι $\dim A := \dim \mathcal{L}(A)$ επομένως $\mathcal{L}(D) = \{f : (f)+D \geq 0\}$ και ο πολλαπλασιαμός με x ορίζει έναν ισομορφισμό στους διανυσματικούς χώρους*

$$\begin{array}{ccc} \mathcal{L}(A) & \longrightarrow & \mathcal{L}\big(A + (x)\big) \\ f & \longmapsto & f + (x) \end{array}$$

και από τις δυώσεις μας στην άλγεβρα ισόμορφοι διανυσματικοί χώροι έχουν την ίδια διάσταση. Άρα $\dim A = \dim A'$. □

Λήμμα 2.58 *Ισχύουν τα ακόλουθα*

i. $\mathcal{L}(0) = K$.

ii. Αν $A < 0$ τότε $\mathcal{L}(A) = \{0\}$.

Απόδειξη:

i. Αν $(x) = 0$ τότε $0 \neq x \in K$ και κατά συνέπεια $K \subseteq \mathcal{L}(0)$.

Αντιστρόφως *αν $0 \neq x \in \mathcal{L}(0)$ τότε $(x) \geq 0$. Αυτό σημαίνει ότι το x δεν έχει πόλους, άρα από το πόρισμα 2.35, $x \in K$ επομένως $\mathcal{L}(0) \subseteq K$. Άρα $\mathcal{L}(0) = K$.*

ii. Υποθέτουμε ότι υπάρχει ένα στοιχείο $0 \neq x \in \mathcal{L}(A)$. Τότε $(x) \geq -A > 0$ (εφόσον $A < 0$) οπότε το x ***έχει τουλάχιστο μία ρίζα*** *αλλά* ***δεν έχει πόλους****, το οποίο όμως είναι αδύνατο. Άρα δεν υπάρχει $x \neq 0$ με $x \in \mathcal{L}(A)$, οπότε $\mathcal{L}(A) = \{0\}$.*

□

Στη συνέχεια θέλουμε να αποδείξουμε ότι ο $\mathcal{L}(A)$ είναι πεπερασμένης διάστασης για κάθε $A \in D_F$. Με $\dim V$ θα συμβολίζουμε απο εδώ και στο εξής την διάσταση ενός διανυσμαικού χώρου V.

Λήμμα 2.59 *Έστω A, B διαιρέτες του F/K με $A \leq B$. Τότε έχουμε ότι $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ και $\dim\big[\mathcal{L}(B)/\mathcal{L}(A)\big] \leq \deg B - \deg A$.*

Απόδειξη: *Αν $x \in \mathcal{L}(A)$ τότε $(x) \geq -A \geq -B$. Άρα $x \in \mathcal{L}(B)$ και έτσι $\mathcal{L}(A) \subseteq \mathcal{L}(B)$.*
Για να αποδείξουμε την δεύτερη σχέση θα υποθέσουμε αρχικά ότι $B = A + P$ για

κάποια $P \in \mathbb{P}_F$. Διαλέγουμε ένα στοιχείο $t \in F$ με $v_P(t) = v_P(B) = v_P(A) + 1$. Για $x \in \mathcal{L}(B)$ έχουμε

$$(x) \geq -B \Leftrightarrow v_P(x) \geq -v_P(B) = v_P(t)$$

απ' όπου

$$v_P(x) + v_P(t) \geq 0 \Leftrightarrow v_P(xt) \geq 0$$

και έτσι $xt \in \mathcal{O}_P$. Άρα έχουμε μία Κ-γραμμική απεικόνιση

$$\psi : \begin{cases} \mathcal{L}(B) & \to & F_P \\ x & \mapsto & (xt)(P) \end{cases} .$$

Το $x \in \mathrm{Ker}(\psi)$ αν και μόνο αν

$$\begin{aligned} v_P(xt) > 0 \quad &\Leftrightarrow \quad v_P(x) + v_P(t) > 0 \\ &\Leftrightarrow \quad v_P(x) > -v_P(t) = -v_P(B) = -v_P(A) - 1 \end{aligned}$$

δηλαδή $v_P(x) \geq -v_P(A)$. Άρα $\mathrm{Ker}(\psi) = \mathcal{L}(A)$ και η ψ δίνει μία Κ-γραμμική $1-1$ απεικόνιση από το $\mathcal{L}(B)/\mathcal{L}(A)$ στο $\mathbb{F}_P$. Οπότε

$$\dim \left[\mathcal{L}(B)/\mathcal{L}(A)\right] \leq \dim F_P = \deg B - \deg A$$ □

2.4 Το θεώρημα Riemman - Roch

Θεώρημα 2.60 (Riemman - Roch) *Έστω F ένα αλγεβρικό σώμα συναρτήσεων. Υπάρχει ένας διαιρέτης W ο οποίος λέγεται κανονικός διαιρέτης και για κάθε $A \in \mathcal{D}_F$ ικανοποιεί την σχέση*

$$\dim \mathcal{L}(A) = \deg A + 1 - g + \dim(W - A) \tag{2.40}$$

για έναν αριθμό g που λέγεται γένος του αλγεβρικού σώματος F.

Για την απόδειξη του θεωρήματος παραπέμπουμε στο βιβλίο [HENS], σελίδα 28.

Παρατήρηση 2.61 *Στον προηγούμενο ορισμό είπαμε ότι $\dim A := \dim \mathcal{L}(A)$, συνεπώς η σχέση (2.40) γίνεται*

$$\dim A = \deg A + 1 - g + \dim(W - A). \tag{2.41}$$

Πόρισμα 2.62 *Για έναν κανονικό διαιρέτη W, έχουμε*

$$\deg W = 2g - 2 \quad \text{και} \quad \dim W = g.$$

Απόδειξη: *Για διαιρέτη $A = 0$ η διάσταση του διανυσματικού χώρου $\dim \mathcal{L}(0) = \dim 0 = 1$, συνεπώς από την σχέση (2.41) έχουμε*

$$1 = \deg 0 + 1 - g + \dim W \Longrightarrow \dim W = g$$

και επειδή βρήκαμε ότι $\dim W = g$ *πάλι από το θεώρημα Riemman - Roch για* $A = W$ *έχουμε*

$$g = \deg W + 1 - g + \dim(W - W) \Longrightarrow \deg W = 2g - 2.$$

□

Για την απόδειξη του επόμενου θεωρήματος θα χρειαστούμε την ακόλουθη πρόταση.

Πρόταση 2.63 *Έστω* $A \in \mathcal{D}_F$. *Αν* $\deg A < 0$ *τότε* $\dim A = 0$.

Απόδειξη: *Έστω ότι* $\dim A > 0$ *από το σχόλιο (2.54) υπάρχει ένας θετικός διαιρέτης* $A' \sim A$ *επομένως* $\deg A = \deg A' \geq 0$, *άτοπο διότι έχουμε υποθέσει ότι* $\deg A < 0$. *Άρα αν* $\deg A < 0$ *τότε* $\dim A = 0$. □

Θεώρημα 2.64 *Αν* A *είναι ένας διαιρέτης του* F/K *βαθμού* $\deg A \geq 2g - 1$ *τότε*

$$\dim A = \deg A + 1 - g.$$

Απόδειξη: *Από το θεώρημα Riemman - Roch ισχύει*

$$\dim A = \deg A + 1 - g + \dim(W - A)$$

όπου W *είναι ένας κανονικός διαιρέτης. Για να αποδείξουμε το ζητούμενο αρκεί να δείξουμε ότι* $\dim(W - A) = 0$. *Επειδή* $\deg W = 2g - 2$ *και* $\deg A \geq 2g - 1$ *έχουμε ότι* $\deg(W - A) < 0$, *συνεπώς από την πρόταση (2.63)* $\dim(W - A) = 0$. □

Παράδειγμα 2.65 *Αν το* $g = 0$ *και* $A > 0$ *από το θεώρημα Riemman - Roch έχουμε ότι*

$$\mathcal{L}\left(\sum n_i P_i\right) = \sum n_i + 1.$$

Απόδειξη:

$$\begin{aligned} \dim \mathcal{L}\left(\sum n_i P_i\right) &= \deg \sum n_i P_i + 1 - g + \dim\left(W - \sum n_i P_i\right) \\ &= \deg \sum n_i P_i + 1 \\ &= \sum n_i + 1 \end{aligned}$$

□

ΚΕΦΑΛΑΙΟ 3

Αλγεβρικές καμπύλες και αλγεβρικά σώματα συναρτήσεων

Στο κεφάλαιο αυτό θεωρούμε ότι το K είναι ένα αλγεβρικά κλειστό σώμα.

3.1 Αφινική πολλαπλότητα

Ορισμός 3.1 *Ο n-διάστατος* ***αφινικός χώρος*** $\mathbb{A}^n = \mathbb{A}^n(K)$ *είναι ένα σύνολο που αποτελείται απ' όλες τις n-άδες των στοιχείων του K.*

Σημείωση 3.2 *Θα λέμε ότι ένα στοιχείο $P := (a_1, \ldots, a_n) \in \mathbb{A}^n$ είναι ένα σημείο και $a_1, \ldots, a_n$ είναι οι συντεταγένες του P.*

Ορισμός 3.3 *Έστω $K[x_1, \ldots, x_n]$ ο δακτύλιος πολυωνύμων με συντελεστές από το K. Ένα υποσύνολο $V \subseteq \mathbb{A}^n$ καλείται* ***αλγεβρικό σύνολο*** *αν υπάρχει σύνολο $M \subseteq K[x_1, \ldots, x_n]$ τέτοιο ώστε*

$$V = \big\{P \in \mathbb{A}^n \big| F(P) = 0 \,\forall\, F \in M\big\}.$$

Ορισμός 3.4 *Μία προσθετική υποομάδα I του δακτυλίου $K[x_1, \ldots, x_n]$ καλείται* ***ιδεώδες*** *αν για κάθε $r \in K[x_1, \ldots, x_n]$ και για κάθε $x \in I$ το $rx \in I$.*

Πρόταση 3.5 *Έστω ένα αλγεβρικό σύνολο $V \subset \mathbb{A}^n$, το σύνολο των πολυωνύμων*

$$I(V) = \big\{F \in K[x_1, \ldots, x_n] \big| F(P) = 0 \,\forall\, P \in V\big\}$$

είναι ιδεώδες του $K[x_1, \ldots, x_n]$ και μπορεί να παραχθεί από πεπερασένα το πλήθος πολυώνυμα, $F_1, \ldots, F_r \in K[x_1, \ldots, x_n]$, επομένως έχουμε

$$V = \big\{P \in \mathbb{A}^n \big| F_1(P) = \cdots = F_r(P) = 0\big\}.$$

Ορισμός 3.6 *Ένα αφινικό αλγεβρικό σύνολο V καλείται* ***ανάγωγο*** *αν δεν μπορεί να γραφεί σαν ένωση δύο μη κενών αλγεβρικών υποσυνόλων του V, δηλαδή αν δεν υπάρχει $V_1, V_2 \subseteq V$ τέτοια ώστε $V = V_1 \cup V_2$.*

Σχόλιο 3.7 *Μπορούμε να πούμε ότι το αφινικό αλγεβρικό σύνολο V είναι ανάγωγο αν και μόνο αν το ιδεώδες $I(V)$ είναι* ***πρώτο****, δηλαδή αν $P_1, P_2 \in I(V)$ με $P_1 \cdot P_2 \in I(V)$ τότε ή $P_1 \in I(V)$ ή $P_2 \in I(V)$.*

Ορισμός 3.8 *Μία* ***αφινική πολλαπλότητα*** *είναι ένα ανάγωγο αλγεβρικό σύνολο.*

Όπως αναφέραμε προηγουμένως, $I(V)$ είναι ιδεώδες του $K[x_1, \ldots, x_n]$ συνεπώς μπορούμε να ορίσουμε τον δακτύλιο πηλίκο του $K[x_1, \ldots, x_n]$ να είναι

$$\Gamma(V) := K[x_1, \ldots, x_n]/I(V).$$

Παρατήρηση 3.9 *Επειδή η αφινική πολλαπλότητα $V \subseteq \mathbb{A}^n$, εξ' ορισμού, είναι ένα ανάγωγο αλγεβρικό σύνολο έπεται ότι το ιδεώδες $I(V)$ είναι πρώτο συνεπώς $\Gamma(V)$ είναι ακέραια περιοχή. Άρα*

$$\Gamma(V) = \big\{ f = F + I(V) \big| F \in K[x_1, \ldots, x_n] \big\},$$

ορίζεται η απεικόνιση

$$\begin{cases} f : V & \longrightarrow & K \\ \quad P & \longmapsto & F(P) \end{cases}$$

Ορισμός 3.10 *Το σώμα $K(V) := Quot\big(\Gamma(V)\big)$ καλείται* ***σώμα των ρητών συναρτήσεων*** *του V και περιέχει το K σαν υπόσωμα, δηλαδή $K \subset K(V)$.*

Ορισμός 3.11 *Έστω $K(V)/K$ είναι μία επέκταση σωμάτων. Ένα πεπερασμένο υποσύνολο $\{g_1/h_1, \ldots, g_n/h_n\} \in K(V)$ καλείται* ***αλγεβρικά ανεξάρτητο*** *υπεράνω του K αν δεν υπάρχουν μη μηδενικά πολυώνυμα $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$ τέτοια ώστε $f\big(g_1/h_1, \ldots, g_n/h_n\big) = 0$.*

Παρατήρηση 3.12 *Ένα υποσύνολο $S \subseteq K(V)$ είναι αλγεβρικά ανεξάρτητο υπεράνω του K αν όλα τα πεπερασμένα υποσύνολά του είναι αλγεβρικά ανεξάρτητα υπεράνω του K.*

Ορισμός 3.13

i. *Μία* ***βάση υπερβατικότητας*** *του $K(V)/K$ είναι ένα μέγιστο αλγεβρικό υποσύνολο του $K(V)$.*

ii. *Δύο βάσεις υπερβατικότητας έχουν τον ίδιο πληθικό αριθμό που λέγεται* ***βαθμός υπερβατικότητας*** *του $K(V)/K$.*

Ορισμός 3.14 *Η* ***διάσταση*** *μίας αφινικής πολλαπλότητας V είναι ο βαθμός υπερβατικότητας του $K(V)/K$.*

Για ένα σημείο $P \in V$ θεωρούμε του τοπικό δακτύλιο της V στο P

$$\mathcal{O}_P(V) = \left\{ f \in K(V) \middle| f = \frac{g}{h},\ g, h \in \Gamma(V) \text{ και } h(P) \neq 0 \right\}$$

με σώμα πηλίκο $K(V)$ που έχει μοναδικό μέγιστο ιδεώδες το σύνολο

$$M_P(V) = \left\{ f \in K(V) \middle| f = \frac{g}{h},\ g, h \in \Gamma(V), h(P) \neq 0 \text{ και } g(P) = 0 \right\}.$$

3.2 Προβολική πολλαπλότητα

Ορίζουμε στο σύνολο $\mathbb{A}^{n+1} \setminus \{(0, \ldots, 0)\}$ μία σχέση ισοδυναμίας $\sim$ η οποία δίνεται από

$$(a_0, \ldots, a_n) \sim (b_0, \ldots, b_n) \iff \exists\, 0 \neq \lambda \in K \text{ τέτοιο ώστε } b_i = \lambda a_i,\ i = 1, \ldots, n.$$

Η κλάση ισοδυναμίας του $(a_0, \ldots, a_n)$ με την σχέση ισοδυναμίας $\sim$ συμβολίζετε με $(a_0 : \cdots : a_n)$.

Ορισμός 3.15 *Ο n-διάστατος **προβολικός χώρος** $\mathbb{P}^n = \mathbb{P}^n(K)$ είναι ένα σύνολο που αποτελείται από όλες τις κλάσεις ισοδυναμίας, δηλαδή*

$$\mathbb{P}^n = \left\{ (a_0 : \cdots : a_n) \middle| a_i \in K,\ \text{όχι όλα τα } a_i = 0 \right\}.$$

Σημείωση 3.16 *Θα λέμε ότι ένα στοιχείο $P := (a_0 : \cdots : a_n) \in \mathbb{P}^n$ είναι ένα σημείο και τα $a_0, \ldots, a_n$ θα είναι οι ομογενείς συντεταγμένες του P.*

Ορισμός 3.17

i. Ένα μονόνυμο βαθμού d είναι ένα πολυώνυμο $G \in K[x_0, \ldots, x_n]$ της μορφής

$$G = a \cdot \prod_{i=0}^{n} x_i^{d_i},\ \text{με } a \in K \text{ και } \sum_{i=0}^{n} d_i = d.$$

*ii. Ένα πολυώνυμο F καλείται **ομογενές πολυώνυμο** αν το F είναι άθροισμα μονονύμων του ίδιου βαθμού.*

*iii. Ένα ιδεώδες $I \subseteq K[x_0, \ldots, x_n]$ το οποίο γεννάται από ομογενή πολυώνυμα καλείται **ομογενές ιδεώδες**.*

Πρόταση 3.18 *Έστω ένα ομογενές πολυώνυμο $F \in K[x_0, \ldots, x_n]$. Για κάθε $P = (a_0 : \cdots : a_n) \in \mathbb{P}^n$*

$$F(P) = 0 \iff F(a_0, \ldots, a_n) = 0 \iff F(\lambda a_0, \ldots, \lambda a_n) = 0.$$

Απόδειξη:

$$F(\lambda a_0, \ldots, \lambda a_n) \overset{\text{ομογενές}}{=}{}^{F} \lambda^d \cdot F(a_0, \ldots, a_n) = \lambda^d \cdot 0 = 0,$$

όπου $d = \deg F$. □

Ορισμός 3.19 *Ένα υποσύνολο $V \subseteq \mathbb{P}^n$ είναι ένα* ***προβολικό αλγεβρικό σύνολο*** *αν υπάρχει ένα σύνολο από ομογενή πολυώνυμα $M \subseteq K[x_0, \ldots, x_n]$ τέτοιο ώστε*

$$V = \big\{P \in \mathbb{P}^n \big| F(P) = 0 \,\forall\, F \in M\big\}.$$

Ορισμός 3.20 *Το ιδεώδες $I(V) \subseteq K[x_0, \ldots, x_n]$ το οποίο γεννάται από ομογενή πολυώνυμα F με $F(P) = 0 \,\forall\, P \in V$ καλείται* ***ομογενές ιδεώδες*** *του V.*

Ορισμός 3.21 *Ένα προβολικό αλγεβρικό σύνολο V καλείται* ***ανάγωγο*** *αν δεν μπορεί να γραφεί σαν ένωση δύο μη κενών αλγεβρικών υποσυνόλων του V, δηλαδή αν δεν υπάρχουν $V_1, V_2 \subseteq V$ τέτοια ώστε $V = V_1 \cup V_2$.*

Σχόλιο 3.22 *Μπορούμε να πούμε ότι το προβολικό αλγεβρικό σύνολο V είναι ανάγωγο αν και μόνο αν το ομογενές ιδεώδες του $I(V)$ είναι* ***πρώτο*** *στο $K[x_0, \ldots, x_n]$.*

Ορισμός 3.23 *Μία* ***προβολική πολλαπλότητα*** *είναι ένα ανάγωγο προβολικό αλγεβρικό σύνολο.*

Όπως και στην αφινική πολλαπλότητα επειδή $I(V)$ είναι ένα ομογενές πρώτο ιδεώδες του $K[x_0, \ldots, x_n]$ μπορούμε και πάλι να ορίσουμε του δακτύλιο πηλίκο του $K[x_1, \ldots, x_n]$ να είναι

$$\Gamma_h(V) := K[x_0, \ldots, x_n].$$

Παρατήρηση 3.24 *Επειδή η προβολική πολλαπλότητα $V \subseteq \mathbb{P}^n$, εξ' ορισμού, είναι ένα ανάγωγο, προβολικό αλγεβρικό σύνολο έπεται ότι το ιδεώδες $I(V)$ είναι ομογενές πρώτο ιδεώδες συνεπώς $\Gamma_h(V)$ είναι ακέραια περιοχή. Άρα*

$$\Gamma_h(V) = \big\{f = F + I(V) \big| F \in K[x_0, \ldots, x_n]\big\}$$

όπου $F \in K[x_0, \ldots, x_n]$ ομογενές πολυώνυμο βαθμού $\deg F = d$.

Ορισμός 3.25 *Το σώμα των ρητών συναρτήσεων της $V \subseteq \mathbb{P}^n$ ορίζεται ως*

$$K(V) := \left\{ \frac{g}{h} \middle| \, g, h \in \Gamma_h(V) \text{ είναι στοιχεία του ίδιου βαθμού και } h \neq 0 \right\}$$

και είναι υπόσωμα του $Quot\big(\Gamma_h(V)\big)$.

Ορισμός 3.26 *Η* ***διάσταση*** *μιας προβολικής πολλαπλότητας V είναι ο βαθμός υπερβατικότητας του $K(V)/K$.*

Θέτουμε P να είναι ένα σημείο της προβολικής πολλαπλότητας $V \in \mathbb{P}^n$, $P = (a_0 : \cdots : a_n) \in V$ και $f \in K(V)$. Γράφουμε $f = g/h$ όπου $g = G + I(V) \in \Gamma_h(V)$ και $h = H + I(V) \in \Gamma_h(V)$ και $G, H \in K[x_0, \ldots, x_n]$ είναι ομογενή πολυώνυμα βαθμού d.

Για $0 \neq \lambda \in K$ ισχύει

$$\frac{G(\lambda a_0, \ldots, \lambda a_n)}{H(\lambda a_0, \ldots, \lambda a_n)} = \frac{\lambda^d \cdot G(a_0, \ldots, a_n)}{\lambda^d \cdot H(a_0, \ldots, a_n)} = \frac{G(a_0, \ldots, a_n)}{H(a_0, \ldots, a_n)},$$

μπορούμε τώρα να θέσουμε

$$f(P) = \frac{G(a_0, \ldots, a_n)}{H(a_0, \ldots, a_n)} \in K,$$

αν $H(P) \neq 0$. *Μπορούμε συνεπώς να πούμε ότι η* f *ορίζεται στο* P *και* $f(P)$ *είναι η τιμή της* f *στο* P.

Για ένα σημείο $P \in V$ *θεωρούμε του τοπικό δακτύλιο της* V *στο* P

$$\mathcal{O}_P(V) = \big\{ f \in K(V) \big| \; f \text{ ορίζεται στο } P \big\}$$

με μέγιστο ιδεώδες

$$M_P(V) = \big\{ f \in \mathcal{O}_P(V) \big| \; f(P) = 0 \big\}.$$

3.3 Κάλυμμα προβολικής πολλαπλότητα με αφινική πολλαπλότητα

Για $0 \leq i \leq n$ *ορίζουμε μια απεικόνιση* $\varphi_i : \mathbb{A}^n \to \mathbb{P}^n$ *με*

$$\varphi_i(a_0, \ldots, a_n) = \big(a_0 : \cdots : a_{i-1} : 1 : a_i : \cdots : a_{n-1}\big)$$

Η φ_i *είναι μία* $1 - 1$ *και επί απεικόνιση από του* $\mathbb{A}^n$ *στο σύνολο*

$$U_i = \big\{ (c_0 : \cdots : c_n) \in \mathbb{P}^n \big| \; c_i \neq 0 \big\}$$

και ο προβολικός χώρος $\mathbb{P}^n$ *είναι η ένωση όλων των* U_i, *δηλαδή*

$$\mathbb{P}^n = \bigcup_{i=0}^{n} U_i$$

έτσι ο $\mathbb{P}^n$ *καλύπτεται από* $n+1$ *αντίγραφα του αφινικού χώρου.*

Έστω $V \subseteq \mathbb{P}^n$ *μία προβολική πολλαπλότητα, τότε* $V = \bigcup_{i=0}^{n} \big(V \cap U_i\big)$. *Υποθέτουμε ότι* $V \cap U_i \neq \emptyset$. *Τότε*

$$V_i := \varphi_i^{-1}\big(V \cap U_i\big) \subseteq \mathbb{A}^n.$$

Προφανώς V_i *είναι μία αφινική πολλαπλότητα και συνεπώς το ιδεώδες της είναι*

$$I(V_i) = \big\{ F(x_0, \ldots, x_{i-1}, 1, x_i, \ldots, x_n) \big| \; F \in I(V) \big\}$$

Για διευκόλυνση μας θα περιοριστούμε μόνο στην περίπτωση όπου $i = n$ *και επομένως* $V \cap U_n \neq \emptyset$.

Ορισμός 3.27 *Έστω* $H_n := \mathbb{P}^n \setminus U_n = \big\{ (a_0 : \cdots : a_n) \in \mathbb{P}^n \big| \; a_n = 0 \big\}$. H_n *καλείται το* ***υπερεπίπεδο στο άπειρο*** *και τα* $P \in V \cap H_n$ *είναι τα σημεία της* V *στο άπειρο.*

Υπάρχει ένας φυσικός K - ισομορφισμός $\alpha : K(V) \to K(V_n)$. Όπου $K(V)$ είναι το σώμα των ρητών συναρτήσεων της προβολικής πολλαπλότητας της V και $K(V_n)$ το σώμα των ρητών συναρτήσεων της αφινικής πολλαπλότητας V_n που ορίσαμε παραπάνω.

Ο ισομορφισμός αυτός ορίζεται ως ακολούθως:
Θέτουμε $f = g/h \in K(V)$ όπου $g, h \in \Gamma_h(V)$ είναι πολυώνυμα του ίδιου βαθμού και $h \neq 0$. Στη συνέχεια διαλέγουμε ομογενή πολυώνυμα $G, H \in K[x_0, \ldots, x_n]$ τα οποία αντιπροσωπεύονται από τα g και h αντίστοιχα. Θέτουμε τώρα $G_* = G(x_0, \ldots, x_{n-1}, 1) \in K[x_0, \ldots, x_{n-1}]$ και $H_* = H(x_0, \ldots, x_{n-1}, 1) \in K[x_0, \ldots, x_{n-1}]$.
Ο δακτύλιος πυλίκο της αφινικής πολλαπλότητας V_n είναι

$$\Gamma(V_n) = K[x_0, \ldots, x_{n-1}]/I(V_n)$$

και η κλάση υπολοίπων των πολυωνύμων G_* και H_* στο $\Gamma(V_n)$ είναι g_* και h_* αντίστοιχα. Τότε $\alpha(f) = g_*/h_*$. Οι τοπικοί δακτύλιοι $\mathcal{O}_P(V \cap U_n)$ και $\mathcal{O}_{\varphi_n^{-1}(P)}(V_n)$ είναι ισόμορφοι γιατί από τον ισομορφισμό α που ορίσαμε ο τοπικός δακτύλιος του σημείου $P \in V \cap U_n$ απεικονίζεται στον τοπικό δακτύλιο του σημείου $\varphi_n^{-1}(P) \in V_n$.

3.4 Το προβολικό κάλυμμα μιας αφινικής πολλαπλότητας

Για ένα πολυώνυμο $F = F(x_0, \ldots, x_n) \in K[x_0, \ldots, x_{n-1}]$ βαθμού d, θέτουμε

$$F^* = x_n^d \cdot F(x_0/x_n, \ldots, x_{n-1}/x_n) \in K[x_0, \ldots, x_n].$$

Το F^* είναι ένα ομογενές πολυώνυμο βαθμού d, $n+1$ πολλαπλοτήτων.

Ορισμός 3.28 Προβολικό κάλυμμα *μιας αφινικής πολλαπλότητας $V \subseteq \mathbb{A}^n$ καλείται μία προβολική πολλαπλότητα $\bar{V} \subseteq \mathbb{P}^n$ που ορίζεται ως*

$$\bar{V} := \left\{ P \in \mathbb{P}^n \,\middle|\, F^*(P) = 0 \; \forall \, F \in I(V) \right\}.$$

Παρατήρηση 3.29

i. Μπορούμε να ξαναβρούμε την V από την $\bar{V}$ με την ίδια διαδικασία που περιγράψαμε στην προηγούμενη παράγραφο, δηλαδή

$$V = \phi_n^{-1}\left(\bar{V} \cap U_n\right) = \left(\bar{V}\right)_n.$$

ii. Το σώμα των ρητών συναρτήσεων του V και του $\bar{V}$ είναι ισόμορφα.

iii. Η διάσταση του V και του $\bar{V}$ είναι ίσες, δηλαδή $\dim V = \dim \bar{V}$.

3.5 Ρητές απεικονίσεις και μορφισμοί

Έστω $V \subseteq P^m$ και $W \subseteq P^n$ είναι δύο προβολικές πολλαπλότητες. Υποθέτουμε ότι $F_0, \ldots, F_n \in K[x_0, \ldots, x_m]$ είναι ομογενή πολυώνυμα με τις ακόλουθες ιδιότητες

i. $\deg F_0 = \cdots = \deg F_n$.

ii. $F_i \in I(V)$, *όχι για όλα τα* i.

iii. $\forall\, H \in I(W)$ *ισχύει ότι* $H(F_0, \ldots, F_n) \in I(V)$.

iv. $F_i G_j \equiv F_j G_i \bmod I(V)$ *για* $0 \leq i, j \leq n$.

Θέτουμε $Q \in V$ και υποθέτουμε ότι $F_i(Q) \neq 0$ για τούλαχιστον ένα $0 \neq i \neq n$ $\big($από το (ii) ώστε να υπάρχει ένα σημείο$\big)$. Τότε το σημείο $\big(F_0(Q) : \cdots : F_n(Q)\big) \in P^n$ επεκτείνεται στο W από το (iii). Θέτουμε $(G_0, \ldots, G_n)$ να είναι μία n-άδα ομογενών πολυωνύμων τέτοια ώστε να ικανοποιούνται οι συνθήκες (i), (ii) και (iii) που αναφέραμε παραπάνω.

Λέμε ότι οι n-άδες των πολυωνύμων $\big(F_0, \ldots, F_n\big)$ και $\big(G_0, \ldots, G_n\big)$ είναι ισοδύναμα αν ισχύει η συνθήκη (iv.).

Η κλάση ισοδυναμίας του $(F_0, \ldots, F_n)$ με την σχέση ισοδυναμίας $\sim$ φαίνεται από την σχέση

$$\phi = (F_0 : \cdots : F_n)$$

και η $\phi : V \to W$ καλείται ***ρητή απεικόνιση***.

Ορισμός 3.30 *Μία ρητή απεικόνιση $\phi = (F_0 : \cdots : F_n)$ ορίζεται ατο σημείο $P \in V$ αν υπάρχουν ομογενή πολυώνυμα $G_0, \ldots, G_n \in K[x_0, \ldots, x_n]$ τέτοιο ώστε $\phi = (G_0 : \cdots : G_n)$ και $G_i(P) \neq 0$ για τουλάχιστον ένα i.*

Τότε θέτουμε

$$\phi(P) = \big(G_0(P) : \cdots : G_n(P)\big) \in W$$

και σύμφωνα με τα (i) και (iv) η συνάρτηση ϕ είναι καλά ορισμένη.

Ορισμός 3.31 *Έστω δύο πολλαπλότητες V_1 και V_2 είναι* ***birational*** *αν υπάρχουν ρητές απεικονίσεις $\phi_1 : V_1 \to V_2$ και $\phi_2 : V_2 \to V_1$ τέτοιο ώστε $\phi_1 \circ \phi_2$ είναι η ταυτοτική απεικόνιση του V_2 και $\phi_2 \circ \phi_1$ είναι η ταυτοτική απεικόνιση του V_1.*

Παρατήρηση 3.32 *Οι πολλαπλότητες V_1 και V_2 είναι birational αν και μόνο αν τα σώματα των ρητών συναρτήσεων τους $K(V_1)$ και $K(V_2)$ είναι K-ισόμορφα.*

Ορισμός 3.33

i. Μία ρητή απεικόνιση $\phi : V \to W$ η οποία ορίζεται για κάθε $P \in V$ καλείται ***μορφισμός***.

ii. Η απεικόνιση ϕ είναι ισόμορφη αν υπάρχει μορφισμός $\psi : W \to V$ τέτοιος ώστε η σύνθεση των $\phi \circ \psi$ και $\psi \circ \phi$ να είναι η ταυτοτική απεικόνιση των W και V αντίστοιχα.

Παρατήρηση 3.34 *Για την περίπτωση (ii), του προηγούμενου ορισμού, τα V και W λέμε ότι είναι ισόμορφα.*

Πόρισμα 3.35 *Η ένοια της ισομορφίας μεταξύ πολλαπλοτήτων συνεπάγεται την αμφίρητη ισοδυναμία. Το αντίστροφο δεν ισχύει πάντα.*

3.6 Αλγεβρικές καμπύλες

Ορισμός 3.36 *Μία προβολική (αφινική) αλγεβρική καμπύλη V είναι μία προβολική (αφινική) πολλαπλότητα διάστασης 1 (εννοούμε μόνο ανάγωγες καμπύλες).*

Παρατήρηση 3.37 *Επειδή η διάσταση της πολλαπλότητας είναι 1, το σώμα των ρητών συναρτήσεων $K(V)$ στο V είναι ένα αλγεβρικό σώμα συναρτήσεων μιας μεταβλητής.*

Ορισμός 3.38 *Ένα σημείο $P \in V$ είναι non-singular αν ο τοπικός δακτύλιος $\mathcal{O}_P(V)$ είναι ένας διακριτός δακτύλιος εκτίμησης.*

Σχόλιο 3.39 *Αν $\mathcal{O}_P(V)$ είναι διακριτός δακτύλιος εκτίμησης τότε $\mathcal{O}_P(V)$ είναι περιοχή κυρίων ιδεωδών με ακριβώς ένα μέγιστο ιδεώδες $\neq \{0\}$.*

Πρόταση 3.40 *Σε μία καμπύλη υπάρχουν μόνο πεπερασμένα το πλήθος singular σημεία.*

Ορισμός 3.41 *Μία καμπύλη V λέγεται **non-singular (ή λεία)** αν όλα τα σημεία $P \in V$ είναι non-singular.*

Ορισμός 3.42 *Μία επίπεδη αφινική καμπύλη είναι μια αφινική καμπύλη $V \subseteq \mathbb{A}^2$.*

Ορισμός 3.43 *Το ιδεώδες $I(V) \subseteq K[x_0, x_1]$ μιας αφινικής καμπύλης V γεννάται από ανάγωγο πολυώνυμο $G \in K[x_0, x_1]$ (το οποίο είναι μοναδικό πάνω από έναν σταθερό παράγοντα).*

Σχόλιο 3.44 *Αντίστροφα από τον προηγούμενο ορισμό, δίνεται ένα ανάγωγο πολυώνυμο $G \in K[x_0, x_1]$, το σύνολο $V = \left\{P \in A^2 \middle| G(P) = 0\right\}$ είναι μία επίπεδη αφινική καμπύλη και το G γεννά τα αντίστοιχα ιδεώδη $I(V)$.*

Για να ελέγχουμε αν ένα σημείο $P \in V$ είναι non-singular ή όχι ακολουθούμε το παρακάτω κριτήριο.

Κριτήριο Jacobi.

Ένα σημείο $P \in V$ είναι non-singular αν και μόνο αν

$$G_{x_0}(P) \neq 0 \text{ ή } G_{x_1}(P) \neq 0,$$

όπου $G_{x_i} \in K[x_0, x_1]$ *είναι οι μερικές παράγωγοι του πολυωνύμου* G *ως προς* x_i *και* $i = 0, 1$.

Ορισμός 3.45 *Μία επίπεδη προβολική καμπύλη είναι μια προβολική καμπύλη* $V \subseteq \mathbb{P}^2$.

Ορισμός 3.46 *Το ιδεώδες* $I(V) \subseteq K[x_0, x_1]$ *μιας προβολικής καμπύλης* V *γενυάται από ανάγωγα πολυώνυμα* $H \in K[x_0, x_1, x_2]$.

Το αντίστοιχο ***Κριτήριο Jacobi*** *της προβολικής πολλαπλότητας μας λέει ότι ένα σημείο* $P \in V$ *είναι non-singular αν και μόνο αν*

$$H_{x_i} \neq 0 \text{ για ένα τουλάχιστον } i = 0, 1, 2.$$

Σημείωση 3.47 *Αν* $V = \left\{ P \in \mathbb{A}^2 \middle| G(P) = 0 \right\}$ *είναι μία επίπεδη αφινική καμπύλη με ένα ανάγωγο πολυώνυμο* $G \in K[x_0, x_1]$ *βαθμού* d, *το προβολικό κάλυμμα* $\bar{V} \subseteq \mathbb{P}^2$ *είναι το σύνολο από τις ρίζες του ομογενούς πολυωνύμου*

$$G^* = x_2^d \cdot G\left(\frac{x_0}{x_2}, \frac{x_1}{x_2}\right).$$

Μπορούμε τώρα να ορίσουμε ρητές απεικονίσεις $\phi : V \to W$, *όπου* V, W *είναι προβολικές καμπύλες. Τότε τα ακόλουθα ισχύουν*

i. Η απεικόνιση ϕ *ορίζεται σε όλα τα non-singular σημεία* $P \in V$. *Επομένως, αν* V *είναι μια non-singular καμπύλη τότε η* ϕ *είναι ένας μορφισμός.*

ii. Αν V *είναι μια non-singular καμύλη και* ϕ *μη σταθερή απεικόνιση τότε η* ϕ *είναι μορφισμός.*

ΚΕΦΑΛΑΙΟ 4

Αλγεβρικά σώματα συναρτήσεων / πεπερασμένων σωμάτων σταθερών

Σ' αυτό το κεφάλαιο θα θεωρούμε $F/\mathbb{F}_q$ να είναι ένα αλγεβρικό σώμα συναρτήσεων (υπερβατικής διάστασης 1) γένους g με σώμα σταθερών το πεπερασμένο σώμα $\mathbb{F}_q$ δηλαδή $\mathbb{F}_q$ είναι αλγεβρικά κλειστό στο F ($\mathbb{F}_q = \{z \in F : z$ αλγεβρικό $/\, \mathbb{F}_q\}$).

4.1 Η ζ-συνάρτηση του σώματος συναρτήσεων

Από το κεφάλαιο 2 γνωρίζουμε ότι:

i. *$\mathcal{D}_F$ είναι η ομάδα των διαιρετών*

ii. *ένας divisor ορίζεται ως:*

$$A = \sum_{P \in \mathbb{P}_F} a_P P$$

και λέμε ότι $A > 0 \iff a_P > 0$.

Λήμμα 4.1 *Για κάθε $n \geq 0$ υπάρχουν πεπερασμένοι το πλήθος θετικοί διαιρέτες βαθμού n.*

Απόδειξη : *Αρκεί να δείξουμε ότι το σύνολο $S := \{P \in \mathbb{P}_{\mathbb{F}} \big| \deg P \leq n\}$, για πρώτους divisor, είναι πεπερασμένο. Διαλέγουμε λοιπόν ένα στοιχείο του F αλλά όχι του $\mathbb{F}_q$, έστω δηλαδή $x \in F \setminus \mathbb{F}_q$ και θεωρούμε το σύνολο $S_0 := \{P_0 \in \mathbb{P}_{\mathbb{F}_q(x)} \big| \deg P_0 \leq n\}$. Προφανώς $P \cap \mathbb{F}_q(x) \in S_0 \; \forall \, P \in S$ και κάθε $P_0 \in S_0$ έχει πεπερασμένες το πλήθος επεκτάσεις στο F. Έχουμε λοιπόν να δείξουμε ότι το S_0 είναι πεπερασμένο σύνολο. Εφόσον τα σημεία του $\mathbb{F}_q(x)$ (εκτός από τον πόλο του x) αντιστοιχούν σε ανάγωγα*

μονικά πολυώνυμα $p(x) \in \mathbb{F}_q[x]$ με τον ίδιο βαθμό S_0 είναι πεπερασμένο σύνολο.
□

Για λόγους πλήρους κατανόησης των όσων ακολουθήσουν ας παραθέσουμε γνώσεις για τους διαιρέτες, που αποκτήσαμε σε προηγούμενο κεφάλαιο.

i. *$\mathcal{P}_F < \mathcal{D}_F$ και $\mathcal{P}_F$ είναι οι κύριοι διαιρέτες και ορίζονται ως εξής*

$$(x) = \sum_{P \in \mathbb{P}_F} u_P(x)P, \text{ με } 0 \neq x \in F$$

ii. *Η ομάδα πηλίκο $\mathcal{C}_F = \mathcal{D}_F/\mathcal{P}_F$ καλείται η ομάδα κλάσης διαιρετών του $F/\mathbb{F}_q$.*

iii. *$A,\ B \in \mathcal{D}_F$ δύο διαιρέτες, τους λέμε ισοδύναμους και γράφουμε $A \sim B$ αν $B = A + (x)$ για κάποιο κύριο διαιρέτη $(x) \in \mathcal{P}_F$.*

iv. *Ο διαιρέτης κλάσης του A στην ομάδα κλάσης διαιρετών $\mathcal{C}_F$ είναι ο $[A]$.*

v. *Αν $A \sim B \iff A \in [B] \iff [A] = [B]$.*

vi. *Ισοδύναμοι διαιρέτες έχουν την ίδια τάξη και την ίδια διάσταση*

$$\deg[A] = \deg A \qquad \text{και} \qquad \dim[A] = \dim A$$

Ορισμός 4.2 *Το σύνολο*

$$\mathcal{D}_F^0 := \{A \in \mathcal{D}_F \big| \deg A = 0\} < \mathcal{D}_F,$$

καλείται ***ομάδα των διαιρετών βαθμού 0*** *και το σύνολο*

$$\mathcal{C}_F^0 := \{[A] \in \mathcal{C}_F \big| \deg[A] = 0\}$$

καλείται ***ομάδα κλάσης διαιρετών βαθμού 0***.

Πρόταση 4.3 *Η ομάδα κλάσης δαιρετών βαθμού 0 ($\mathcal{C}_F^0$) είναι μία πεπερασμένη ομάδα και ορίζουμε την* ***class group*** *στο $F/\mathbb{F}_q$ να είναι $h := h_F := \operatorname{ord} \mathcal{C}_F^0$.*

Απόδειξη: *Διαλέγουμε έναν διαιρέτη $B \in \mathcal{D}_F$ βαθμού $n := \deg B \geq g$ (g είναι το γένος του αλγεβρικού σώματος συναρτήσεων F). Θεωρούμε το σύνολο των διαιρετών κλάσης βαθμού n*

$$\mathcal{C}_F^n := \{[C] \in \mathcal{C}_F \big| \deg[C] = n\}.$$

Η απεικόνιση

$$\begin{cases} \mathcal{C}_F^0 & \longrightarrow & \mathcal{C}_F^n \\ [A] & \longmapsto & [A+B] \end{cases}$$

είναι 1-1 και επι, αρκεί λοιπόν να δείξουμε ότι το σύνολο $\mathcal{C}_F^n$ είναι πεπερασμένο. Θέλουμε $\forall\ [C] \in \mathcal{C}_F^n$ να υπάρχει ένας διαιρέτης $A \in [C]$ με $A \geq 0$. Πράγματι, εφόσον $\deg C = n \geq g$, έχουμε από το θεώρημα Riemann - Roch ότι $\dim[C] \geq$

$n+1-g \geq 1$. *Συνεπώς από το λήμμα 4.1 υπάρχουν πεπερασμένοι το πλήθος θετικοί διαιρέτες βαθμού* n. *Άρα* $\mathcal{C}_F^n$ *είναι πεπεραμένο.* □

Ορίζουμε του θετικό ακέραιο $0 < \partial \in \mathbb{Z}$ *με*

$$\partial := \min\{\deg A \big| A \in \mathcal{D}_F,\ \deg A > 0\}.$$

Η εικόνα της απεικόνισης του βαθμού $\deg : \mathcal{D}_F \to \mathbb{Z}$ *είναι υποομάδα των ακεραίων που γεννούται από το* ∂ *δηλαδή ισχύει* $\mathrm{Im}(\deg) = \langle \partial \rangle < \mathbb{Z}$ *και επιπλέον ο βαθμός κάθε διαιρέτη του* $F/\mathbb{F}_q$ *είναι πολλαπλάσιο του* ∂, *δηλαδή* $\deg A = \partial k,\ k \in \mathbb{Z}$.

Για τη συνέχεια, θέλουμε να μελετήσουμε τους αριθμούς

$$\begin{array}{rcl} A_n & := & \big|\{A \in \mathcal{D}_F | A \geq 0,\ \deg A = n\}\big| \\ & \underset{\deg A = \partial k}{=} & \big|\{A \in \mathcal{D}_F | A \geq 0,\ n = \partial k,\ k \in \mathbb{Z}\}\big| \end{array}$$

Παρατηρούμε ότι

$$A_0 = 1 \text{ και } A_1 = \big|\{P \in \mathbb{P}_F : \deg P = 1\}\big|. \tag{4.1}$$

Λήμμα 4.4

i. $A_n = 0$ *αν* $\partial \nmid n$.

ii. *Για μία* ***fixed κλάση διαιρετών*** $[C] \in \mathcal{C}_F$, *έχουμε*

$$\big|\{A \in [C] | A \geq 0\}\big| = \frac{1}{q-1}\left(q^{\dim[C]} - 1\right).$$

iii. *Για κάθε ακέραιο* $n > 2g-2$ *με* $\partial \mid n$

$$A_n = \frac{h}{q-1}\left(q^{n+1-g} - 1\right).$$

Απόδειξη:

i. *Παραπάνω ορίσαμε ότι* $A_n := \big|\{A \in \mathcal{D}_F | A \geq 0,\ n = \partial k,\ k \in \mathbb{Z}\}\big|$, *συνεπώς αν* $\partial \nmid n \Rightarrow A_n = 0$.

ii. *Θέλουμε να δείξουμε ότι το πλήθος των θετικών διαιρετών* $0 \neq A \in [C]$, $[C]$ *fixed κλάση διαιρετών είναι ίσο με* $\frac{1}{q-1}\left(q^{\dim[C]} - 1\right)$. *Αφού* $A \in [C] \Leftrightarrow A \sim C \Rightarrow A = (x) + C$, *για κάποιο* $x \in F$ *με* $(x) \geq -C \Rightarrow x \in \mathcal{L}(C) \setminus \{0\}$. *Υπάρχουν ακριβώς* $q^{\dim[C]} - 1$ *στοιχεία του* $\mathcal{L}(C) \setminus \{0\}$ *και δύο απ' αυτά δίνουν τον ίδιο διαιρέτη αν και μόνον αν διαφέρουν κατά ένα μη μηδενικό σταθερό παράγοντα* $0 \neq a \in \mathbb{F}_q$.

iii. *Υπάρχουν* $h = h_F$ *κλάσεις διαιρετών βαθμού* n, $[C_1], [C_2], \ldots, [C_h]$. *Από το προηγούμενο ερώτημα και από το θεώρημα Riemann - Roch*

$$\big|\{A \in [C_j] \,:\, A \geq 0\}\big| = \frac{1}{q-1}\left(q^{\dim[C_j]} - 1\right) = \frac{1}{q-1}\left(q^{n+1-g} - 1\right).$$

Κάθε διαιρέτης βαθμού n εκτείνεται σε ακριβώς μία από τις κλάσεις διαιρετών $[C_1], [C_2], \ldots, [C_h]$, επομένως για να υπολογίσουμε το A_n θα λογαριάσουμε το άθροισμα σε όλες τις κλάσεις, δηλαδή

$$A_n = \sum_{j=1}^{n} \left|\{A \in [C_j] \,:\, A \geq 0\}\right| = \frac{h}{q-1}\left(q^{n+1-g} - 1\right).$$

□

Ορισμός 4.5 *Η δυναμοσειρά*

$$Z(t) := Z_F(t) := \sum_{n=0}^{\infty} A_n t^n \in \mathbb{C}[[t]]$$

*όπου $A_n := \left|\{A \in \mathcal{D}_F | A \geq 0,\ \deg A = n\}\right|$ καλείται η **ζήτα συνάρτηση** του $F/\mathbb{F}_q$.*

Παρατηρήσεις 4.6

i. *Θεωρούμε το t ως μιγαδική μεταβλητή.*

ii. *Η $Z(t)$ είναι δυναμοσειρά υπεράνω του σώματος των μιγαδικών αριθμών.*

Τώρα θα δείξουμε ότι η ζήτα συνάρτηση του $F/\mathbb{F}_q$ συγκλίνει για σε μία περιοχή του 0.

Πρόταση 4.7 *Η δυναμοσειρά $Z(t) = \sum_{n=0}^{\infty} A_n t^n$ συγκλίνει για $|t| < q^{-1}$. Συγκεκριμένα, για $|t| < q^{-1}$ έχουμε:*

i. *Αν το αλγεβρικό σώμα συναρτήσεων $F/\mathbb{F}_q$ είναι γένους $g = 0$ τότε*

$$Z(t) = \frac{1}{q-1}\left(\frac{q}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}}\right).$$

ii. *Αν $g \geq 1$, τότε $Z(t) = F(t) + G(t)$ με*

$$F(t) = \frac{1}{q-1} \sum_{0 \leq \deg[C] \leq 2g-2} q^{\dim[C]} \cdot t^{\deg[C]},$$

$\left(\text{όπου } [C] \text{ τρέχει όλες τις κλάσεις διαιρετών } [C] \in \mathcal{C}_F \text{ με } 0 \leq \deg[C] \leq 2g-2\right)$ και

$$G(t) = \frac{h}{q-1}\left(q^{1-g}\,(qt)^{2g-2+\partial}\,\frac{1}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}}\right).$$

Απόδειξη:

i. Αρχικά, αφού το αλγεβρικό σώμα συναρτήσεων $F/\mathbb{F}_q$ είναι γένους $g = 0$ έχει class number $h = 1$, δηλαδή κάθε διαιρέτης A βαθμού μηδέν είναι κύριος. Από το λήμμα 4.4.(iii) έχουμε ότι $\forall\ \mathbb{Z} \ni n > 2g-2$ με $\partial \mid n$, $A_n = \frac{h}{q-1}\left(q^{n+1-g}-1\right)$. Αφού $g = 0$ διαλέγουμε τον ακέραιο $n = 0 > 2g-2$ και από το θεώρημα Riemann - Roch έχουμε ότι

$$\dim A = \deg A + 1 - g \overset{\substack{\deg A=0\\ g=0}}{=} 1.$$

Μπορούμε να βρούμε ένα μη μηδενικό στοιχείο $x \neq 0$ με $(x) \geq -A$. Οι διαιρέτες A και (x) είναι βαθμού 0. Συνεπώς $A = -(x) = \left(\frac{1}{x}\right)$ είναι κύριος διαιρέτης.
Τώρα η ζήτα συνάρτηση του $F/\mathbb{F}_q$ από τα παραπάνω γίνεται

$$\begin{aligned}\sum_{n=0}^{\infty} A_n t^n &= \sum_{n=0}^{\infty} A_{\partial n} t^{\partial n} = \sum_{n=0}^{\infty} \frac{1}{q-1}\left(q^{\partial n+1}-1\right) t^{\partial n} \\ &= \frac{1}{q-1}\left(q\sum_{n=0}^{\infty}(qt)^{\partial n} - \sum_{n=0}^{\infty} t^{\partial n}\right) \\ &= \frac{1}{q-1}\left(\frac{q}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}}\right)\end{aligned}$$

για $|qt| < 1 \Rightarrow |t| < q^{-1}$.

ii. Για $g \geq 1$ οι υπολογισμοί είναι παρόμοιοι:

$$\begin{aligned}Z(t) &= \sum_{n=0}^{\infty} A_n t^n = \sum_{\deg[C]\geq 0} \left|\{A \in [C] \,:\, A \geq 0\right| \cdot t^{\deg[C]} \\ &= \sum_{\deg[C]\geq 0} \frac{q^{\dim[C]}-1}{q-1} \cdot t^{\deg[C]} \\ &= \frac{1}{q-1} \sum_{0\leq \deg[C]\leq 2g-2} q^{\dim[C]} \cdot t^{\deg[C]} \\ &\quad + \frac{1}{q-1} \sum_{\deg[C]>2g-2} q^{\deg[C]+1-g} \cdot t^{\deg[C]} \\ &\quad - \frac{1}{q-1} \sum_{\deg[C]\geq 0} t^{\deg[C]} = F(t) + G(t),\end{aligned}$$

με

$$F(t) = \frac{1}{q-1} \sum_{0\leq \deg[C]\leq 2g-2} q^{\dim[C]} \cdot t^{\deg[C]}.$$

Τώρα για να αποδείξουμε ότι

$$G(t) = \frac{1}{q-1} \sum_{\deg[C]>2g-2} q^{\deg[C]+1-g} \cdot t^{\deg[C]} - \frac{1}{q-1} \sum_{\deg[C]\geq 0} t^{\deg[C]}$$

θα κάνουμε κάποιους υπολογισμούς.
Για το πρώτο άθροισμα. Από το λήμμα $4.4\,\deg[C] > 2g-2$ *με*

$$\partial \mid \deg[C] \Rightarrow \deg[C] = n\partial > 2g-2 \Rightarrow n > \frac{2g-2}{\partial} \Rightarrow n = \frac{2g-2}{\partial} + 1$$

Για το δεύτερο άθροισμα. Αφού $\deg[C] \geq 0$ *θέτω* $n = \deg[C]$. *Συνεπώς τελικά έχουμε*

$$\begin{aligned} G(t) &= \sum_{n=\frac{2g-2}{\partial}+1}^{\infty} hq^{n\partial+1-g} \cdot t^{n\partial} - \sum_{n=0}^{\infty} ht^{n\partial} \\ &= \frac{1}{q-1}\left(hq^{1-g}(qt)^{2g-2+\partial}\frac{1}{1-(qt)^{\partial}} - h\frac{1}{1-t^{\partial}}\right) \\ &= \frac{h}{q-1}\left(q^{1-g}(qt)^{2g-2+\partial}\frac{1}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}}\right). \end{aligned}$$

Συνεπώς $Z(t) = F(t) + G(t)$. □

Πόρισμα 4.8 *Η δυναμοσειρά* $Z(t)$ *μπορεί να επεκταθεί σε μια* ***ρητή συνάρτηση*** *του* $\mathbb{C}$ *με απλό πόλο στο* $t = 1$.

Απόδειξη: *Η* $G(t)$ *έχεια απλό πόλο στο* $t = 1$ *γιατί* $1/(1-t^{\partial})$ *έχει απλό πόλο στο στο* $t = 1$, *συνεπώς και η* $Z(t)$ *έχει απλό πόλο στο* $t = 1$. □

Πρόταση 4.9 (Γινόμενο Euler) *Για* $|t| < q^{-1}$ *η συνάρτηση* $Z(t)$ *μπορεί να παρασταθεί σαν απολύτως συγκλίνον γινόμενο*

$$Z(t) = \prod_{P \in \mathbb{P}_F} \left(1 - t^{\deg P}\right)^{-1}. \tag{4.2}$$

Για $|t| < q^{-1}$ *η συνάρτηση* $Z(t) \neq 0$.

Απόδειξη: *Το γινόμενο* $\prod_{P\in\mathbb{P}_F}\left(1-t^{\deg P}\right)^{-1}$ *για* $|t| < q^{-1}$ *συγκίνει απόλυτα. Εφόσον από την πρόταση 4.7*

$$\sum_{P\in\mathbb{P}_F} |t|^{\deg P} \leq \sum_{n=0}^{\infty} A_n |t|^n < \infty.$$

Κάθε παράγοντας της (4.2) μπορεί να γραφεί σαν γεωμετρική σειρά και συνεπώς παίρνουμε

$$\prod_{P\in\mathbb{P}_F}\left(1-t^{\deg P}\right)^{-1} = \prod_{P\in\mathbb{P}_F}\sum_{n=0}^{\infty} t^{\deg(nP)} = \sum_{0\leq A\in\mathcal{D}_F} t^{\deg A} = \sum_{n=0}^{\infty} A_n t^n = Z(t).$$

□

Στη συνέχεια, διαλέγουμε μία αλγεβρική κλειστότητα $\bar{\mathbb{F}}_q$ *του σώματος σταθερών* $\mathbb{F}_q$ *και θεωρούμε την επέκταση του σώματος σταθερών* $\bar{F} = F\bar{\mathbb{F}}_q$ *του σώματος* $F/\mathbb{F}_q$. *Για κάθε* $r \geq 1$ *υπάρχει ακριβώς μία επέκταση* $\mathbb{F}_{q^r}/\mathbb{F}_q$ *με* $[\mathbb{F}_{q^r} : \mathbb{F}_q] = r$ *και θέτουμε*

$$F_r := F\mathbb{F}_{q^r} \subseteq \bar{F}.$$

Ορισμός 4.10 *Έστω $f(x) \in K[x]$ και ότι*

$$f(x) = a(x - r_1) \cdots (x - r_n)$$

μία παραγοντοποίηση του $f(x)$, όπου $a \in K$. Το πολυώνυμο $f(x)$ ονομάζεται διαχωρίσιμο όταν κανένα από τα $(x - r_i)$, με $i = 1, \ldots, n$ δεν επαναλαμβάνεται.

Ορισμός 4.11 *Έστω L/K μία επέκταση σωμάτων.*

i. *Η επέκταση L/K ονομάζεται **κανονική** αν κάθε πολυώνυμο $f(x) \in K[x]$, που έχει μία ρίζα στο L έχει όλες τις ρίζες στο L.*

ii. *Ένα στοιχείο $a \in L$ λέγεται διαχωρίσιμο, ή αν είναι υπερβατικό ή όταν το ανάγωγο πολυώνυμό του είναι διαχωρίσιμο. Η επέκταση L/K λέγεται διαχωρίσιμη αν κάθε στοιχείο της είναι διαχωρίσιμο.*

iii. *Μία κανονική και διαχωρίσιμη επέκταση ονομάζεται επέκταση Galois.*

Ορισμός 4.12 *Αν L είναι ένα σώμα, τότε ονομάζουμε **αυτομορφισμό** του L μία απεικόνιση $\sigma : L \longrightarrow L$ η οποία είναι ισομορφισμός (1-1 και επί).*
*Αν L/K είναι μία επέκταση σώματος, τότε λέμε ότι ένας αυτομορφισμός σ του L διατηρεί **σημειακά σταθερό** το K όταν $\sigma(c) = c$, $\forall\, c \in K$.*

Ορισμός 4.13 (Ομάδα Galois) *Έστω L/K μία επέκταση σώματος, ονομάζουμε **ομάδα Galois** της επέκτασης, την ομάδα*

$$Gal(L/K) = \{\sigma \big| \sigma \text{ αυτομορφισμός του } L,\ \sigma(c) = c\, \forall\, c \in K\}$$

με πράξη την σύνθεση των απεικονίσεων.

Ορισμός 4.14 *Έστω $F_r/\mathbb{F}_{q^r}$ είναι μία αλγεβρική επέκταση του αλγεβρικού σώματος συναρτήσεων $F/\mathbb{F}_q$. Για μία θέση $P \in \mathbb{P}_F$ και μία θέση $P' \in \mathbb{P}_{F_r}$ για την οποία ισχύει ότι η θέση P' επεκτείνει την θέση P ορίζουμε τα ακόλουθα:*

1. $Con_{F_r/F}(P) := \sum_{P'|P} e(P'|P) \cdot P'$,
2. $e(P'|P) := e$ *με* $\upsilon_{P'}(x) = e \cdot \upsilon_P(x)\ \forall\, x \in F$.

Λήμμα 4.15

i. *F_r/F είναι μία κυκλική επέκταση βαθμού r (F_r/F είναι επέκταση Galois με κυκλική ομάδα Galois τάξης r). Η ομάδα Galois $Gal(F_r/F)$ γεννάται από έναν αυτομορφισμό Frobenious $\sigma : \mathbb{F}_{q^r} \to \mathbb{F}_{q^r}$ με $\sigma(a) = a^q$.*

ii. *$\mathbb{F}_{q^r}$ είναι το πλήρες σώμα σταθερών του F_r.*

iii. *Το σώμα $F_r/\mathbb{F}_{q^r}$ έχει το ίδιο γένος με το σώμα $F/\mathbb{F}_q$.*

iv. Έστω $P \in \mathbb{P}_F$ είναι μία θέση βαθμού m. Τότε το P διασπάται στο F_r σε άθροισμα θέσεων, δηλαδή $Con_{F_r/F}(P) = P_1 + \cdots + P_d$ με $d := \text{μκδ}(m, r)$ ανά δύο διαφορετικών θέσεων $P_i \in \mathbb{P}_{F^r}$ με βαθμό $\deg P_i = m/d$.

Ορισμός 4.16 *Ορίζουμε του διαιρέτη $Diff(F_r/F) := \sum_{P \in \mathbb{P}_F} \sum_{P'|P} d(P'|P) \cdot P'$ και ο διαφορικός εκθέτης του P' υπεράνω του P ορίζεται $d(P'|P) := -\upsilon_{P'}(t)$.*

Θεώρημα 4.17 (Τύπος γένους του Hurwitz)

a) $F/\mathbb{F}_q$ αλγεβρικό σώμα συναρτήσεων γένους g με $\mathbb{F}_q$ σώμα σταθερών του F και $\mathbb{F}_{q^r}/\mathbb{F}_q$ είναι μία απλή επέκταση.

b) $F_r/\mathbb{F}_{q^r}$ αλγεβρικό σώμα συναρτήσεων γένους g' και $\mathbb{F}_{q^r}$ είναι το σώμα σταθερών του F_r.

Τότε έχουμε

$$2g' - 2 = \frac{[F_r : F]}{[\mathbb{F}_{q^r} : \mathbb{F}_q]}(2g - 2) + \deg Diff(F_r/F).$$

Για την απόδειξη αυτού του θεωρήματος παραπέμπουμε στο βιβλίο [HENS], σελίδα 88.

Ορισμός 4.18 *Έστω F_r/F μία πεπερασμένη και διαχωρίσιμη επέκταση αλγεβρικών σωμάτων αριθμών. Αν $P \in \mathbb{P}_F$ και $P' \in \mathbb{P}_{F_r}$ έτσι ώστε $P'|P$, τότε $P'|P$ είναι ramified αν και μόνο αν $P' \leq Diff(F_r/F)$. Σε όλες τις άλλες θέσεις $P \in \mathbb{P}_F$ είναι unramified στο F_r/F.*

Απόδειξη: *(Λήμματος (4.15))*

i. Γνωρίζουμε ότι η επέκταση $\mathbb{F}_{q^r}/\mathbb{F}_q$ είναι είναι κυκλική βαθμού r γιατί η ομάδα Galois $Gal(\mathbb{F}_{q^r}/\mathbb{F}_q) = \langle a \mapsto a^q \rangle$, που γεννάται από τον αυτομορφισμό Frobenious $a \mapsto a^q$ είναι κυκλική τάξης r.
Θέλουμε να δείξουμε ότι $[F_r : F] = [\mathbb{F}_{q^r} : \mathbb{F}_q] = r$.
Η ανισότητα $[F_r : F] \leq [\mathbb{F}_{q^r} : \mathbb{F}_q]$ αποδεικνύεται εύκολα. Θα πρέπει να δείξουμε ότι το ελάχιστο πολλυώνυμο $s(t) \in \mathbb{F}_q[t]$ με $s(a) = 0$ είναι ανάγωγο πολλυώνυμο στο $F[t]$. Υποθέτουμε το αντίθετο, έστω ότι υπάρχουν μονικά πολλυώνυμα $g(t)$, $h(t) \in F[t]$ με $1 \leq \deg g < \deg s$ και $1 \leq \deg h < \deg s$ τέτοια ώστε $s(t) = g(t) \cdot h(t)$. Κάθε ρίζα των $g(t)$, $h(t)$ στο F_r θα είναι ρίζα και του $s(t)$ συνεπώς θα είναι αλγεβρική υπεράνω του $\mathbb{F}_q$. Επειδή $F/\mathbb{F}_q$ (όπως ορίσαμε στην αρχή του κεφαλαίου) είναι ένα αλγεβρικό σώμα συναρτήσεων έχουμε ότι οι συντελεστές των πολυωνύμων είναι αλγεβρικοί υπεράνω του $\mathbb{F}_q$. Τέλος επειδή $\mathbb{F}_q$ είναι το πλήρες σώμα σταθερών του F (περιέχει δηλαδή όλα τα στοιχεία του F τα οποία είναι αλγεβρικά υπεράνω του $\mathbb{F}_q$) οι συντελεστές των $g(t)$, $h(t)$ θα περιέχονται στο $\mathbb{F}_q$, όμως αυτό έρχεται σε αντίθεση με τον αρχικό συλογισμό μας, δηλαδή ότι το $s(t)$ είναι το ελαχίστου βαθμού πολλυώνυμο. Άρα δεν υπάρχουν τέτοια $g(t)$, $h(t)$ και συνεπώς το $s(t)$ είναι ανάγωγο στο $F[t]$.

ii. *Θεωρούμε ένα στοιχείο $\delta \in F_r$ το οποίο είναι αλγεβρικό υπεράνω του $\mathbb{F}_{q^r}$ και θέλουμε να δείξουμε ότι $\delta \in \mathbb{F}_{q^r}$. Το στοιχείο αυτό είναι αλγεβρικό υπεράνω του $\mathbb{F}_q$ και υπάρχουν πεπερασμένα το πλήθος στοιχεία $a_1, \ldots, a_r \in \mathbb{F}_{q^r}$ τέτοια ώστε $\delta \in F(a_1, \ldots, a_r)$. Η επέκταση $\mathbb{F}_q(a_1, \ldots, a_r)/\mathbb{F}_q$ είναι πεπερασμένη επομένως $\mathbb{F}_q(a_1, \ldots, a_r) = \mathbb{F}_q(a) = \mathbb{F}_{q^r}$ για κάποιο $a \in \mathbb{F}_{q^r}$ (εδώ θα χρησιμοποιήσουμε την το γεγονός ότι $\mathbb{F}_q$ είναι το σώμα σταθερών του F). Εφόσον δ είναι αλγερικό υπεράνω του $\mathbb{F}_q$ μπορούμε να βρούμε $\beta \in F_r$ με $\mathbb{F}_q(a, \delta) = \mathbb{F}_q(\beta)$. Επιπλέον $F(\beta) = F(a, \delta) \overset{\delta \in F(a)}{=} F(a)$ και από (i) έχουμε ότι*

$$[\mathbb{F}_q(\beta) : \mathbb{F}_q] = [F(\beta) : F] = [F(a) : F] = [\mathbb{F}_q(a) : \mathbb{F}_q].$$

Συνεπώς $\delta \in \mathbb{F}_q(\beta) = \mathbb{F}_q(a) = \mathbb{F}_{q^r}$.

iii. *Από (i) F_r είναι μία πεπερασένη απλή επέκταση του σώματος συναρτήσεων F βαθμού $[F_r : F] = [\mathbb{F}_{q^r} : \mathbb{F}_q] = r$. Θέτουμε $P \in \mathbb{P}_F$ τέτοιο ώστε το ελάχιστο πολυώνυμο $\phi(t) \in \mathbb{F}_q[t]$ με $\phi(a) = 0$ (από (ii) το ελάχιστο πολυώνυμο παραμένει ανάγωγο υπεράνω του F) να έχει τους συντελεστές στον δακτύλιο εκτίμησης $_P$ (δηλαδή a είναι ακέραιος αλγεβρικός υπεράνω του $_P$) επιπλέον θέτουμε $P' \in \mathbb{P}_{F_r}$ με τη θέση P' να είναι επέκταση της θέσης P (συμβ. $P'|P$) τότε*

$$d(P'|P) \leq \upsilon_{P'}\big(\phi'(a)\big) \text{ με } \phi'(t) = \frac{d}{dt}\phi(t) \in \mathbb{F}_q[t].$$

Όμως το a είναι απλή ρίζα του ελαχίστου πολυωνύμου υπεράνω του $\mathbb{F}_q$ επομένως $\phi'(a) \neq 0$. Εφόσον $\phi'(a) \in \mathbb{F}_{q^r} \Rightarrow \upsilon_{P'}\big(\phi'(a)\big) = 0$. Έτσι έχουμε $0 \leq d(P'|P) \leq 0 \Rightarrow d(P'|P) = 0$ και επομένως $Diff\,(F_r/F) = 0$.

Συνεπώς έχουμε ότι

$$2g' - 2 = \frac{r}{r}(2g - 2) + \deg 0 \Longrightarrow 2g' - 2 = 2g - 2 \Longrightarrow g' = g.$$

Άρα $F_r/\mathbb{F}_{q^r}$ και $F/\mathbb{F}_q$ έχουν το ίδιο γένος.

iv. *Από το (iii) $Diff\,(F_r/F) = 0$ συνεπώς $P' \nleq Diff\,(F_r/F)$ (εξ' ορισμού της θέσης) άρα οι θέσεις $P \in \mathbb{P}_F$ είναι unramified στο F_r/F. Θεωρούμε ότι μερικές θέσεις $P' \in \mathbb{P}_{F_r}$ επεκτείνουν την P.*

Το σώμα υπολοίπων του σημείου P' είναι η σύνθεση του $\mathbb{F}_{q^r}$ με το σώμα υπολοίπων F_P του σημείου P. Θέτουμε $z(P') \in (F_r)_{P'}$ όπου z είναι ένα στοιχείο του $_{P'}$. Υπάρχει ένα ενδιάμεσο σώμα K τέτοιο ώστε $\mathbb{F}_q \subseteq K \subseteq \mathbb{F}_{q^r}$ με $z \in L$, ορίζουμε $L := FK$ η επέκταση $K/\mathbb{F}_q$ είναι προφανώς πεπερασμένη εφόσον ισχύει $[\mathbb{F}_{q^r} : \mathbb{F}_q] = [\mathbb{F}_{q^r} : K] \cdot [K : \mathbb{F}_q]$ και η επέκταση $\mathbb{F}_{q^r}/\mathbb{F}_q$ είναι πεπερασμένη. Θέτουμε $P_1 := P' \cap L$ και $P_2, \ldots, P_\delta$ να είναι οι άλλες θέσεις του L/K που επεκτείνουν τη θέση P. Επιλέγουμε $u \in L$ τέτοιο ώστε για τη διακριτή εκτίμηση υ να ισχύουν

$$\upsilon_{P_1}(z - u) > 0 \text{ και } \upsilon_{P_i}(u) \geq 0 \text{ με } 2 \leq i \leq \delta.$$

Επειδή $v_{P_1}(z-u) > 0$ *από τον ορισμό (2.31)* $(z-u)(P_1) = 0 \Rightarrow z(P_1) = u(P_1) \Rightarrow z(P') = u(P')$ *και το* u *βρίσκεται στο ακέραιο κάλλυμα του* $_P$ *στο* L. *Όπως είπαμε η επέκταση* $K/\mathbb{F}_q$ *είναι πεπερασμένη, έστω* $[K : \mathbb{F}_q] = w$, *θεωρούμε λοιπόν την ακόλουθη βάση ως βάση ακεραιότητας της επέκτασης* L/F *για όλες τις θέσεις* $P \in \mathbb{P}_F$, $\{1, b, \ldots, b^{w-1}\}$. *Συνεπώς για οποιαδήποτε άλλη βάση* $\{g_1, \ldots, g_w\}$ *της* $K/\mathbb{F}_q$

$$\sum_{i=0}^{w-1} {}_P \cdot b_i = \sum_{j=1}^{w} {}_P \cdot g_j$$

και επειδή επιλέξαμε $u \in L$ *έχουμε ότι*

$$u = \sum_{j=1}^{w} s_j \cdot g_j \text{ με } s_j \in {}_P g_j \in K.$$

Συνεπώς

$$z(P') = u(P') = \sum_{j=1}^{w} s_j \cdot g_j \in F_P \mathbb{F}_{q^r}.$$

Ορίζουμε $l := \text{εκπ}(m, r)$. *Επειδή* $F_P = \mathbb{F}_{q^m}$, *η σύνθεση του* $\mathbb{F}_{q^r}$ *με το σώμα υπολοίπων του σημείου* P *είναι*

$$\mathbb{F}_{q^m} \cdot \mathbb{F}_{q^r} = \mathbb{F}_{q^l}.$$

Επομένως

$$\deg P' = [\mathbb{F}_{q^l} : \mathbb{F}_{q^r}] = \frac{m}{d}.$$

Τώρα μπορούμε να θεωρήσουμε έναν πρώτο διαιρέτη $P \in \mathbb{P}_F$. *Διαλέγουμε* $x \in F$ *τέτοιο ώστε ο* P *να είναι η μοναδική ρίζα του* x *στο* $\mathbb{P}_F$, *έτσι ο μηδενικός διαιρέτης* $(x)_0^F$ *του* x *στο* $\mathcal{D}_F$ *είναι της μορφής* $(x)_0^F = hP,\ h > 0$.

$$\begin{aligned}(x)_0^{F_r} &= \textstyle\sum_{P' \in \mathbb{P}_{F_r}} v_{P'}(x) \cdot P' = \sum_{P \in \mathbb{P}_F} \sum_{P'|P} e(P'|P) \cdot v_P(x) \cdot P' \\ &= \textstyle\sum_{P \in \mathbb{P}_F} v_P(x) \cdot Con_{F_r/F}(P) = Con_{F_r/F}\left(\sum_{P \in \mathbb{P}_F} v_P(x) \cdot P\right) \\ &= Con_{F_r/F}\big((x)_0^{F_r}\big) = h \cdot Con_{F_r/F}(P)\end{aligned}$$

Έχουμε τώρα ότι

$$\begin{aligned}[F_r : \mathbb{F}_{q^r}(x)] &= \deg\big((x)_0^{F_r}\big)\ \forall\, x \in F_r \setminus \mathbb{F}_{q^r} \\ &= h \cdot \deg\big(Con_{F_r/F}(P)\big) \qquad (4.3)\end{aligned}$$

Για να καταλήξουμε στο ζητούμενο πρέπει πρώτα να δείξουμε ότι

$$[F_r : \mathbb{F}_{q^r}(x)] = [F : \mathbb{F}_q].$$

Έχουμε λοιπόν ότι $[F_r : \mathbb{F}_{q^r}(x)] \leq [F : \mathbb{F}_q]$ *και θέλουμε να δείξουμε ότι τα στοιχεία* $\gamma_1, \ldots, \gamma_\nu \in F$ *τα οποία είναι γραμμικά ανεξάρτητα υπεράνω του* $\mathbb{F}_q(x)$, *είναι γραμμικά ανεξάρτητα και υπεράνω του* $\mathbb{F}_{q^r}(x)$. *Υποθέτουμε ότι*

δεν είναι γραμμικά ανεξάτητα υπεράνω του $\mathbb{F}_{q^r}(x)$ και θα καταλήξουμε σε άτοπο. Αφού είναι γραμμικά εξαρτημένα $\exists\, f_i(x) \in \mathbb{F}_q[x]$ τα οποία είναι ίσα με το μηδέν όχι για όλα τα $1 \leq i \leq \nu$ έτσι ώστε να ισχύει

$$\sum_{i=1}^{\nu} f_i(x) \cdot \gamma_i = 0.$$

Στη συνέχεια πολλαπλασιάζοντας με τον κοινό παρονομαστή μπορούμε να υποθέσυμε ότι όλα τα $f_i(x) \in \mathbb{F}_{q^r}[x]$. Η παραπάνω σχέση μας δίνει το σύνολο

$$\{x^j \gamma_i | 1 \leq i \leq \nu \text{ και } j \geq 0\}$$

το οποίο είναι γραμμικά εξαρτημένο υπεράνω του $\mathbb{F}_{q^r}$ άρα είναι γραμμικά εξαρτημένο υπεράνω του $\mathbb{F}_q$, συνεπώς τα $\gamma_1, \ldots, \gamma_\nu$ είναι γραμμικά εξαρτημένα υπεράνω του $\mathbb{F}_q(x)$. Όμως εμείς υποθέσαμε ότι είναι γραμμικά ανεξάρτητα υπεράνω του $\mathbb{F}_q(x)$ και συνεπώς καταλήγουμε σε άτοπο όπως θέλουμε.
Συνεπώς η σχέση (4.3) γίνεται

$$h \cdot \deg\left(Con_{F_r/F}(P)\right) = [F_r : \mathbb{F}_{q^r}(x)] = [F : \mathbb{F}_q] = \deg\left((x)_0^F\right) = h \cdot \deg P.$$

Άρα αφού $\deg\left(Con_{F_r/F}(P)\right) = deg(P) = m$ συμπεραίνουμε ότι $Con_{F_r/F}(P) = P_1 + \cdots + P_d$ με τις θέσεις P_i να είναι βαθμου m/d. □

Πρόταση 4.19 *Έστω $Z(t)$ (αντίστοιχα $Z_r(t)$) ορίζουμε να είναι η ζήτα συνάρτηση του F (αντίστοιχα του $F_r = F\mathbb{F}_{q^r}$). Τότε*

$$Z_r(t^r) = \prod_{\zeta^r=1} Z(\zeta t)\ \forall\, t \in \mathbb{C}. \tag{4.4}$$

Πριν προχωρήσουμε στην απόδειξη αυτής της πρότασης θα αναφερθούμε σε μία πολυωνυμική ταυτότητα.

Έστω r , $m \in \mathbb{N}$ και $d = μκδ(m, r)$ τότε

$$\left(x^{r/d} - 1\right)^d = \prod_{\zeta^r=1} \left(x - \zeta^m\right). \tag{4.5}$$

Παρατηρήσεις 4.20

i. Στο γινόμενο της σχέσης (4.5) το ζ τρέχει όλες τις r ρίζες της μονάδας στο $\mathbb{C}$.

ii. Τα δύο μέλη της (4.5) είναι μονικά πολυώνυμα ίδιου βαθμού.

iii. Κάθε r/d ρίζα της μονάδας είναι πολλαπλότητας d.

Απόδειξη : *(Πρότασης 4.19)*
Θέλουμε να δείξουμε ότι

$$Z_r(t^r) = \prod_{\zeta^r=1} Z(\zeta t).$$

Από την πρόταση (4.9) για $|t| < q^{-1}$ *έχουμε*

$$Z_r(t^r) = \prod_{P\in\mathbb{P}_F} \prod_{P'|P} \left(1 - t^{r\cdot \deg P'}\right)^{-1}. \tag{4.6}$$

Τώρα στη σχέση (4.5) θέτουμε $x = t^{-m}$ *και συνεπώς έχουμε:*

$$\begin{aligned} \left(t^{-m\cdot r/d} - 1\right)^d &= \prod_{\zeta^r=1} \left(t^{-m} - \zeta^m\right) \overset{\cdot t^{mr}}{\Longrightarrow} \\ \left(1 - t^{m\cdot r/d}\right)^d &= \prod_{\zeta^r=1} \left(1 - (\zeta\cdot t)^m\right) \end{aligned} \tag{4.7}$$

Για τις σταθερές θέσεις $P \in \mathbb{P}_F$ *θέτουμε* $m := \deg P$ *και* $d := \mu\kappa\delta(r, m)$ *επομένως από τη σχέση (4.7) και το λήμμα (4.15) έχουμε*

$$\begin{aligned} \prod_{P'|P} \left(1 - t^{r\cdot \deg P'}\right) &= (1 - t^{r\cdot m/d})^d \\ &= \prod_{\zeta^r=1} \left(1 - (\zeta\cdot t)^m\right) \\ &= \prod_{\zeta^r=1} \left(1 - (\zeta\cdot t)^{\deg P}\right) \end{aligned} \tag{4.8}$$

Άρα από τις σχέσεις (4.8) και (4.6) έχουμε

$$\begin{aligned} Z_r(t^r) &= \prod_{P\in\mathbb{P}_F} \prod_{\zeta^r=1} \left(1 - (\zeta\cdot t)^{\deg P}\right)^{-1} \\ &= \prod_{\zeta^r=1} \prod_{P\in\mathbb{P}_F} \left(1 - (\zeta\cdot t)^{\deg P}\right)^{-1} \\ &= \prod_{\zeta^r=1} Z(\zeta t) \end{aligned}$$

□

Πόρισμα 4.21 (F. K. Schmidt) $\partial = 1$

Απόδειξη: *Όπως έχουμε πει ο αριθμός* ∂ *είναι θετικός ακέραιος άρα* $1 \le \partial \in \mathbb{Z}$ *και επιπλέον στην πολυωνυμική ταυτότητα της σχέσης (4.5) ο αριθμός* $r \in \mathbb{N}$ *άρα* $1 \le r \in \mathbb{Z}$*, συνεπώς μπορούμε να επιλέξουμε* $r = \partial$ *άρα για* $\zeta^\partial = 1$ *και εφόσον* $\partial \mid \deg P \; \forall\, P \in \mathbb{P}_F$ *έχουμε*

$$Z(\zeta t) = \prod_{P\in\mathbb{P}_F} \left(1 - (\zeta t)^{\deg P}\right)^{-1} = \prod_{P\in\mathbb{P}_F} \left(1 - t^{\deg P}\right)^{-1} = Z(t).$$

Χρησιμοποιώντας την προηγούμενη σχέση στο λήμμα (4.19) έχουμε $Z_\partial(t^\partial) = Z(t)^\partial$*. Από το λήμμα (4.15) το σώμα συναρτήσεων* F_r *είναι επέκταση του σώματος συναρτήσεων* F *συνεπώς η* $Z(t)$ *επεκτείνεται σε μία ρητή συνάρτηση του* $\mathbb{C}$ *την* $Z_\partial(t^\partial)$ *και από το πόρισμα (4.8) έχει απλό πόλο στο* $t = 1$*, συνεπώς και η* $Z(t)^\partial$ *έχει απλό πόλο τάξης* ∂ *στο* $t = 1$*. Άρα* $\partial = 1$*.* □

Πόρισμα 4.22

i. Κάθε σώμα συναρτήσεων $F/\mathbb{F}_q$ γένους 0 είναι ρητό και η ζήτα συνάρτησή του είναι

$$Z(t) = \frac{1}{(1-t)(1-qt)}.$$

ii. Αν το σώμα συναρτήσεων $F/\mathbb{F}_q$ είναι γένους $g \geq 1$ τότε η ζήτα συνάρτησή του είναι της μορφής $Z(t) = F(t) + G(t)$ με

$$F(t) = \frac{1}{q-1} \sum_{0 \leq \deg[C] \leq 2g-2} q^{\dim[C]} \cdot t^{\deg[C]}$$

και

$$G(t) = \frac{h}{q-1} \left(q^g \cdot t^{2g-1} \cdot \frac{1}{1-qt} - \frac{1}{1-t} \right).$$

Απόδειξη: *Αρχικά για το (i) να πούμε ότι κάθε σώμα συναρτήσεων γένους $g = 0$ έχει έναν διαιρέτη, έστω $A \in \mathcal{D}_F$ βαθμού $\deg A = 1$ και συνεπώς το αλγεβρικό σώμα συναρτήσεων $F/\mathbb{F}_q$ είναι ρητό. Το υπόλοιπο μέρος της απόδειξης έχει αποδειχθεί στην πρόταση (4.7) και χρησιμοποιώντας το πόρισμα (4.21) έχουμε τελειώσει.* □

Πρόταση 4.23 (Συναρτησιακή εξίσωση της ζήτα συνάρτησης) *Η **ζήτα συνάρτηση** του $F/\mathbb{F}_q$ ικανοποιεί την **συναρτησιακή εξίσωση***

$$Z(t) = q^{g-1} \cdot t^{2g-2} \cdot Z\left(\frac{1}{qt}\right). \tag{4.9}$$

Απόδειξη: *Θα διακρίνουμε δύο περιπτώσεις για το γένος g.*

Περίπτωση α: $g = 0$.

Αν θέσουμε στην συναρτησιακή εξίσωση (4.9) $g = 0$ θα πάρουμε

$$Z(t) = q^{-1} \cdot t^{-2} \cdot Z\left(\frac{1}{qt}\right)$$

το οποίο και θέλουμε να αποδείξουμε.
Τώρα αν στο πόρισμα (4.22.i) υπολογίσουμε την ζήτα συνάρτηση για $t = 1/qt$ θα πάρουμε

$$Z\left(\frac{1}{qt}\right) = \frac{qt^2}{(1-t)\cdot(1-qt)} \Rightarrow Z\left(\frac{1}{qt}\right) = qt^2 Z(t) \Rightarrow Z(t) = q^{-1} \cdot t^{-2} \cdot Z\left(\frac{1}{qt}\right).$$

Περίπτωση β: $g \geq 1$.

Από το πόρισμα (4.22.ii) μπορούμε να γράψουμε την ζήτα συνάρτηση στη μορφή

$$Z(t) = F(t) + G(t).$$

Αρχικά για θα αναφερθούμε στο $F(t)$, γνωρίζουμε από προηγούμενα ότι

$$F(t) = \frac{1}{q-1} \sum_{0 \le \deg[C] \le 2g-2} q^{\dim[C]} \cdot t^{\deg[C]}$$

Θέτουμε W να είναι ένας κανονικός διαιρέτης του F και από το θεώρημα Riemann-Roch έχουμε

$$\begin{aligned} F(t) &= \frac{1}{q-1} \sum_{0 \le \deg[C] \le 2g-2} q^{\deg[C]+1-g+\dim[W-C]} \cdot t^{\deg[C]} \\ &= \frac{1}{q-1} q^{g-1} t^{2g-2} \sum_{0 \le \deg[C] \le 2g-2} q^{\deg[C]-(2g-2)+\dim[W-C]} \cdot t^{\deg[C]-(2g-2)} \\ &= \frac{1}{q-1} q^{g-1} t^{2g-2} \sum_{0 \le \deg[C] \le 2g-2} q^{\dim[W-C]} \cdot \left(\frac{1}{qt}\right)^{\deg[W-C]} \\ &= q^{g-1} t^{2g-2} F\left(\frac{1}{qt}\right) \end{aligned}$$

Συνεπώς

$$F(t) = q^{g-1} t^{2g-2} F\left(\frac{1}{qt}\right) \tag{4.10}$$

Χρησιμοποιήσαμε ότι $\deg[W] = 2g-2$ και αν η κλάση διαιρετών $[C]$ τρέχει όλους τους διαιρέτες κλάσης με $0 \le \deg[C] \le 2g-2$ το ίδιο γίνεται και με την κλάση διαιρετών $[W-C]$.

Αναφερόμενοι τώρα στη $G(t)$, γνωρίζουμε από προηγούμενα ότι

$$G(t) = \frac{h}{q-1}\left(q^g \cdot t^{2g-1} \cdot \frac{1}{1-qt} - \frac{1}{1-t}\right)$$

Αν θέσουμε $t = 1/qt$ τότε

$$G\left(\frac{1}{qt}\right) = \frac{h}{q-1}\left(qt\frac{1}{1-qt} - q^{-g+1}t^{-2g+2}\frac{1}{1-t}\right)$$

και αν βγάλουμε κοινό παράγοντα την ποσότητα $q^{-g+1}t^{-2g+2}$ τότε

$$G\left(\frac{1}{qt}\right) = q^{-g+1}t^{-2g+2} \underbrace{\frac{h}{q-1}\left(q^g \cdot t^{2g-1} \cdot \frac{1}{1-qt} - \frac{1}{1-t}\right)}_{G(t)}$$

Συνεπώς

$$G(t) = q^{g-1} t^{2g-2} G\left(\frac{1}{qt}\right) \tag{4.11}$$

*Άρα από τις σχέσεις (4.10) και (4.11) προκύπτει η **συναρτησιακή εξίσωση** της **ζήτα συνάρτησης***

$$\begin{aligned} Z(t) &= F(t) + G(t) = q^{g-1}t^{2g-2}F(1/qt) + q^{g-1}t^{2g-2}G(1/qt) \quad \Rightarrow \\ Z(t) &= q^{g-1}t^{2g-2}\left[F(1/qt) + G(1/qt)\right] \quad \Rightarrow \\ Z(t) &= q^{g-1}t^{2g-2}Z(1/qt) \end{aligned}$$

□

Ορισμός 4.24 *Το πολυώνυμο* $L(t) := L_F(t) := (1-t)(1-qt)Z(t)$ *ονομάζεται* ***L - πολυώνυμο*** *του* $F/\mathbb{F}_q$.

Παρατηρήσεις 4.25

i. *Το L - πολυώνυμο είναι ένα πολυώνυμο με ακέραιους συντελεστές (προφανές) και είναι βαθμού* $\deg L(t) \leq 2g$, *το οποίο είναι προφανές αφού*

$$\deg Z(t) = \max\big\{\deg F(t)\,,\,\deg G(t)\big\} \leq \max\{2g-2\,,\,2g-3\} = 2g-2$$

και

$$\deg\big[(1-t)(1-qt)\big] = 2.$$

Συνεπώς,

$$\deg L(t) = \deg\big[(1-t)(1-qt\big] + \deg Z(t) \leq 2g.$$

ii. *Μέσω της* $L(t)$ *μπορούμε να προσδιορίσουμε τους αριθμούς* A_n *με* $n \geq 0$ *εφόσον*

$$Z(t) = \sum_{n=0}^{\infty} A_n t^n$$

άρα

$$L(t) = (1-t)(1-qt)\sum_{n=0}^{\infty} A_n t^n. \tag{4.12}$$

Θεώρημα 4.26

i. $L(t) \in \mathbb{Z}[t]$ *και* $\deg L(t) = 2g$.

ii. *Η συναρτησιακή εξίσωση του* $L(t)$ *είναι*

$$L(t) = q^g t^{2g} L\left(\frac{1}{qt}\right).$$

iii. $L(1) = h$, *την τάξη του* $F/\mathbb{F}_q$.

iv. $L(t) = a_0 + a_1 t + \cdots + a_{2g}t^{2g}$, *τότε ισχύουν τα ακόλουθα:*

(α') $a_0 = 1$ *και* $a_{2g} = q^g$.

(β') $a_{2g-i} = q^{g-i}a_i$ *με* $0 \leq i \leq g$.

(γ') $a_1 = N - (q+1)$ *όπου* $N = \big|\{P \in \mathbb{P}_F : \deg P = 1\}\big|$

v. *Το* $L(t)$ *παραγοντοποιείται στο* $\mathbb{C}[t]$ *στη μορφή*

$$L(t) = \prod_{i=1}^{2g}(1 - a_i t). \tag{4.13}$$

Οι μιγαδικοί αριθμοί $a_i \in \mathbb{C}$ *για* $i = 1, \ldots, g$ *είναι ακέραιοι αλγεβρικοί που μπορούν να διατεχθούν με τέτοιο τρόπο ώστε να ισχύει* $a_i \cdot a_{g+i} = q$ *για* $i = 1, \ldots, g$.

vi. *Αν* $L_r(t) := (1-t)(1-q^r t)Z_r(t)$ *ορίζουμε να είναι το* L*-πολυώνυμο της επέκτασης του σώματος σταθερών* $F_r = F\mathbb{F}_{q^r}$*, τότε*

$$L_r(t) = \prod_{i=1}^{2g}(1-a_i^r t), \tag{4.14}$$

όπου $a_i \in \mathbb{C}$ *με* $i = 1, \ldots, 2g$ *είναι οι αριθμοί που δίνονται από τη σχέση (4.13).*

Απόδειξη : *Αρχικά υποθέτουμε ότι* $g = 0$*, όμως όλα τα παραπάνω ισχύουν τετριμένα, επομένως θα αποδείξουμε το θεώρημα δεχόμενοι ότι το γένος* $g \geq 1$*.*

i. *Το έχουμε αποδείξει στην παρατήρηση (4.25).*

ii. *Στην πρόταση (4.23) απόδειξαμε ότι η συναρτησιακή είσωση του* $F/\mathbb{F}_q$ *είναι*

$$Z(t) = q^{g-1}t^{2g-2}Z\left(\frac{1}{qt}\right) \Rightarrow Z\left(\frac{1}{qt}\right) = q^{1-g}t^{2-2g}Z(t).$$

Αν θέσουμε $t = 1/qt$ *τότε*

$$L\left(\frac{1}{qt}\right) = \left(1-\frac{1}{qt}\right)\left(1-\frac{1}{t}\right)Z\left(\frac{1}{qt}\right)$$

άρα από την προηγούμενη σχέση συνεπάγεται ότι

$$\begin{aligned} L\left(\frac{1}{qt}\right) &= \frac{qt-1}{qt}\cdot\frac{t-1}{t}\cdot q^{1-g}\cdot t^{2-2g}Z(t) \Rightarrow \\ L\left(\frac{1}{qt}\right) &= q^{-g}\cdot t^{-2g}\underbrace{(1-t)\cdot(1-qt)\cdot Z(t)}_{L(t)} \Rightarrow \\ L\left(\frac{1}{qt}\right) &= q^{-g}\cdot t^{-2g}\cdot L(t) \end{aligned}$$

Συνεπώς

$$L(t) = q^g t^{2g} L\left(\frac{1}{qt}\right).$$

iii. *Γνωρίζουμε ότι η ζήτα συνάρτηση γράφεται ως*

$$Z(t) = F(t) + G(t)$$

όπου $F(t)$ *και* $G(t)$ *είναι οι συναρτήσεις για τις οποίες μιλήσαμε στο πόρισμα (4.22.ii), άρα*

$$\begin{aligned} L(t) &= (1-t)(1-qt)Z(t) \Rightarrow \\ L(t) &= (1-t)(1-qt)\big(F(t)+G(t)\big) \Rightarrow \\ L(t) &= (1-t)(1-qt)F(t) + (1-t)(1-qt)G(t) \end{aligned}$$

Ονομάζουμε $L_1(t) := (1-t)(1-qt)F(t)$ *και* $L_2(t) := (1-t)(1-qt)G(t)$, *αντικαθισούμε τις συναρτήσεις* $F(t)$ *και* $G(t)$ *από το πόρισμα (4.22.ii) και συνεπώς έχουμε*

$$L_1(t) = (1-t)(1-qt)F(t) = \frac{1-t}{q-1} \sum_{0 \leq \deg[C] \leq 2g-2} q^{\dim[C]} \cdot t^{\deg[C]} \quad (4.15)$$

και

$$\begin{aligned} L_2(t) &= (1-t)(1-qt)\frac{h}{q-1}\left(q^g \cdot t^{2g-1} \cdot \frac{1}{1-qt} - \frac{1}{1-t}\right) \Rightarrow \\ L_2(t) &= \frac{h}{q-1}\big(q^g \cdot t^{2g-1} \cdot (1-t) - (1-qt)\big) \end{aligned} \quad (4.16)$$

Επομένως η τιμή του L - πολυωνύμου για $t = 1$ *είναι* $L(1) = L_1(1) + L_2(1)$, *από τις σχέσεις (4.15) και (4.16) έχουμε ότι* $L_1(1) = 0$ *και* $L_2(1) = h$, *άρα*

$$L(1) = h.$$

iv. Δείξαμε στο πρώτο σκέλος του θεωρήματος αυτού ότι το L - πολυώνυμο είναι βαθμού $2g$, *άρα το L - πολυώνυμο είναι της μορφής* $L(t) = a_0 + a_1 t + \cdots + a_{2g}t^{2g}$. *Από την συναρτησιακή εξίσωση του L - πολυωνύμου έχουμε ότι* $L(t) = q^g t^{2g} L(1/qt)$, *συνεπώς*

$$\begin{aligned} L(t) &= q^g t^{2g}\left(a_0 + a_1\frac{1}{qt} + \cdots + a_{2g-1}\frac{1}{q^{2g-1}t^{2g-1}} + a_{2g}\frac{1}{q^{2g}t^{2g}}\right) \Rightarrow \\ L(t) &= a_0 q^g t^{2g} + a_1 q^{g-1}t^{2g-1} + \cdots + a_{2g-1}q^{-g+1}t + a_{2g}q^{-g} \Rightarrow \\ L(t) &= \frac{a_{2g}}{q^g} + \frac{a_{2g-1}}{q^{g-1}}t + \cdots + a_g t^g + \cdots + a_1 q^{g-1}t^{2g-1} + a_0 q^g t^{2g} \end{aligned}$$

άρα

$$a_0 + a_1 t + \cdots + a_g t^g + \cdots + a_{2g}t^{2g} = \frac{a_{2g}}{q^g} + \frac{a_{2g-1}}{q^{g-1}}t + \cdots + a_g t^g + \cdots + a_0 q^g t^{2g}$$

επομένως

$$\begin{array}{rclcrcl} a_0 &=& a_{2g}/q^g & \Rightarrow & a_{2g-0} &=& q^{g-0}a_0 \quad \Rightarrow \\ a_1 &=& a_{2g-1}/q^{g-1} & \Rightarrow & a_{2g-1} &=& q^{g-1}a_1 \quad \Rightarrow \\ & \vdots & & & \vdots & & \vdots \\ a_g &=& a_g & \Rightarrow & a_{2g-g} &=& q^{g-g}a_g \quad \Rightarrow \\ & \vdots & & & \vdots & & \vdots \\ a_{2g} &=& a_0 q^g & \Rightarrow & a_{2g-0} &=& q^{g-0}a_0 \end{array}$$

Επομένως από τον παραπάνω συλλογισμό δείξαμε ότι

$$a_{2g-i} = q^{g-i}a_i \text{ για } i = 0, \ldots, g. \quad (4.17)$$

Μας μένει λοιπόν να δείξουμε ότι $a_0 = 1$, $a_1 = N - (q+1)$ *και* $a_{2g} = q^g$, *για τα* a_0 *και* a_1 *θα συγκρίνουμε τους συντελεστές των* t^0 *και* t^1 *αντίστοιχα του* L *- πολυωνύμου της σχέσης (4.12) (για διευκόλυνση μας θα αναπτύξουμε το* L *- πολυώνυμο μόνο για τις τιμές που μας ενδιαφέρουν).*

$$\begin{aligned} a_0 + a_1 t &= (1-t)(1-qt)\big(A_0 + A_1 t\big) \Rightarrow \\ a_0 + a_1 t &= A_1 q t^3 + \big[A_0 q - A_1(q+1)\big]t^2 \\ &\quad + \big[A_1 - A_0(q+1)\big]t + A_0 \end{aligned} \tag{4.18}$$

Στη σχέση (4.18) απαλοίφουμε τους όρους $A_1 q t^3$ *και* $\big[A_0 q - A_1(q+1)\big]t^2$ *που δεν μας ενδιαφέρουν και επομένως η σχέση (4.18) γίνεται*

$$a_0 + a_1 t = A_0 + \big[A_1 - A_0(q+1)\big]t.$$

Συνεπώς

$$a_0 = A_0 \tag{4.19}$$

$$a_1 = A_1 - A_0(q+1) \tag{4.20}$$

Από τον ορισμό των A_i *με* $i = 1, \ldots, n$ *είχαμε ορίσει ότι* $A_0 = 1$ *και* $A_1 = \big\{\#P \in \mathbb{P}_F : \deg P = 1\big\} = N$, *(βλ. 4.1), επομένως οι σχέσεις (4.19) και (4.20) γίνονται*

$$a_0 = 1 \text{ και } a_1 = N - (q+1).$$

Χρησιμοποιώντας τώρα ότι $a_0 = 1$ *και τη σχέση (4.17) για* $i = 0$ *έχουμε*

$$a_{2g} = q^g a_0 \Rightarrow a_{2g} = q^g.$$

υ. Θεωρούμε το reciprocal πολυώνυμο

$$L^{\perp}(t) := t^{2g} L\left(\frac{1}{t}\right) = a_0 t^{2g} + a_1 t^{2g-1} + \cdots + a_{2g}. \tag{4.21}$$

Το reciprocal πολυώνυμο είναι ένα μονικό πολυώνυμο, εφόσον $a_0 = 1$ *όπως έχουμε δείξει, με συντελεστές στο* $\mathbb{Z}$, *συνεπώς οι ρίζες του reciprocal πολυωνύμου* $a_1, \ldots, a_{2g} \in \mathbb{C}$ *είναι ακέραιοι αλγεβρικοί αριθμοί και έχουμε*

$$L^{\perp}(t) = \prod_{i=1}^{2g} (t - a_i)$$

και από τη σχέση (4.21) για $t = 1/t$ *έχουμε*

$$L(t) = t^{2g} L^{\perp}\left(\frac{1}{t}\right) = t^{2g} \prod_{i=1}^{2g} \frac{(1 - a_i t)}{t} = \prod_{i=1}^{2g} (1 - a_i t).$$

Παρατηρούμε ότι οι ρίζες του $L^{\perp}(t)$ είναι αντίστροφες από τις ρίζες του $L(t)$ εφόσον $L(1/a_i)=0$. Μπορούμε τώρα εύκολα να δούμε ότι η συναρτησιακή εξίσωση του reciprocal πολυωνύμου από το (ii) είναι

$$L^{\perp}(t)=q^g\frac{1}{t^{2g}}L^{\perp}\left(\frac{q}{t}\right).$$

Προφανώς οι ρίζες του reciprocal πολυωνύμου είναι εκείνες για τις οποίες

$$L^{\perp}(t)=0\Longleftrightarrow L^{\perp}\left(\frac{q}{t}\right)=0.$$

Επομένως οι ρίζες είναι

$$a_1,\frac{q}{a_1},\ldots,a_k,\frac{q}{a_k},\underbrace{q^{1/2},\ldots,q^{1/2}}_{m-\text{φορές}},\underbrace{-q^{1/2},\ldots,-q^{1/2}}_{n-\text{φορές}}.$$

Τα m , n είναι τέτοια ώστε το γινόμενο των ριζών να μας δίνει τον σταθερό όρο της σχέσης (4.21), δηλαδή το $a_{2g}=q^g$, επομένως

$$a_1\cdot\frac{q}{a_1}\cdot\cdots\cdot a_k\cdot\frac{q}{a_k}\cdot\left(q^{1/2}\right)^m\cdot\left(-q^{1/2}\right)^n=q^g. \tag{4.22}$$

Εφόσον q^g είναι μία θετική ποσότητα συνεπάγεται ότι ο αριθμός n είναι άρτιος, συνεπώς η σχέση (4.22) διαμορφώνεται ως εξής:

$$q^{k+(1/2)\cdot(m+n)}=q^g$$

άρα

$$k+\frac{1}{2}\cdot(m+n)=g\Rightarrow m+n+2k=2g$$

και από τη σχέση αυτή συμπεραίνουμε ότι και ο αριθμός m είναι άρτιος. Μπορούμε συνεπώς να αναδιατάξουμε τους αριθμούς $a_1,\ldots,a_{2g}$ έτσι ώστε $a_{g+i}=q/a_i\Rightarrow a_ia_{g+i}=q$ για $i=1,\ldots,g$.

vi. Θέλουμε να δείξουμε ότι το L - πολυώνυμο του $F_r=F\mathbb{F}_{q^r}$ είναι:

$$L_r(t)=\prod_{i=1}^{2g}\left(1-a_i^rt\right). \tag{4.23}$$

Χρησιμοποιώντας την σχέση (4.4) της πρότασης (4.19) και το L - πολυώνυμο για $t=\zeta t$,

$$L(\zeta t)=(1-\zeta t)(1-q\zeta t)Z(\zeta t) \tag{4.24}$$

έχουμε:

$$\begin{aligned}
L_r(t^r) &= (1-t^r)(1-q^rt^r)Z_r(t^r)\overset{(4.4)}{=}(1-t^r)(1-q^rt^r)\prod_{\zeta^r=1}Z(\zeta t)\\
&= (1-t^r)(1-q^rt^r)\prod_{\zeta^r=1}\frac{L(\zeta t)}{(1-\zeta t)(1-q\zeta t)}\overset{(4.24)}{=}\prod_{\zeta^r=1}L(\zeta t)\\
&= \prod_{i=1}^{2g}\prod_{\zeta^r=1}\left(1-a_i\zeta t\right)=\prod_{i=1}^{2g}\left(1-a_i^rt^r\right).
\end{aligned}$$

Προφανώς αν θέσουμε $t^r=t$, τότε αποδείξαμε την σχέση (4.23).

□

Παρατήρηση 4.27 *Το προηγούμενο θεώρημα μας δείχνει ότι οι αριθμοί*

$$N(F) := N = \big|\{P \in \mathbb{P}_F : \deg P = 1\}\big| \tag{4.25}$$

εύκολα υπολογίζονται αν γνωρίζουμε το L - πολυώνυμο του $F/\mathbb{F}_q$. Γενικότερα θεωρούμε ότι για $r \geq 1$ ο αριθμός

$$N_r := N(F_r) = \big|\{P \in \mathbb{P}_{F_r} : \deg P = 1\}\big|,$$

όπου $F_r = F\mathbb{F}_{q^r}$ είναι η επέκταση του σώματος σταθερών του $F/\mathbb{F}_q$ βαθμού r.

Πόρισμα 4.28 *Για κάθε $r \geq 1$,*

$$N_r = q^r + 1 - \sum_{i=1}^{2g} a_i^r,$$

όπου $a_1, \ldots, a_{2g} \in \mathbb{C}$ είναι οι αντίστροφοι των ριζών του $L(t)$ $\big($ή διαφορετικά είναι οι ρίζες του $L^{\perp}(t)\big)$. Ειδικότερα, εφόσον $N_r = N(F)$ έχουμε

$$N(F) = q + 1 - \sum_{i=1}^{2g} a_i.$$

Απόδειξη: *Στο θεώρημα (4.26.iv) είδαμε ότι $N - (q+1)$ είναι ο συντελεστής του t του πολυωνύμου $L(t)$ και εφόσον $N_r = N(F)$ έχουμε ότι $N_r - (q^r + 1)$ είναι ο συντελεστής του t του πολυωνύμου $L_r(t)$. Από την άλλη, εφόσον*

$$L_r(t) = \prod_{i=1}^{2g} \big(1 - a_i^r t\big)$$

ο συντελεστής του t είναι ο $-\sum_{i=1}^{2g} a_i^r$.

Συνεπώς

$$N_r = q^r + 1 - \sum_{i=1}^{2g} a_i^r$$

και γενικότερα εφόσον $N_r = N(F)$ έχουμε

$$N(F) = q + 1 - \sum_{i=1}^{2g} a_i.$$

□

Σημείωση 4.29 *Στην περίπτωση που γνωρίζουμε τους αριθμούς N_r για κατάλληλο το πλήθος r, τότε ένα από τα N_r μπορεί να υπολογίσει τους συντελεστές του $L(t)$.*

Πόρισμα 4.30 *Έστω το L-πολυώνυμο του $F/\mathbb{F}_q$ να είναι*

$$L(t) = \sum_{i=1}^{2g} a_i t^i$$

και $S_r := N_r - (q^r + 1)$, τότε έχουμε:

i.
$$L'(t)/L(t) = \sum_{r=1}^{\infty} S_r r^{r-1}. \tag{4.26}$$

ii. $a_0 = 1$ *και*
$$ia_i = S_i a_0 + S_{i-1} a_1 + \cdots + S_1 a_{i-1} \tag{4.27}$$
για $i = 1, \ldots, g$.

Επομένως, δοθέντων N_i με $i = 1, \ldots, g$ μπορούμε να προσδιορίσουμε το $L(t)$ από από τη σχέση (4.27) και τις εξισώσεις $a_{2g-i} = q^{g-i} a_i$ για $i = 1, \ldots, g$ (βλ. θεώρημα (4.26.iv)).

Απόδειξη:

i. Δείξαμε στο θεώρημα (4.26.υ) ότι

$$L(t) = \prod_{i=1}^{2g} (1 - a_i t),$$

και επιπλέον από στο προηγούμενο πόρισμα είδαμε ότι

$$-\sum_{i=1}^{2g} a_i^r = N_r - (q^r + 1) \stackrel{\text{ορ}}{=} S_r$$

συνεπώς

$$\begin{aligned} \frac{L'(t)}{L(t)} &= \sum_{i=1}^{2g} \frac{-a_i}{(1 - a_i t)} = \sum_{i=1}^{2g} \left((-a_i) \cdot \sum_{r=0}^{\infty} (a_i t)^r \right) \\ &= \sum_{r=1}^{\infty} \left(-\sum_{i=1}^{2g} a_i^r \right) t^{r-1} = \sum_{r=1}^{\infty} S_r t^{r-1}. \end{aligned}$$

ii. Γνωρίζουμε από το θεώρημα (4.26) ότι $a_0 = 1$, και από τη σχέση (4.26) έχουμε ότι

$$\begin{aligned} L'(t) &= L(t) \cdot \sum_{r=1}^{\infty} S_r t^{r-1} \Rightarrow \\ a_1 + 2a_2 t + \cdots + (2g) a_{2g} t^{2g-1} &= \left(a_0 + a_1 t + \cdots + a_{2g} t^{2g} \right) \cdot \sum_{r=1}^{\infty} S_r t^{r-1} \\ &\Longrightarrow \end{aligned}$$

$$\begin{aligned} a_1 &= a_0 S_1 \\ 2a_2 &= S_2 a_0 + S_1 a_1 \\ 3a_3 &= S_3 a_0 + S_2 a_1 + S_1 a_2 \\ 4a_4 &= S_4 a_0 + S_3 a_1 + S_2 a_2 + S_1 a_3 \\ &\vdots \end{aligned}$$

Θέτουμε i τον συνελεστή του a του πρώτου μέλους (≡ δείκτη του a). Παρατηρούμε λοιπόν ότι οι δείκτες του S ξεκινούν από το i και φθάνουν στο 1 και οι δείκτες του a ξεκινούν από το 0 και φθάνουν στο $i-1$. Άρα οι συντελεστές των t^{i-1} για $i = 1, \ldots, g$ υπολογίζονται από την σχέση (4.27).

□

4.2 Το θεώρημα των Hasse-Weil

Στην παράγραφο αυτή θα δώσουμε μία απόδειξη του θεωρήματος των Hasse-Weil. Η απόδειξη που θα δώσουμε οφείλεται στον Bombieri. Με $F/\mathbb{F}_q$ θα συμβολίζουμε ένα σώμα συναρτήσεων με σώμα σταθερών το $\mathbb{F}_q$ και το οποίο έχει γένος g. Γράφουμε την ζήτα συνάρτηση ως

$$Z_F(t) = L_F(t)/(1-t)(1-qt).$$

Με $\alpha_1, \ldots, \alpha_{2g}$ θα συμβολίζουμε τα αντίστροφα των ριζών του L_F. Θέτουμε

$$N(F) = \#\{P \in \mathbb{P}_F : \deg(P) = 1\}$$

και θεωρούμε την επέκταση των σταθερών $F_r = F\mathbb{F}_{q^r}$ και θέτουμε $N_r = N(F_r)$. Το αποτέλεσμα που θέλουμε να αποδείξουμε είναι το

Θεώρημα 4.31 (Hasse-Weil) *Τα αντίστροφα των ριζών του πολυωνύμου $L_F(t)$ ικανοποιούν την*

$$|\alpha_i| = q^{1/2}, \text{ για } i = 1, \ldots, 2g.$$

Το θεώρημα των Hasse-Weil είναι γνωστό ως η εικασία του Riemann για σώματα συναρτήσεων. Πράγματι όπως έχουμε ορίσει η κλασική συνάρτηση του Riemann δίνεται από τον

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s},$$

όπου $s \in \mathbb{C}$ και $\mathrm{Re}(s) > 1$. Ορίζουμε την απόλυτη νόρμα ενός divisor A ως

$$\mathcal{N}(A) := q^{\deg(A)}.$$

Έτσι η απόλυτη νόρμα ενός πρώτου διαιρέτη είναι το πλήθος των στοιχείων που έχει το σώμα υπολοίπων $\mathbb{F}_P$. Η συνάρτηση

$$\zeta_F(s) := Z_F(q^{-s}),$$

μπορεί να γραφεί ως

$$\zeta_F(s) = \sum_{n=0}^{\infty} A_n q^{-sn} = \sum_{A \in \mathcal{D}_F, A \geq 0} \mathcal{N}(A)^{-s},$$

το οποίο είναι το ανάλογο με την ζήτα συνάρτηση του σώματος των ρητών αριθμών και σε πλήρη αναλογία με του ορισμό των ζήτα συναρτήσεων σωμάτων αριθμών. Παρατηρούμε ότι το θεώρημα των Hasse-Weil λέει ότι

$$\zeta_F(s) = 0 \Rightarrow Z_F(q^{-s}) = 0 \Rightarrow |q^{-s}| = q^{-1/2}.$$

Αφού δε $|q^{-s}| = q^{-\mathrm{Re}(s)}$, *η τελευταία εξίσωση μεταφράζεται σε*

$$\zeta_F(s) = 0 \Rightarrow \mathrm{Re}(s) = 1/2,$$

μία πολύ σημαντική έκφραση του θεωρήματος των Hasse-Weil είναι το παρακάτω

Θεώρημα 4.32 *Το πλήθος των θέσεων βαθμού ένα στο σώμα συναρτήσεων* $F/\mathbb{F}_q$ *μπορεί να εκτιμηθεί με βάση την παρακάτω ανισότητα:*

$$|N - (q+1)| \leq 2gq^{1/2}.$$

Απόδειξη: *Έχουμε ότι*

$$N - (q+1) = -\sum_{i=1}^{2g} \alpha_i.$$

και το ζητούμενο φράγμα προκύπτει άμεσα. □

Προχωρούμε τώρα στην απόδειξη του θεωρήματος των Hasse-Weil

Λήμμα 4.33 *Έστω* $m \geq 1$. *Το θεώρημα των Hasse-Weil ισχύει για το σώμα* $F/\mathbb{F}_q$ *αν και μόνο αν ισχύει για την επέκταση* $F_m/\mathbb{F}_{q^m}$.

Απόδειξη: *Τα αντίστροφα των ριζών του* $L_F(t)$ *είναι τα* $\alpha_1, \ldots, \alpha_{2g}$. *Από το θεώρημα (4.26) τα αντίστροφα των ριζών του* $L_m(t)$ *είναι τα* $\alpha_1^m, \ldots, \alpha_{2g}^m$, *όπου* $L_m(t)$ *είναι το* L*-πολυώνυμο του σώματος* F_m. *Η απόδειξη του λήμματος προκύπτει αν παρατηρήσουμε ότι*

$$|\alpha_i| = q^{1/2} \Leftrightarrow |\alpha_i^m| = (q^m)^{1/2}.$$

□

Το παρακάτω λήμμα ανάγει την απόδειξη του θεωρήματος Hasse-Weil στην απόδειξη μίας ανισότητας που μοιάζει με το φράγμα του θεωρήματος 4.32.

Λήμμα 4.34 *Αν υπάρχει μία σταθερά* $c \in \mathbb{R}$ *για την οποία για κάθε* $r \geq 1$ *ισχύει η ανισότητα*

$$|N_r - (q^r + 1)| \leq cq^{r/2} \tag{4.28}$$

τότε το θεώρημα των Hasse-Weil είναι αληθές.

Απόδειξη: *Είναι γνωστό ότι* $|N_r - (q^r + 1) = \sum_{i=1}^{2g} \alpha_i^r$, *οπότε η (4.28) μας δίνει*

$$\left| \sum_{i=1}^{2g} \alpha_i^r \right| \leq cq^{r/2}, \tag{4.29}$$

για κάθε $r \geq 1$. *Θεωρούμε την μερόμορφη συνάρτηση*

$$H(t) := \sum_{i=1}^{2g} \frac{\alpha_i t}{1 - \alpha_i t}.$$

Θέτουμε $\rho := \min\{\alpha_i^{-1} : 1 \leq i \leq 2g\}$.*Η ακτίνα σύγκλισης του αναπτύγματος της* $H(t)$ *σε δυναμοσειρά υπολογίζεται σε* ρ, *αφού τα* $(\alpha_1^{-1}, \ldots, \alpha_{2g}^{-1})$ *είναι οι μοναδικοί πόλοι της* $H(t)$ *και* ρ *είναι η απόσταση του* 0 *από κάθε πόλο. Από την άλλη για* $|t| < \rho$ *έχουμε*

$$H(t) = \sum_{i=1}^{2g} \sum_{r=1}^{\infty} (\alpha_i t)^r = \sum_{i=1}^{\infty} \sum_{i=1}^{2g} \alpha_i^r t^r.$$

Από τα θεωρήματα σύγκλισης της γεωμετρικής σειράς η παραπάνω σειρά αυτή συγλίνει για $|t| \leq q^{1/2}$, *συνεπώς* $q^{1/2} \leq \rho$. *Άρα έχουμε ότι* $q^{1/2} \geq |\alpha_i|$ *για* $i = 1, \ldots, 2g$. *Αφού* $\prod_{i=1}^{2g} \alpha_i = q^g$ $\big($*από το θεώρημα (4.26)*$\big)$ *καταλήγουμε στο ότι* $|\alpha_i| = q^{1/2}$. □

Παρατηρούμε ότι η εξίσωση (4.28) είναι ισοδύναμη με ένα άνω και κάτω φράγμα για το N_r. *Δηλάδη η (4.28) είναι ισοδύναμη με την ύπαρξη δύο σταθερών* $c_1, c_2 > 0$ *ώστε*

$$N_r \leq q^r + 1 + c_1 q^{r/2} \tag{4.30}$$

και

$$N_r \geq q^r + 1 - c_2 q^{r/2} \tag{4.31}$$

για κάθε $r \geq 1$. *Το θεώρημα των Hasse-Weil θα έχει αποδειχτεί αρκεί να αποδείξουμε τις (4.30) και (4.31) για μία κατάλληλη επέκταση των σταθερών του* F.

Πρόταση 4.35 *Υποθέτουμε ότι το* $F/\mathbb{F}_q$ *ικανοποιεί τα παρακάτω*

- *Το* q *είναι τετράγωνο*
- $q > (g+1)^4$.

Τότε το πλήθος $N = N(F)$ *των θέσεων του* $F/\mathbb{F}_q$ *βαθμού ένα μπορεί να εκτιμηθεί από την*

$$N < (q+1) + (2g+1)q^{1/2}.$$

Απόδειξη: *Μπορούμε να υποθέσουμε ότι υπάρχει μία θέση* Q *στο* $\mathbb{P}_F$ *βαθμού ένα (διαφορετικά* $N = 0$ *και η πρόταση είναι τετριμμένη). Θέτουμε*

$$q_0 = q^{1/2}, \;\; m := q_0 - 1 \text{ και } n := 2g + q_0.$$

Παρατηρούμε ότι

$$r := q - 1 + (2g+1)q^{1/2} = m + nq_0.$$

Θα λέμε ότι ένας φυσικός αριθμός i είναι πολικός αριθμός στο Q αν και μόνο αν υπάρχει $x \in F$ ώστε $(x)_\infty = iQ$, δηλαδή αν υπάρχει συνάρτηση x που να παρουσιάζει μόνο στο Q πόλο τάξης i. Θέτουμε

$$T := \{i | 0 \leq i \leq m \text{ και το } i \text{ είναι πολικός αριθμός του } Q\}$$

Για κάθε $i \in T$ διαλέγουμε ένα $u_i \in F$, ώστε $(u_i)_\infty = iQ$. Το σύνολο $\{u_i, i \in T\}$ αποτελεί μία βάση του διανυσματικού χώρου $\mathcal{L}(mQ)$. Θεωρούμε του χώρο

$$\mathcal{L} := \mathcal{L}(mQ) \cdot \mathcal{L}(nQ)^{q_0} \subseteq \mathcal{L}(rQ).$$

Εξ' ορισμού δηλαδή το σύνολο $\mathcal{L}$ αποτελείται από τα πεπερασμένα αθροίσματα της μορφής $\sum x_\nu y_\nu^{q_0}$ με $x_\nu \in \mathcal{L}(mQ)$ και $y_\nu \in \mathcal{L}(nQ)$. Το σύνολο $\mathcal{L}$ είναι ένας διανυσματικός χώρος υπέρ το $\mathbb{F}_q$ και $\mathcal{L} \subseteq \mathcal{L}(rQ)$.

Θα κατασκευάσουμε ένα στοιχείο $0 \neq x \in \mathcal{L}$ ώστε να έχει ρίζες σε όλα τα $P \in \mathbb{P}_F$ βαθμού ένα και είναι διαφορετικά του Q. Αν έχουμε κατασκευάσει ένα τέτοιο στοιχείο τότε ο $(x)_0$ θα έχει βαθμό:

$$\deg(x)_0 \geq N - 1.$$

Από την άλλη, αφού $x \in \mathcal{L} \subset \mathcal{L}(rQ)$ θα έχουμε

$$\deg(x)_0 = \deg(x)_\infty \leq r = q - 1 + (2g+1)q^{1/2}.$$

Ο συνδιασμός των δύο παραπάνω ανισοτήτων θα μας δώσει το επιθυμητό αποτέλεσμα.

Για να καταλήξουμε στην κατασκευή του παραπάνω επιθυμητού x θα αποδείξουμε τους ισχυρισμούς:

Ισχυρισμός 1. *Κάθε $y \in \mathcal{L}$ μπορεί να γραφτεί μονοσήμαντα στην μορφή*

$$y = \sum_{i \in T} u_i z_i^{q_0} \text{ με } z_i \in \mathcal{L}(nQ), \tag{4.32}$$

όπου η $\{u_i | i \in T\}$ είναι η βάση του $\mathcal{L}(mQ)$ που ορίσαμε παραπάνω. Το ότι κάθε στοιχείο y γράφεται στην μορφή (4.32) είναι σαφές από τον ορισμό του $\mathcal{L}$. Θα αποδείξουμε την μοναδικότητα. Ας υποθέσουμε ότι υπάρχει μία έκφραση

$$0 = \sum_{i \in T} u_i x_i^{q_0} \tag{4.33}$$

όπου τα $x_i \in \mathcal{L}(nQ)$ και δεν είναι όλα 0. Για ένα δείκτη $i \in T$ με $x_i \neq 0$ έχουμε

$$v_Q(u_i x_i^{q_0}) \equiv v_Q(u_i) \equiv -i mod q_0.$$

Αφού $m = q_0 - 1$ οι αριθμού $i \in T$ είναι ανά δύο διαφορετικοί modulo q_0. Συνεπώς η τριγωνική ανισότητα δίνει

$$v_Q(\sum_{i \in T} u_i x_i^{q_0}) = \min\{v_Q(u_i x_i^{q_0}) : i \in T\} \neq \infty.$$

Άρα η (4.33) δεν μπορεί να ισχύει, άτοπο.

Ορίζουμε την συνάρτηση $\lambda : \mathcal{L} \to \mathcal{L}\big((q_0 m + n)Q\big)$ *η οποία δίνεται από τον τύπο:*

$$\lambda\left(\sum_{i\in T} u_i z_i^{q_0}\right) := \sum_{i\in T} u_i^{q_0} z_i,$$

όπου τα $z_i \in \lambda(nQ)$. *Από του ισχυρισμό ένα η συνάρτηση είναι καλά ορισμένη. Παρατηρούμε ότι δεν είναι* $\mathbb{F}_q$ *γραμμική αλλά είναι ένας ομομορφισμός των αβελιανών ομάδων των διανυσματικών χώρων* $\mathcal{L}$ *και* $\mathcal{L}\big((q_0 m + n)Q\big)$.

Ισχυρισμός 2 *Ο πυρήνας της* λ *δεν είναι* 0. *Αφού ο* λ *είναι ένας ομομορφισμός από το* $\mathcal{L}$ *στο* $\mathcal{L}\big((q_0 m + n)Q\big)$, *αρκεί να δείξουμε ότι*

$$\dim \mathcal{L} > \dim \mathcal{L}\big((q_0 m + n)Q\big). \tag{4.34}$$

Από τον ισχυρισμό 1 και από το θεώρημα Riemann-Roch έχουμε

$$\dim \mathcal{L} = \dim(mQ) \cdot \dim(nQ) \geq (m + 1 - g)(n + 1 - g).$$

Από την άλλη, αφού

$$q_0 m + n = q_0(q_0 - 1) + (2g + q_0) = 2g + q_0$$

έχουμε

$$\dim \mathcal{L}\big((q_0 m + n)Q\big) = (2g + q) + 1 - g = g + q + 1.$$

Συνεπώς η (4.34) προκύπτει αν μπορέσουμε να δείξουμε ότι

$$(m + 1 - g)(n + 1 - g) > g + q + 1. \tag{4.35}$$

Θεωρούμε τις παρακάτω ισοδυναμίες

$$\begin{aligned}
&(m + 1 - g)(n + 1 - g) > g + q + 1 \\
\Leftrightarrow\ &(q_0 - g)(2g + q_0 + 1 - g) > g + q_1 \\
\Leftrightarrow\ &q - g^2 + q_0 - g > g + q + 1 \\
\Leftrightarrow\ &q_0 > g^2 + 2g + 1 = (g + 1)^2 \\
\Leftrightarrow\ &q > (g + 1)^4.
\end{aligned}$$

Η τελευταία όμως ανισότητα είναι κομάτι των υποθέσεων που έχουμε κάνει, οπότε η (4.35) έχει αποδειχτεί.

Ισχυρισμός 3. *Έστω* $0 \neq x \in \mathcal{L}$ *ένα στοιχείο του πυρήνα του* $\mathcal{L}$ *και* $P \neq Q$ *είναι μία θέση βαθμού 1. Τότε* $x(P) = 0$.

Παρατηρούμε ότι $y(P) \neq \infty$ *για κάθε* $y \in \mathcal{L}$ *αφού το* Q *είναι ο μοναδικός πόλος της συνάρτησης* y. *Επιπλέον, αφού* $\mathbb{F}_q$ *είναι το σώμα υπολοίπων του* P, *έχουμε*

ότι $y(P)^q = y(P)$. *Έστω λοιπόν ένα στοιχείο* $x \in \mathcal{L}$ *με* $\lambda(x) = 0$. *Γράφουμε* $x = \sum_{i\in T} u_i z_i^{q_0}$ *και έχουμε*

$$x(P)^{q_0} = \left(\sum_{i\in T} u_i(P)\cdot z_i(P)^{q_0}\right)^{q_0} =$$

$$= \sum_{i\in T} u_i^{q_0}(P)\cdot z_i(P)^q =$$

$$\left(\sum_{i\in T} u_i^{q_0} z_i\right)(P) = \lambda(x)(P) = 0.$$

και ο ισχυρισμός έχει αποδειχτεί. □

Η προηγούμενη πρόταση μας δίνει ένα άνω φράγμα για το πλήθος των θέσεων βαθμού ένα. Προκειμένου να αποδείξουμε το κάτω φράγμα θα χρειαστούμε ένα ομαδοθεωρητικό λήμμα:

Λήμμα 4.36 *Θεωρούμε μία ομάδα* G' *η οποία είναι το ευθή γινόμενο*

$$G' = \langle\sigma\rangle \times G$$

μίας κυκλικής ομάδας $\langle\sigma\rangle$ *και μίας υποομάδας* $G \subseteq G'$ *ώστε* $|G| = m$, $|\sigma| = n$ *και* $m \mid n$. *Αν η* $H \subseteq G'$ *είναι μία υποομάδα της* G' *ώστε*

$$|H| = ne \text{ και } |H \cap G| = e, \tag{4.36}$$

τότε υπάρχουν ακριβώς e *το πλήθος υποομάδες* $U \subseteq H$ *ώστε*

$$U \text{ είναι κυκλική τάξης } n \text{ και } U \cap G = \{1\}. \tag{4.37}$$

Απόδειξη: *Για ένα στοιχείο* $\tau \in G$ *θεωρούμε την κυκλική υποομάδα* $\langle\sigma\tau\rangle \subseteq G'$. *Το γινόμενο είναι ευθή άρα* $\sigma\tau = \tau\sigma$ *και συνεπώς* $|\sigma\tau| = |\sigma| = n$, *αφού* $|\tau| \mid n$. *Τα στοιχεία* $\lambda \in G'$ *έχουν μοναδική αναπαράσταση ως γινόμενα* $\lambda = \sigma^i\rho$, *όπου* $\rho \in G$. *Άρα* $\langle\sigma\tau\rangle \cap G = \{1\}$ *και* $\langle\sigma\tau\rangle \neq \langle\sigma\tau'\rangle$ *για* $\tau \neq \tau'$. *Κάθε* $\tau \in G$ *δίνει λοιπόν μία διαφορετική υποομάδα* $U \subset G'$ *με τις ιδιότητες (4.37).*

Η υποομάδα $G \subseteq G'$ *είναι κανονική οπότε* $H/(H \cap G) \cong HG/G$. *Συνεπώς οι ιδιότητες (4.36) δίνουν ότι* $HG = G'$ *αφού το πηλίκο* HG/G *έχει τάξη* n, *και επιπλέον* $H/(H \cap G)$ *είναι κυκλική τάξης* n. *Διαλέγουμε ένα στοιχείο* $\lambda_0 \in H$ *το οποίο να έχει τάξη* n *modulo* $H \cap G$. *Γράφουμε* $\lambda_0 = \sigma^a\tau'$, *με* $\tau' \in G$ *και* $a \in \mathbb{Z}$. *Παρατηρούμε ότι* $(a, n) = 1$, *διαφορετικά θα υπήρχε* d *με* $1 \leq d < n$ *ώστε* $\sigma^{ad} = 1$, *και τότε* $\lambda_0^d = (\tau')^d \in H \cap G$, *και η τάξη του* λ_0 *modulo* $H \cap G$ *θα ήταν μικρότερη του* n.

Μπορούμε λοιπόν να διαλέξουμε κατάλληλη δύναμη t *ώστε το* $\lambda = \lambda_0^t$ *να έχει αναπαράσταση της μορφής* $\lambda = \sigma\tau_0$, *με* $\tau_0 \in G$. *Πράγματι αρκεί να διαλέξουμε ως* t *του αντίστοφο του* a *modulo* n. *Ας υποθέσουμε ότι,* $H \cap G = \{\psi_1, \ldots, \psi_e\}$. *Ορίζουμε*

$$U^{(j)} = \langle\sigma\tau\psi_j\rangle \text{ για } j = 1, \ldots, e.$$

Οι υποομάδες $U^{(j)} \subseteq H$ είναι κυκλικές τάξης n και είναι ανά δυό διαφορετικές και $U^{(j)} \cap F = \{1\}$.

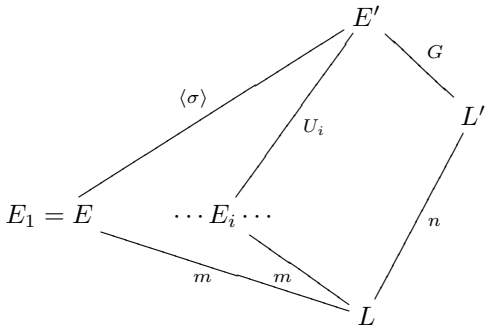
Απομένει να δείξουμε ότι η H δεν περιέχει άλλη κυκλική υποομάδα U τάξης n με $U \cap G = \{1\}$. Πράγματι, έστω U μία τέτοια υποομάδα που να ικανοποιεί την (4.37). Όπως παραπάνω μπορούμε να βρούμε ένα γεννήτορα της U της μορφής $\sigma\tau_1$ με $\tau_1 \in G$. Αφού $\sigma\tau_1 \in H$ και $\sigma\tau_0 \in H$ έχουμε:

$$\tau_0^{-1}\tau_1 = (\sigma\tau_0)^{-1}(\sigma\tau_1) \in H \cap G = \{\psi_1, \ldots, \psi_e\}.$$

Δηλαδή $\tau_1 = \tau_0\psi_j$ για κάποιο j και $U = \langle\sigma\tau_1\rangle = \langle\sigma\tau_0\psi_j\rangle = U^{(j)}$. □

Η επόμενη πρόταση είναι το βασικό βήμα στην απόδειξη ενός κάτω φράγματος για το N_r. Θεωρούμε ότι έχουμε την εξής κατάσταση E/L είναι μία επέκταση του Galois από σώματα συναρτήσεων βαθμού $[E : L] = m$ και υποθέτουμε ότι το $\mathbb{F}_q$ είναι το πλήρες σώμα των σταθερών των E και L. Διαλέγουμε ένα ακέραιο $n > 0$ με $m \mid n$ και θέτουμε $E' := E\mathbb{F}_{q^n}$ και $L' := L\mathbb{F}_{q^n} \subseteq E'$ να είναι οι επεκτάσεις των σωμάτων συναρτήσεων που προκείπτουν με επέκταση των σταθερών. Η επέκταση E'/L είναι Galois με ομάδα Galois την $G' = \langle\sigma\rangle \times G$, όπου $G := \mathrm{Gal}(E'/L') \cong \mathrm{Gal}(E/L)$ και σ είναι ο αυτομορφισμός του Frobenious του σώματος E'/E, δηλαδή $\sigma(z) = z$ για $z \in E$ και $\sigma(a) = a^q$ για $a \in \mathbb{F}_{q^n}$. Από το προηγούμενο λήμμα έχουμε ότι το G' περιέχει ακριβώς m το πλήθος κυκλικές υποομάδες $U \subseteq G'$ με $|U| = n$ και $U \cap G = \{1\}$, ας τις ονομάσουμε $U_1, \ldots, U_n$. Υποθέτουμε ότι $U_1 = \langle\sigma\rangle$.

Ας είναι E_i το σταθερό σώμα της U_i για $i = 1, \ldots, m$. Έχουμε ότι $E_1 = E$ και μπορούμε να σχηματίσουμε τον παρακάτω πύργο σωμάτων:



Θα συμβολίζουμε με $g(E_i)$ το γένος του E_i και με $N(E_i)$ (αντ. με $N(L)$) το πλήθος των θέσεων βαθμού ένα των σωμάτων E_i (αντ. L).

Πρόταση 4.37 *Με τους παραπάνω συμβολισμούς και υποθέσεις ισχύουν τα εξής*

1. *Το $\mathbb{F}_q$ είναι το πλήρες σώμα των σταθερών του E_i για $1 \le i \le m$.*
2. *Το $E' = E_i\mathbb{F}_{q^n}$ και $g(E_i) = g(E)$ για $i = 1, \ldots, m$.*
3. *$m \cdot N(L) = \sum_{i=1}^{m} N(E_i)$.*

Απόδειξη : *Θα αποδείξουμε πρώτα τα 1,2. Παρατηρούμε ότι* $U_i \cap G = \{1\}$. *Συνεπώς από θεωρία Galois το* E' *είναι η σύνθεση των σωμάτων* E_i *και* L', *δηλαδή* $E' = E_iL' = E_iL\mathbb{F}_{q^n} = E_i\mathbb{F}_{q^n}$ *είναι η σταθερή επέκταση του* E_i *με* $\mathbb{F}_{q^n}$. *Αφού* $[E' : E_i] = |U_i| = n$ *το παραπάνω έχει ώς συνέπεια ότι το* $\mathbb{F}_q$ *είναι το πλήρες σώμα των σταθερών του* E_i. *Το γένος είναι γεωμετρική αναλλοίωτος και παραμένει το ίδιο μετά από επεκτάσεις των σταθερών, οπότε* $g(E_i) = g(E') = g(E)$ *για κάθε* $i = 1, \ldots, m$.

Θα αποδείξουμε τώρα το 3. Θεωρούμε τα σύνολα $X := \{P \in \mathbb{P}_L : \deg(P) = 1\}$ *και για* $i = 1, \ldots, m$ *τα σύνολα* $X_i : \{Q \in \mathbb{P}_{E_i} : \deg(Q) = 1\}$. *Θα πρέπει να αποδείξουμε ότι*

$$\left| \bigcup_{i=1}^{m} X_i \right| = m \cdot |X|. \tag{4.38}$$

Έστω ένα $P \in X$. *Διαλέγουμε μία θέση* $P' \in \mathbb{P}_{E'}$ *που να βρίσκεται υπέρ του* P *και θέτουμε* $P_1 := P' \cap E$ *τον περιορισμό της στο* E. *Ο δείκτης αδράνειας* $f(P_1/P) \mid m$ *αφού η επέκταση* E/L *είναι Galois και όλοι οι δείκτες των θέσεων που βρίσκονται υπέρ το* P *είναι ίδιοι. Συνεπώς* $f(P_1/P) \mid n$ *και το σώμα υπολοίπων του* P' *είναι* $\mathbb{F}_{p^n}$. *Δηλάδη* $f(P'/P) = n$. *Θεωρούμε τον δείκτη διακλάδωσης* $e = e(P'/P)$ *του* P *στην επέκταση* E'/L *και έστω* r *το πλήθος των θέσεων του* $\mathbb{P}_{E'}$ *που επεκτείνουν την* P. *Έχουμε*

$$mn = [E' : L] = e(P'/P)f(P'/P)r = enr.$$

Συνεπώς $m = er$ *και η απόδειξη της (4.38) ανάγεται στης απόδειξη των παρακάτω ισχυρισμών:*

Ισχυρισμός 1 *Για κάθε* $Q \in X_i$ *με* $Q \mid P$ *υπάρχει ακριβώς μία θέση* $Q' \in \mathbb{P}_{E'}$ *που επεκτείνει τον* Q.

Ισχυρισμός 2 *Για κάθε θέση* $Q' \in \mathbb{P}_{E'}$ *με* $Q' \mid P$ *υπάρχουν ακριβώς* e *το πλήθος διαφορετικές θέσεις* $Q \in \bigcup_{i=1}^{m} X_i$ *ώστε* $Q' \mid Q$.

Θα αποδείξουμε το πρώτο ισχυρισμό. Έστω $Q' \in \mathbb{P}_{E'}$ *θέση υπέρ της θέσης* Q *του* X_i *και* $Q \mid P$. *Τότε*

$$f(Q'/Q) = f(Q'/Q)f(Q/P) = f(Q'/P) = n.$$

Στον παραπάνω τύπο χρησιμοποιήσαμε ότι $f(Q/P) = 1$ *αφού το* Q *είναι μία θέση του* X_i. *Συνεπώς* $f(Q'/Q) = [E' : E_i]$ *το οποίο δίνει ότι το* Q' *είναι η μοναδική επέκταση του* Q *στο* $E' : E_i$.

Θα αποδείξουμε τώρα τον δεύτερο ισχυρισμό. Έστω $Q' \in \mathbb{P}_{E'}$ *με* $Q' \mid P$. *Έστω* $H = \mathrm{Gal}(E'/L)$ *η ομάδα ανάλυσης του* Q' *υπέρ του* P, Z *το σταθερό σώμα του* H *και* $P_Z := Q' \cap Z$. *Τότε*

$$|H| = e(Q'/P) \cdot f(Q'/P) = en$$

και $f(P_Z/P) = 1$. *Συνεπώς έχουμε ότι το* $\mathbb{F}_q$ *είναι το πλήρες σώμα σταθερών του* Z. *Από την θεωρία Galois γνωρίζουμε ότι το σταθερό σώμα του* $H \cap G$ *είναι η*

σύνθεση των σωμάτων Z και L'. Έχουμε λοιπόν ότι $ZL' = ZL\mathbb{F}_{q^n} = Z\mathbb{F}_{q^n}$ και $[Z\mathbb{F}_{q^n} : Z] = n$, αφού δείξαμε ότι το $\mathbb{F}_q$ είναι το πλήρες σώμα σταθερών του Z. Έτσι έχουμε

$$|H \cap G| = [E' : Z]/[ZL' : Z] = ne/n = e.$$

Αφού το P_Z δεν διακλαδίζεται στο $ZL' = Z\mathbb{F}_{q^n}$ έχουμε ότι $T := ZL'$ είναι το σώμα αδρανείας και $H \cap G$ είναι η ομάδα αδρανείας του Q'/P.

Τώρα θα κάνουμε χρήση του λήμματος 4.36: ακριβώς e το πλήθος από τις κυκλικές ομάδες $U_1, \ldots, U_m \subseteq \mathrm{Gal}(E'/L)$ τάξης n με $U_i \cap G = \{1\}$ περιέχονται στην ομάδα H και ας τις ονομάσουμε $U_{i_1}, \ldots, U_{i_e}$. Θέτουμε $Q_{i_j} := Q' \cap E_{i_j}$. Αφού τα E_{i_j} περιέχουν το σώμα ανάλυσης του Q' υπέρ το P το Q' είναι η μοναδική θέση του E' υπέρ του Q_{i_j}. Από την άλλη $e(Q'/Q_{i_j}) = 1$ αφού το E' είναι μία επέκταση των σταθερών του E_{i_j}. Αυτό έχει ως αποτέλεσμα $f(Q'/Q_{i_j}) = [E' : E_{i_j}] = n = f(Q'/P)$ συνεπώς $\deg(Q_{i_j}) = 1$. Με αυτό τον τρόπο έχουμε κατασκευάσει e διαφορετικές θέσεις $Q_{i_j} \in \bigcup_{i=1}^{m} X_i$ ώστε $Q' \mid Q_{i_j}$.

Αντιστρόφως ας υποθέσουμε ότι $Q \in X_i$ για κάποιο $i \in \{1, \ldots, m\}$ και ότι $Q' \mid Q$. Τότε $f(Q'/Q) = n$. Οπότε $U_i = \mathrm{Gal}(E' : E_i)$ περιέχεται στην ομάδα ανάλυσης H του Q' υπέρ το P, δηλαδή U_i είναι μία από τις ομάδες U_{i_j} και Q είναι η θέση Q_{i_j}. Αυτό αποδεικνύει τον ισχυρισμό 2 και το ζητούμενο αποτέλεσμα. □

Επιστρέφουμε τώρα στην απόδειξη του θεωρήματος Hasse-Weil. Θα πρέπει να αποδείξουμε ένα κάτω φράγμα για το πλήθος $N_r = N(F_r)$. Μπορούμε να διαλέξουμε ένα ρητό σώμα συναρτήσεων $F_0 = \mathbb{F}_q(t)$ ώστε το F/F_0 να είναι μία διαχωρίσιμη επέκταση, καθώς και μία επέκταση $E \supset F$ ώστε η επέκταση E/F_0 να είναι Galois. Μπορεί το σώμα των σταθερών του E να είναι μία επέκταση $\mathbb{F}_{q^d}$ του σώματος $\mathbb{F}_q$. Σε αυτή την περίπτωση θεωρούμε τα σώματα $F\mathbb{F}_{q^d}$, $F_0\mathbb{F}_{q^d} = \mathbb{F}_{q^d}(t)$ αντί των σωμάτων F, F_0. Η επέκταση $E/F_0\mathbb{F}_{q^d}$ είναι Galois, οπότε αρκεί να αποδείξουμε το θεώρημα των Hasse-Weil για το σώμα $F\mathbb{F}_{q^d}/\mathbb{F}_{q^d}$. Υποθέτουμε ότι λοιπόν χωρίς περιορισμό της γενικότητας ότι το $\mathbb{F}_q$ είναι επίσης το πλήρες σώμα των σταθερών για το E. Επιπλέον υποθέρουμε ότι

$$q \text{ είναι τετράγωνο, και } q > (g(E) + 1)^4. \tag{4.39}$$

Θέτουμε $m := [E : F]$ και $n := [E : F_0]$ και θεωρούμε τις επεκτάσεις των σταθερών $E' = E\mathbb{F}_{q^n}$, $F' = F\mathbb{F}_{q^n}$ και $F_0' := F_0\mathbb{F}_{q^n}$. Από το λήμμα 4.36 υπάρχουν ακριβώς m το πλήθος διαφορετικές κυκλικές υποομάδες $V_1, \ldots, V_m \subseteq \mathrm{Gal}(E'/F)$ τάξης n ώστε $V_i \cap \mathrm{Gal}(E'/F') = \{1\}$. Από την άλλη πλευρά υπάρχουν n κυκλικές υποομάδες $U_1, \ldots, U_n \subseteq \mathrm{Gal}(E'/F_0)$ με την ιδιότητα $|U_j| = n$ και $U_j \cap \mathrm{Gal}(E'/F_0') = \{1\}$. Ισχύει ότι $V_i \cap \mathrm{Gal}(E'/F_0') = \{1\}$ αφού το E' είναι η σύνθεση του F_0' με το σταθερό σώμα της V_i. Μπορούμε να υποθέσουμε λοιπόν ότι $V_i = U_i$ για $i = 1, \ldots, m$. Θα συμβολίζουμε με E_i το σταθερό σώμα της U_i για $i = 1, \ldots, n$. Η πρόταση 4.37 μας δίνει ότι

$$m \cdot N(F) = \sum_{i=1}^{m} N(E_i), \tag{4.40}$$

$$n \cdot N(F_0) = \sum_{i=1}^{n} N(E_i). \tag{4.41}$$

Αφού έχουμε υποθέσει τις (4.39) έχουμε τα άνω φράγματα

$$N(E_i) \leq q + 1 + (2g(E) + 1)q^{1/2},$$

για όλα τα $1 \leq i \leq n$ *από την πρόταση 4.35. Οι θέσεις του* $F_0 = \mathbb{F}_q(t)$ *βαθμού ένα είναι ο πόλος του* t *και οι ρίζες των* $t - \alpha$ *για κάθε* $\alpha \in \mathbb{F}_q$*. Συνεπώς* $N(F_0) = q + 1$*. Αυτό το συνδιάζουμε με τις (4.40,4.41) και έχουμε*

$$m \cdot N(F) = n \cdot N(F_0) + \sum_{i=1}^{m} N(E_i) - \sum_{i=1}^{n} N(E_i) =$$

$$n(q+1) - \sum_{i=m+1}^{n} N(E_i) \geq$$

$$\geq n(q+1) - (n-m)(q + 1 + (2g(E) + 1)q^{1/2}) =$$

$$m(q+1) - (n-m)((2g(E) + 1)q^{1/2}).$$

Δηλαδή

$$N(F) \geq q + 1 - \frac{n-m}{m}(2g(E) + 1)q^{1/2}.$$

Παρατηρούμε ότι οι αριθμοί $m, n, g(E)$ *είναι αναλλοίωτοι υπό επεκτάσεις του σταθερών, δηλαδή καταφέραμε να πετύχουμε ένα κάτω φράγμα*

$$N_r \geq q^r + 1 - c_2 q^{r/2}.$$

Βιβλιογραφία

[HENS] Henning Stichtenoth, Algebraic Function Field and Codes, Springer-Verlag, Heidelberg Berlin, 1993.

[JOR] Joseph Rotman, Galois Theory, Springer-Verlag, New York, 1990.

[TOMA] Tom M. Apostol, Introduction to Analytic Number Theory, Springer-Verlag, New York, 1976.

[ΓΙΑΝΑΝ] Γιάννης Α. Αντωνιάδης, L-σειρές, ΕΠΕΑΕΚ "Προμηθέας", Ηράκλειο, 1999.

[ΣΩΤΝΤ] Σωτήρης Κ. Ντούγιας, Απειροστικός Λογισμός Ι, Leader Books, Αθήνα 2003.

[ΜΙΧΜΑ] Μιχάλης Μαλιάκας, Εισαγωγή στη Μεταθετική Άλγεβρα, Σοφία, Θεσσαλονίκη, 2005.