Πανεπιστημιο Κρητης
Σχολη Θετικων & Τεχνολογικων Επιστημων
Τμημα Μαθηματικων

Το Θεωρημα Των Πρωτων Αριθμων σε Σωματα Συναρτησεων

Γιωργος Ν. Καπετανακης

Μεταπτυχιακή εργασία

Επιβλέπων καθηγητής:
Θεόδουλος Γαρεφαλάκης

ΗΡΑΚΛΕΙΟ
2008

Στο δάσκαλο και μαθηματικό
Αθανάσιο Τριάντη, το αναλλοίωτο
από το χρόνο πρότυπό μου.

Πρόλογος

Το παρόν κείμενο είναι η μεταπτυχιακή μου εργασία στο πλαίσιο του μεταπτυχιακού προγράμματος *«Τα μαθηματικά και οι εφαρμογές τους»* των τμημάτων Μαθηματικών και Εφαρμοσμένων Μαθηματικών του Πανεπιστημίου Κρήτης, στην κατεύθυνση *«θεωρητικά μαθηματικά»*. Την τριμελή επιτροπή της εργασίας αποτέλεσαν οι κύριοι Θεόδουλος Γαρεφαλάκης (επιβλέπων), Μανόλης Λυδάκης και Νίκος Τζανάκης.

Περίληψη. Η κλασική θεωρία αριθμών ασχολείται με ζητήματα που αφορούν το σύνολο $\mathbb{Z}$ των ακεραίων αριθμών. Προκειμένου να λυθούν διάφορα προβλήματα της κλασικής θεωρίας αριθμών αναπτύχθηκε η αλγεβρική θεωρία αριθμών, η οποία μελετάει το σώμα κλασμάτων του $\mathbb{Z}$, δηλαδή το $\mathbb{Q}$, το σύνολο των ρητών αριθμών, και πεπερασμένες αλγεβρικές επεκτάσεις του, τα λεγόμενα *αριθμητικά σώματα*.

Εμπνεόμενοι από τις ομοιότητες του συνόλου $\mathbb{Z}$ με το σύνολο $\mathbb{F}[x]$, δηλαδή το σύνολο των πολυωνύμων μιας μεταβλητής πάνω από ένα πεπερασμένο σώμα $\mathbb{F}$, θα μιμηθούμε τις παραπάνω κατασκευές. Έτσι θα μελετήσουμε το σώμα $\mathbb{F}(x)$, το σώμα των ρητών συναρτήσεων πάνω από ένα πεπερασένο σώμα $\mathbb{F}$, και πεπερασμένες αλγεβρικές επεκτάσεις του, τα *σώματα συναρτήσεων*. Θα αποδείξουμε λοιπόν, τα αντίστοιχα θεωρήματα της κλασικής θεωρίας αριθμών, όπως το θεώρημα των πρώτων αριθμών, ή ακόμα και ανοιχτών προβλημάτων της θεωρίας αριθμών, όπως την υπόθεση Riemann.

Οι εν λόγω μαθηματικές οντότητες μπορούν να μελετηθούν με εργαλεία της αλγεβρικής γεωμετρίας ή ακόμα και της μιγαδικής ανάλυσης, όμως στο παρόν κείμενο θα προσπαθήσουμε να περιοριστούμε σε μια καθαρά αλγεβροαριθμοθεωρητική προσέγγιση. Συχνά, πολλά αποτελέσματα ισχύουν και στη γενικότερη περίπτωση, που το $\mathbb{F}$ αντικαθίσταται από κάποιο τυχαίο σώμα. Θα προσπαθήσουμε να μην περιορίσουμε την ισχύ των αποτελεσμάτων αν κάτι τέτοιο δεν είναι απαραίτητο.

Ευχαριστίες. Θα ήθελα να ευχαριστήσω όλους εκείνους που με βοήθησαν με τον τρόπο τους. Κατ᾽ αρχάς ευχαριστώ την οικογένειά μου Νίκο, Μαρία, Έρη, Μάγια και Προκόπη (σε φθίνουσα σειρά ηλικίας), καθώς και την ευρύτερη οικογένειά μου και ειδικά τον θείο μου Δημήτρη. Στη συνέχεια ένα μεγάλο ευχαριστώ σε όλους τους δασκάλους μου, ξεκινώντας από τον Αθανάσιο Τριάντη (στον οποίο αφιερώνω και την εργασία), μετά στους καθηγητές μου από το Πανεπιστήμιο Αθηνών, κυρίους Δημήτρη Βάρσο και Ευάγγελο Ράπτη και τέλος στους καθηγητές

μου από το Πανεπιστήμιο Κρήτης, τους κυρίους Αλέξη Κουβιδάκη, Γιώργο Κωστάκη, Μιχάλη Παπαδημητράκη και Νίκο Τζανάκη. Ιδιαίτερα θα ήθελα να ευχαριστήσω τον επιβλέποντα Θεόδουλο Γαρεφαλάκη για την εμπιστοσύνη που μου έδειξε, την άψογη συνεργασία, τη σωστή καθοδήγηση και τη συνεχή ενθάρρυνση. Ακόμα ένα τεράστιο ευχαριστώ σε **όλους** τους φίλους μου.

Τέλος, θα ήταν άδικο αν δεν αναφέρω ότι πολλοί από τους ελληνικούς όρους οφείλονται στον κ. Τζανάκη, ενώ το φιλολογικό έλεγχο έκανε η Πόπη Ξηρουχάκη, την οποία ευχαριστώ.

Συμβολισμοί. Σε ολόκληρη την εργασία με $\overline{K}$ θα συμβολίζουμε την αλγεβρική θήκη του σώματος K, και με $\overline{K}^F$ την αλγεβρική θήκη του K στο F, δηλαδή όλα τα στοιχεία του F που είναι αλγεβρικά πάνω από το K. Αν δεν υπάρχει κίνδυνος σύγχυσης θα συμβολίζουμε με $\mathbb{F}$ το τυχαίο πεπερασμένο σώμα, με q το πλήθος των στοιχείων του και με p την χαρακτηριστική του. Αν R δακτύλιος, με R^* θα συμβολίζουμε το σύνολο των αντιστρέψιμων στοιχείων του R. Ακόμα με $|S|$ θα συμβολίζουμε τον πληθάριθμο του συνόλου S. Τέλος, τα χρώματα της τράπουλας συμβολίζουν το τέλος μιας απόδειξης και σε κάθε ένα από τα τέσσερα κεφάλαια χρησιμοποιείται διαφορετικό χρώμα, ενώ η σειρά τους (το ♠ στο $1^ο$ κεφάλαιο, το ♣ στο $2^ο$ κ.ο.κ.) είναι μη τυχαία.

Τεχνικά. Το παρόν κείμενο είναι επεξεργασμένο από το σύστημα προετοιμασίας εγγράφων LaTeX, ενώ καθ' όλη τη συγγραφή χρησιμοποιήθηκε αποκλειστικά ελεύθερο λογισμικό ανοιχτού κώδικα.

Γιώργος Ν. Καπετανάκης
Ηράκλειο 2008

Περιεχόμενα

ΚΕΦΑΛΑΙΟ 1

Σώματα συναρτήσεων

Στο κεφάλαιο αυτό θα αναφέρουμε κυρίως ορισμούς, αλλά και κάποιες απλές βασικές ιδιότητες των σωμάτων συναρτήσεων. Θεωρούνται γνωστές κάποιες βασικές γνώσεις άλγεβρας, θεωρίας Galois, θεωρίας αριθμών, αλγεβρικής θεωρίας αριθμών και μιγαδικής ανάλυσης.

1.1. Γενικές προαπαιτούμενες αλγεβρικές γνώσεις

ΟΡΙΣΜΟΣ 1.1.1. Έστω K σώμα και F επέκτασή του. Αν υπάρχει $x \in F$, με x μη αλγεβρικό πάνω από το K, τέτοιο ώστε η επέκταση $F/K(x)$ να είναι πεπερασμένη, τότε λέμε ότι η επέκταση F/K έχει *βαθμό υπερβατικότητας 1*, και η επέκταση F/K ονομάζεται *αλγεβρικό σώμα συναρτήσεων μιας μεταβλητής* πάνω από το K ή απλά *σώμα συναρτήσεων* (algebraic function field of one variable ή function field). Τέλος, το σώμα $\overline{K}^F$ καλείται το *σώμα σταθερών* του F/K.

Ο παραπάνω ορισμός μπορεί να δείχνει δύσχρηστος, όμως το παρακάτω λήμμα διευκολύνει την κατάσταση.

ΛΗΜΜΑ 1.1.2. *Η επέκταση F/K έχει βαθμό υπερβατικότητας 1 ανν $\forall\, x \in F \setminus \overline{K}^F$ ισχύει ότι η επέκταση $F/K(x)$ είναι πεπερασμένη.*

ΑΠΟΔΕΙΞΗ. ($\Rightarrow$) Αφού η F/K έχει βαθμό υπερβατικότητας 1, τότε $\exists\, z \in F \setminus \overline{K}^F$ τέτοιο ώστε $F/K(z)$ πεπερασμένη.

Έστω τυχαίο $x \in F \setminus \overline{K}^F$. Τότε $x \in F$, άρα x αλγεβρικό πάνω από το $K(z)$, άρα υπάρχει $f_1(X, Z) \in K(Z)[X]$, με $f_1(x, z) = 0$. Έτσι υπάρχει $f_2(X, Z) \in K[Z, X]$, με $f_2(x, z) = 0$, άρα z αλγεβρικό πάνω από το $K(x)$, άρα $[K(x, z) : K(x)] < \infty$.

Ακόμα $[F : K(z)] < \infty$ και

$$[F : K(z)] = [F : K(x, z)] \cdot [K(x, z) : K(z)],$$

άρα $[F : K(x, z)] < \infty$.

Τέλος, έχουμε ότι

$$[F : K(x)] = [F : K(x, z)] \cdot [K(x, z) : K(x)]$$

και από τα παραπάνω καταλήγουμε ότι $[F : K(x)] < \infty$, δηλαδή το ζητούμενο.

($\Leftarrow$) Άμεσο. ♠

ΛΗΜΜΑ 1.1.3. *Έστω F/K σώμα συναρτήσεων. Η επέκταση $\overline{K}^F/K$ είναι πεπερασμένη.*

Απόδειξη. Έστω σώμα E, με $K \subseteq E \subseteq F$ και E αλγεβρικό πάνω από το K. Έστω τώρα $x \in F$ υπερβατικό πάνω από το K και $k_1, \ldots, k_n \in E$ γραμμικά ανεξάρτητα πάνω από το K. Τότε, προφανώς, τα $k_1, \ldots, k_n$ είναι γραμμικά ανεξάρτητα πάνω από το $K(x)$. Ακόμα, προφανώς, $E(x) \subseteq F$ κι έτσι καταλήγουμε ότι

$$[E : K] \leq [E(x) : K(x)] \leq [F : K(x)] < \infty.$$

Εφαρμόζοντας το παραπάνω για $E = \overline{K}^F$ έχουμε το ζητούμενο. ♠

Ειδικές, αλλά πολύ χρήσιμες στην περίπτωσή μας κατηγορίες σωμάτων συναρτήσεων, είναι οι παρακάτω.

Ορισμος 1.1.4. Ένα *ολικό σώμα συναρτήσεων* (global function field) είναι ένα σώμα συναρτήσεων $F/\mathbb{F}$, όπου $\mathbb{F}$ πεπερασμένο.

Ορισμος 1.1.5. Το σώμα συναρτήσεων F/K λέγεται *ρητό* αν $F = K(x)$ για κάποιο $x \in F$.

Μια συνάρτηση που θα μας χρειαστεί αργότερα είναι η διακριτή αποτίμηση, που ορίζεται ως εξής:

Ορισμος 1.1.6. Έστω F σώμα. Λέμε ότι μια συνάρτηση

$$u : F \to \mathbb{Z} \cup \{\infty\}$$

είναι *διακριτή αποτίμηση* αν ικανοποιεί τις παρακάτω ιδιότητες.

(α') $u(x) = \infty \iff x = 0$.
(β') $u(xy) = u(x) + u(y)\ \forall\, x, y \in F$.
(γ') $u(x + y) \geq \min\{u(x), u(y)\}\ \forall\, x, y \in F$.
(δ') $\exists\, z \in F\ :\ u(z) = 1$.
(ε') $u(a) = 0\ \forall\, a \in K \setminus \{0\}$.

Ακόμα η ιδιότητα (γ') ονομάζεται *τριγωνική ανισότητα*.

Από τον παραπάνω ορισμό εύκολα βλέπει κανείς ότι μια διακριτή αποτίμηση είναι επί, ενώ το παρακάτω λήμμα είναι κι αυτό άμεσο.

Λημμα 1.1.7 (Ισχυρή Τριγωνική Ανισότητα). *Έστω u διακριτή αποτίμηση του σώματος συναρτήσεων F/K και $x, y \in F$ τέτοια ώστε $u(x) \neq u(y)$. Τότε $u(x + y) = \min\{(u(x), u(y)\}$.*

Απόδειξη. Από τον ορισμό 1.1.6 έχουμε ότι $u(ax) = u(x)$ για $a \in K \setminus \{0\}$, άρα $u(y) = u(-y)$. Ακόμα υποθέτουμε χωρίς βλάβη της γενικότητας ότι $u(x) < u(y)$. Τότε αν $u(x+y) > u(x)$ από τον 1.1.6 έχουμε ότι

$$u(x) = u((x + y) - y) \geq \min\{u(x + y), u(y)\} > u(x),$$

άτοπο. ♠

1.2. Πρώτοι

Σκοπός μας σε αυτήν την παράγραφο, είναι να ορίσουμε τα πρώτα στοιχεία για την θεωρία μας και να μελετήσουμε κάποιες βασικές ιδιότητές τους.

ΟΡΙΣΜΟΣ 1.2.1. Ένας *δακτύλιος αποτίμησης* (valuation ring) του σώματος συναρτήσεων F/K είναι ένας δακτύλιος $\mathcal{O}$, για τον οποίο $K \subsetneqq \mathcal{O} \subsetneqq F$ και αν $z \in F$, τότε $z \in \mathcal{O}$ ή $z^{-1} \in \mathcal{O}$.

Ας δούμε ένα λήμμα που συμπληρώνει τον παραπάνω ορισμό.

ΛΗΜΜΑ 1.2.2. *Αν $\mathcal{O}$ είναι δακτύλιος αποτίμησης του F/K, τότε ισχύει ότι $\overline{K}^F \subseteq \mathcal{O}$.*

ΑΠΟΔΕΙΞΗ. Έστω $x \in \overline{K}^F$. Αν $x = 0$ τότε προφανώς $x \in \mathcal{O}$, έτσι μας μένει να δείξουμε ότι $x \in \mathcal{O}$ για $x \neq 0$.

Πράγματι, αν $x \neq 0$ και $x^{-1} \notin \mathcal{O}$, τότε επειδή $x \in F$ από τον ορισμό 1.2.1 θα πάρουμε ότι $x \in \mathcal{O}$, οπότε μας μένει να δείξουμε ότι $x \in \mathcal{O}$ στην περίπτωση που $x \neq 0$ και $x^{-1} \in \mathcal{O}$.

Όμως παρατηρούμε ότι αν $x \neq 0$ και $x^{-1} \in \mathcal{O}$, τότε μιας που το x είναι αλγεβρικό πάνω από το K, θα υπάρχουν $n \geq 1$ και $a_0, \ldots, a_{n-1} \in K$ τέτοια ώστε

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0.$$

Η τελευταία σχέση, αν πολλαπλασιάσουμε με x^{-n+1}, μας δίνει ότι

$$x = -a_{n-1} - a_{n-2}x^{-1} - \cdots - a_0 x^{-n+1},$$

απ᾽ όπου εύκολα παρατηρούμε ότι όλα τα μέλη του δεξιού μέλους της ισότητας ανήκουν στο $\mathcal{O}$, επομένως $x \in \mathcal{O}$. ♠

ΠΟΡΙΣΜΑ 1.2.3. *Αν $\mathcal{O}$ είναι δακτύλιος αποτίμησης του F/K, τότε ισχύει ότι $\overline{K}^F \setminus \{0\} \subseteq \mathcal{O}^*$.*

ΑΠΟΔΕΙΞΗ. Άμεσο από το λήμμα 1.2.2. ♠

Η παρακάτω πρόταση μας δείχνει κάποιες χρήσιμες αλγεβρικές ιδιότητες των δακτυλίων αποτίμησης των σωμάτων συναρτήσεων.

ΠΡΟΤΑΣΗ 1.2.4. *Αν ο $\mathcal{O}$ είναι δακτύλιος αποτίμησης του σωμάτος συναρτήσεων F/K, τότε ο $\mathcal{O}$ είναι τοπικός δακτύλιος*[1].

ΑΠΟΔΕΙΞΗ. Αρκεί να δείξουμε ότι το $P := \mathcal{O} \setminus \mathcal{O}^*$ είναι ιδεώδες του $\mathcal{O}$. Έτσι έστω $x \in P$ και $z \in \mathcal{O}$, τότε αν $xz \in \mathcal{O}^*$ θα είχαμε ότι $x \notin P$, άτοπο, άρα $xz \in P$. Έστω τώρα $x, y \in P$. Χωρίς βλάβη της γενικότητας υποθέτουμε ότι $x/y \in \mathcal{O}$. Τότε $1 + x/y \in \mathcal{O}$ και από το προηγούμενο $y(1 + x/y) = x + y \in \mathcal{O}$. ♠

[1] Δηλαδή έχει μοναδικό μεγιστικό ιδεώδες.

Έτσι σύμφωνα με την τελευταία πρόταση μπορούμε να μιλάμε για το μεγιστικό ιδεώδες P ενός δακτυλίου αποτίμησης $\mathcal{O}$. Αυτό θα μας βοηθήσει να ορίσουμε και τους «πρώτους» μας, πριν όμως από τον ορισμό, ας δούμε ένα χρήσιμο λήμμα.

ΛΗΜΜΑ 1.2.5. *Αν $\mathcal{O}$ είναι δακτύλιος αποτίμησης του F/K και P το μεγιστικό ιδεώδες του, τότε ισχύει ότι $P \cap \overline{K}^F = \{0\}$.*

ΑΠΟΔΕΙΞΗ. Αν $x \in \overline{K}^F \setminus \{0\}$, τότε από το πόρισμα 1.2.3 έχουμε ότι $x \in \mathcal{O}^*$, άρα $x \notin \mathcal{O} \setminus \mathcal{O}^* = P$. Από το τελευταίο και το προφανές γεγονός ότι $0 \in P \cap \overline{K}^F$ παίρνουμε το ζητούμενο. ♠

Το θεώρημα που ακολουθεί είναι ιδιαίτερα χρήσιμο.

ΘΕΩΡΗΜΑ 1.2.6. *Έστω $\mathcal{O}$ ένας δακτύλιος αποτίμησης του σωμάτος συναρτήσεων F/K και P το μεγιστικό ιδεώδες του. Τότε*

(α΄) το P είναι κύριο ιδεώδες και
(β΄) αν $P = t\mathcal{O}$, τότε κάθε $z \in F \setminus \{0\}$ έχει μοναδική αναπαράσταση της μορφής $z = t^n u$, με $n \in \mathbb{Z}$ και $u \in \mathcal{O}^*$.

ΑΠΟΔΕΙΞΗ. **α΄)** Έστω P όχι κύριο και $x_1 \in P \setminus \{0\}$. Τότε $P \neq x_1\mathcal{O}$ και άρα $\exists\, x_2 \in P \setminus x_1\mathcal{O}$. Τότε $x_2 x_1^{-1} \notin \mathcal{O}$, άρα υποχρεωτικά $x_2^{-1}x_1 \in P$, δηλαδή $x_1 \in x_2 P$. Συνεχίζοντας επαγωγικά μπορούμε να κατασκευάσουμε μια άπειρη ακολουθία $(x_i)_{i\in\mathbb{N}} \in P$, τέτοια ώστε $x_i \in x_{i+1}P$ και $x_{i+1} \neq x_i$ για κάθε $i \geq 1$. Θα δείξουμε ότι κάτι τέτοιο είναι αδύνατο.

Αρκεί λοιπόν να αποδείξουμε ότι για την τυχαία πεπερασμένη ακολουθία $x_1, \ldots, x_n \in P$, με $x_1 = x \in P \setminus \{0\}$, $x_i \in x_{i+1}P$ και $x_i \neq x_{i+1}$ για κάθε $1 \leq i \leq n-1$, έχουμε ότι $n \leq [F : K(x)] < \infty$.

Από τα λήμματα 1.1.2 και 1.2.5 καταλήγουμε στο ότι $[F : K(x)] < \infty$. Για την αριστερή ανισότητα αρκεί να δείξουμε ότι τα $x_1, \ldots, x_n$ είναι γραμμικά ανεξάρτητα πάνω από το $K(x)$.

Έστω λοιπόν

$$\sum_{i=1}^{n} \phi_i x_i = 0 \tag{1.1}$$

με $\phi_i \in K(x)$ ένας μη τετριμμένος γραμμικός συνδυασμός. Εύκολα βλέπουμε ότι μπορούμε να υποθέσουμε ότι $\phi_i \in K[x]$ και ότι αν $a_i := \phi_i(0)$ υπάρχει $j \in \{1, \ldots, n\}$ τέτοιο ώστε $a_j \neq 0$ και $a_i = 0\ \forall\, i > j$. Έτσι η (1.1) γίνεται

$$-\phi_j x_j = \sum_{i \neq j} \phi_i x_i \tag{1.2}$$

με $x_i \in x_j P$ για $i < j$ και $\phi_i = x g_i$ για $i > j$ ($g_i \in K[x]$). Έτσι η (1.2) δίνει

$$-\phi_j = \sum_{i<j} \phi_i \cdot \frac{x_i}{x_j} + \sum_{i>j} \frac{x}{x_j} \cdot g_i x_i. \tag{1.3}$$

Σύμφωνα με τα παραπάνω, όλοι οι όροι του δεξιού μέλους της (1.3) ανήκουν στο P, άρα $\phi_j \in P$. Όμως, $\phi_j = a_j + xg_j$ με $g_j \in \mathcal{O}$ και $x \in P$, δηλαδή $xg_j \in P$, άρα $a_j \in P \cap K \setminus \{0\}$, άτοπο. Άρα τα $x_1, \ldots, x_n$ είναι γραμμικά ανεξάρτητα πάνω από το $K(x)$.

β′) Η μοναδικότητα της αναπαράστασης είναι τετριμμένη, άρα αρκεί να δείξουμε την ύπαρξή της. Δίχως βλάβη της γενικότητας υποθέτουμε ότι $z \in \mathcal{O}$, αλλιώς $z^{-1} \in \mathcal{O}$ και εργαζόμαστε με αρνητικούς. Αν $z \in \mathcal{O}^*$, τότε $z = t^0 z$.Αν $z \in P$, τότε $z = tz_1$, με $z_1 \in \mathcal{O}$. Αν $z_1 \in \mathcal{O}^*$ τελειώσαμε. Διαφορετικά, $z_1 \notin \mathcal{O}^*$ άρα $z_1 \in P$, οπότε $z_1 = tz_2$, με $z_2 \in \mathcal{O}$ και $z = t^2 z_2$. Αν $z_2 \in \mathcal{O}^*$, τελειώσαμε· διαφορετικά, $z_2 \in P$, $z_2 = tz_3$, όπου $z_3 \in \mathcal{O}$, και $z = t^3 z_3$. Αυτή η διαδικασία σταματά, δηλαδή σε κάποιο βήμα n είναι $z_n \in \mathcal{O}^*$, διότι διαφορετικά θα είχαμε μια άπειρη ακολουθία $z, z_1, z_2, \ldots$ με $z \in z_1 P$, $z_1 \in z_2 P, \ldots, z_i \in z_{i+1} P$ και, όπως στο (α′), αυτό αποκλείεται. Έτσι έχουμε ότι $z = t^n z_n$, με $z_n \in \mathcal{O}^*$. ♠

Ορισμος 1.2.7. Ένας *πρώτος* (prime ή place) P του σώματος συναρτήσεων F/K είναι το μεγιστικό ιδεώδες κάποιου δακτύλιου αποτίμησης. Ακόμα, με $\mathbb{P}_F$ (ή απλά $\mathbb{P}$ αν δεν υπάρχει κίνδυνος σύγχυσης) συμβολίζουμε το σύνολο των πρώτων του σώματος συναρτήσεων F/K.

Μια διαισθητική παρατήρηση στον παραπάνω ορισμό είναι ότι οι δακτύλιοι αποτίμησης και οι πρώτοι βρίσκονται σε 1-1 αντιστοιχία. Από το λήμμα που ακολουθεί θα δούμε ότι κάτι τέτοιο είναι σωστό.

Λημμα 1.2.8. *Έστω P πρώτος και $\mathcal{O}$ ο αντίστοιχος δακτύλιος αποτίμησης*[2]*. Ισχύει ότι*

$$\{z \in F^* \mid z^{-1} \notin P\} \cup \{0\} = \mathcal{O}.$$

Αποδειξη. Έστω $y \in \mathcal{O} \setminus \{0\}$. Αν $y \in \mathcal{O}^*$, τότε $y^{-1} \in \mathcal{O}^*$, άρα $y^{-1} \notin P$, δηλαδή $y \in \{z \in F^* \mid z^{-1} \notin P\}$. Αν $y \notin \mathcal{O}^*$, τότε $y \in \mathcal{O} \setminus \mathcal{O}^* = P$, επομένως $y^{-1} \notin P$, έτσι $y \in \{z \in F^* \mid z^{-1} \notin P\}$. Συνολικά $\mathcal{O} \subseteq \{z \in F^* \mid z^{-1} \notin P\} \cup \{0\}$.

Έστω τώρα $y \in \{z \in F^* \mid z^{-1} \notin P\}$. Αν $y \notin \mathcal{O}$, τότε επειδή ο $\mathcal{O}$ είναι δακτύλιος αποτίμησης έχουμε ότι $y^{-1} \in \mathcal{O}$. Όμως $y^{-1} \notin P$, άρα $y^{-1} \in \mathcal{O}^*$, δηλαδή $y \in \mathcal{O}$, άτοπο. ♠

Έτσι, από τα παραπάνω, έχει νόημα ο όρος *δακτύλιος αποτίμησης του πρώτου P* και ο συμβολισμός

$$\mathcal{O}_P := \{z \in F^* \mid z^{-1} \notin P\} \cup \{0\}.$$

Ακόμα, σύμφωνα με το (β′) του 1.2.6 ο παρακάτω ορισμός έχει νόημα.

Ορισμος 1.2.9. Έστω $P \in \mathbb{P}_F$. Ορίζουμε ως *τάξη* στον P τη συνάρτηση $\mathrm{ord}_P : F \to \mathbb{Z} \cup \{\infty\}$, όπου αν $P = t\mathcal{O}$ και $z \in F \setminus \{0\}$, τότε $\mathrm{ord}_P(z) := n$ (όπου n εκείνος του 1.2.6(β′)), και $\mathrm{ord}_P(0) := \infty$.

Μια πολύ σημαντική ιδιότητα της τάξης δίνεται από το παρακάτω θεώρημα.

[2]Δηλαδή αυτός για τον οποίο $P = \mathcal{O} \setminus \mathcal{O}^*$.

ΘΕΩΡΗΜΑ 1.2.10. *Έστω F/K σώμα συναρτήσεων.*

(α΄) Για κάθε $P \in \mathbb{P}$ η συνάρτηση ord_P είναι διακριτή εκτίμηση του F/K.
(β΄) Ισχύει ότι

$$\begin{aligned} \mathcal{O}_P &= \{z \in F \mid \mathrm{ord}_P(z) \geq 0\}, \\ \mathcal{O}_P^* &= \{z \in F \mid \mathrm{ord}_P(z) = 0\}, \\ P &= \{z \in F \mid \mathrm{ord}_P(z) > 0\} \text{ και} \end{aligned}$$

$P = x\mathcal{O}_P$ αννν $\mathrm{ord}_P(x) = 1$.
(γ΄) Κάθε δακτύλιος αποτίμησης του F/K είναι μεγιστικός ως προς τον εγκλεισμό υποδακτυλίων του F.

ΑΠΟΔΕΙΞΗ. **α΄)** Το μόνο μη προφανές είναι η ισχύς της τριγωνικής ανισότητας αν $x, y \neq 0$. Έστω λοιπόν $x, y \in F \setminus \{0\}$. Τότε αν $\mathrm{ord}_P(x) = n$ και $\mathrm{ord}_P(y) = m$, με $n \leq m$, έχουμε ότι αν $P = t\mathcal{O}_P$, τότε $x = t^n u_1$ και $y = t^m u_2$, με $u_1, u_2 \in \mathcal{O}_P^*$. Έτσι

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

με $z \in \mathcal{O}_P$. Αν $z = 0$, τότε $\mathrm{ord}_P(x+y) = \infty > \min\{\mathrm{ord}_P(x), \mathrm{ord}_P(y)\}$. Αν $z \neq 0$, τότε $z = t^k u$, με $k \geq 0$ και $u \in \mathcal{O}_P^*$, έτσι $x + y = t^{n+k}u$, οπότε

$$\mathrm{ord}_P(x+y) = n + k \geq n = \min\{\mathrm{ord}_P(x), \mathrm{ord}_P(y)\}.$$

β΄) Θεωρούμε ότι $P = t\mathcal{O}_P$. Το ότι $\mathcal{O}_P^* = \{z \in F \mid \mathrm{ord}_P(z) = 0\}$ είναι προφανές από το θεώρημα 1.2.6 και τον ορισμό 1.2.9.

Έστω $y \in \{z \in F \mid \mathrm{ord}_P(z) > 0\}$, τότε $y = t \cdot (t^{\mathrm{ord}_P(y)-1}u)$, με $u \in \mathcal{O}^*$. Όμως $t \in \mathcal{O}$, $\mathrm{ord}_P(y) - 1 \geq 0$ και $u \in \mathcal{O}$, οπότε $t^{\mathrm{ord}_P(y)-1}u \in \mathcal{O}$, επομένως $y \in t\mathcal{O} = P$. Έτσι παίρνουμε ότι $\{z \in F \mid \mathrm{ord}_P(z) > 0\} \subseteq P$. Έστω $y \in P$. Αν $\mathrm{ord}_P(y) = 0$, τότε από τα παραπάνω $y \in \mathcal{O}_P^*$, άτοπο. Αν $\mathrm{ord}_P(y) < 0$, τότε $\mathrm{ord}_P(y^{-1}) > 0$ και σύμφωνα με τα παραπάνω $y^{-1} \in P$, άτοπο. Έτσι $\mathrm{ord}_P(y) > 0$ και άρα $P \subseteq \{z \in F \mid \mathrm{ord}_P(z) > 0\}$, δηλαδή συνολικά $\{z \in F \mid \mathrm{ord}_P(z) > 0\} = P$.

Το ότι $\mathcal{O}_P = \{z \in F \mid \mathrm{ord}_P(z) \geq 0\}$ είναι άμεσο από τα προγούμενα και το ότι $\mathcal{O}_P = P \cup \mathcal{O}_P^*$, ενώ το ότι $P = x\mathcal{O}_P$ ανν $\mathrm{ord}_P(x) = 1$ είναι άμεσο.

γ΄) Έστω $\mathcal{O}$ δακτύλιος αποτίμησης του σώματος συναρτήσεων F/K, P το μεγιστικό ιδεώδες του και $z \in F \setminus \mathcal{O}$. Αρκεί να δείξουμε ότι $F = \mathcal{O}[z]$. Πράγματι, αν $y \in F$ τότε (μιας που $\mathrm{ord}_P(z^{-1}) > 0$, αφού $z \notin \mathcal{O}$) για $k \geq 0$ αρκετά μεγάλο θα έχουμε ότι $\mathrm{ord}_P(yz^{-k}) \geq 0$, άρα αν $w := yz^{-k}$, τότε $w \in \mathcal{O}$ και $y = wz^k \in \mathcal{O}[z]$. ♠

Εφόσον το P είναι μεγιστικό ιδεώδες του $\mathcal{O}_P$, το ${}^{\mathcal{O}_P}/_P$ είναι σώμα και εύκολα βλέπει κανείς ότι $P \cap K = \{0\}$. Έτσι λαμβάνοντας υπ᾽ όψιν

το ότι εξ ορισμού $K \subseteq \mathcal{O}_P$ έχουμε ότι το K είναι υπόσωμα[3] του $\mathcal{O}_P/P$, άρα έχει νόημα ο παρακάτω ορισμός.

ΟΡΙΣΜΟΣ 1.2.11. Έστω P πρώτος του σώματος συναρτήσεων F/K, τότε ο αριθμός

$$\deg P := \left[\mathcal{O}_P/P : K\right]$$

ονομάζεται *βαθμός* του P.

Το παρακάτω θεώρημα μας δείχνει όχι μόνο ότι ο βαθμός ενός πρώτου είναι πεπερασμένος, αλλά μας δίνει και ένα άνω φράγμα.

ΘΕΩΡΗΜΑ 1.2.12. *Έστω P πρώτος του σώματος συναρτήσεων F/K και $x \in P \setminus \{0\}$, τότε*

$$\deg P \leq [F : K(x)] < \infty.$$

ΑΠΟΔΕΙΞΗ. Κατ' αρχάς, προφανώς το x είναι υπερβατικό πάνω από το K, έτσι, από το λήμμα 1.1.2, αρκεί να δείξουμε την αριστερή ανισότητα. Έστω λοιπόν $z_1, \ldots, z_n \in \mathcal{O}_P$ τέτοια ώστε τα $\bar{z_1}, \ldots, \bar{z_n} \in \mathcal{O}_P/P$, με $\bar{z_i} := z_i + P$, να είναι γραμμικά ανεξάρτητα πάνω από το K. Θα δείξουμε ότι τα $z_1, \ldots, z_n$ είναι γραμμικά ανεξάρτητα πάνω από το $K(x)$. Αν όχι, υπάρχουν $\phi_i \in K(x)$ τέτοια ώστε

$$\sum_{i=1}^{n} \phi_i z_i = 0. \tag{1.4}$$

Ομοίως, με την απόδειξη του θεωρήματος 1.2.6 υποθέτουμε ότι $\phi_i \in K[x]$ και ότι αν $\phi_i = a_i + x g_i$ ($a_i \in K$, $g_i \in K[x]$), τότε δεν είναι όλα τα $a_i = 0$. Όμως $x \in P$ και $a_i \in K$, άρα $\bar{\phi_i} = \bar{a_i} = a_i$ και έτσι η (1.4) περνώντας στον πηλικοδακτύλιο δίνει

$$\sum_{i=1}^{n} a_i \bar{z_i} = 0,$$

δηλαδή έναν μη τετριμμένο μηδενικό γραμμικό συνδυασμό των $\bar{z_1}, \ldots, \bar{z_n}$, άτοπο. ♠

Οι παρακάτω ορισμοί θα μας δώσουν έννοιες που θα μας φανούν πολύ χρήσιμες σε τεχνικό επίπεδο.

ΟΡΙΣΜΟΣ 1.2.13. Έστω F/K σώμα συναρτήσεων, $z \in F$, $P \in \mathbb{P}_F$ και $\mathrm{ord}_P(z) = m$. Αν $m > 0$, τότε λέμε ότι ο P είναι *ρίζα* του z τάξης m και αν $m < 0$, τότε λέμε ότι ο P είναι *πόλος* του z τάξης $-m$.

Ας δούμε τώρα μια σημαντική ιδιότητα των πόλων και των ριζών· το επόμενο θεώρημα θα μας οδηγήσει στο ζητούμενο αποτέλεσμα.

---

[3] Στην πραγματικότητα το K δεν είναι υπόσωμα του $\mathcal{O}_P/P$, αλλά η εικόνα του K στο $\mathcal{O}_P/P$, μέσω της εμφύτευσης

$$\phi : \begin{array}{ccc} K & \hookrightarrow & \mathcal{O}_P/P \\ x & \mapsto & x + P \end{array},$$

που είναι ισόμορφη με το K.

ΘΕΩΡΗΜΑ 1.2.14. *Έστω F/K σώμα συναρτήσεων και R δακτύλιος τέτοιος ώστε $K \subseteq R \subseteq F$. Αν I είναι μη τετριμμένο ιδεώδες του R τότε υπάρχει κάποιος $P \in \mathbb{P}_F$ τέτοιος ώστε $I \subseteq P$ και $R \subseteq \mathcal{O}_P$.*

ΑΠΟΔΕΙΞΗ. Θεωρούμε το σύνολο

$$\mathcal{F} := \{S \mid S \text{ υποδακτύλιος του } F \text{ με } R \subseteq S \text{ και } IS \neq S\}.$$

Προφανώς $R \in \mathcal{F}$, άρα $\mathcal{F} \neq \emptyset$. Ακόμα, το $\mathcal{F}$ είναι εφοδιασμένο με την προφανή μερική διάταξη του εγκλεισμού, ενώ αν $\mathcal{H} \subseteq \mathcal{F}$ ένα υποσύνολο του $\mathcal{F}$ με ολική διάταξη, τότε το $T := \bigcup\{S \mid S \in \mathcal{H}\}$ είναι υποδακτύλιος του F, με $R \subseteq T$. Θα δείξουμε ότι $IT \neq T$.

Έστω λοιπόν ότι $IT = T$, τότε $1 = \sum_{i=1}^{n} a_i s_i$ με $a_i \in I$, $s_i \in T$. Εφόσον όμως το $\mathcal{H}$ έχει ολική διάταξη θα υπάρχει $S_0 \in \mathcal{H}$ τέτοιο ώστε $s_1, \ldots, s_n \in S_0$, άρα $1 = \sum_{i=1}^{n} a_i s_i \in IS_0$, άτοπο. Άρα από το λήμμα του Zorn (δες [ΣΗΑ, σελ. 40]) το $\mathcal{F}$ περιέχει κάποιο μεγιστικό στοιχείο, έστω $\mathcal{O}$. Θα δείξουμε ότι το $\mathcal{O}$ είναι δακτύλιος αποτίμησης.

Εφόσον $I \neq \{0\}$ και $I\mathcal{O} \neq \mathcal{O}$, έχουμε ότι $\mathcal{O} \subsetneq F$ και $I \subseteq \mathcal{O} \setminus \mathcal{O}^*$. Υποθέτουμε ότι υπάρχει $z \in F$ με $z, z^{-1} \notin \mathcal{O}$ (δηλαδή ότι το $\mathcal{O}$ δεν είναι δακτύλιος αποτίμησης). Τότε $I\mathcal{O}[z] = \mathcal{O}[z]$ και $I\mathcal{O}[z^{-1}] = \mathcal{O}[z^{-1}]$ (αλλιώς το $\mathcal{O}$ δεν θα ήταν μεγιστικό στοιχείο του $\mathcal{F}$), και άρα μπορούμε να βρούμε $a_0, \ldots, a_n, b_0, \ldots, b_m \in I\mathcal{O}$ τέτοια ώστε

$$1 = a_0 + a_1 z + \cdots + a_n z^n \text{ και} \tag{1.5}$$

$$1 = b_0 + b_1 z^{-1} + \cdots + b_m z^{-m}, \tag{1.6}$$

ενώ προφανώς $m, n \geq 1$. Υποθέτουμε ότι m, n τέτοια ώστε $m \leq n$ και είναι τα ελάχιστα δυνατά. Πολλαπλασιάζουμε την (1.5) με $1 - b_0$ και την (1.6) με $a_n z_n$ και παίρνουμε

$$1 - b_0 = (1 - b_0)a_0 + (1 - b_0)a_1 z + \cdots + (1 - b_0)a_n z^n \text{ και}$$
$$0 = (b_0 - 1)a_n z^n + b_1 a_n z^{n-1} + \cdots + b_m a_n z^{n-m}.$$

Προσθέτωντας τις παραπάνω εξισώσεις παίρνουμε την

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

με $c_i \in I\mathcal{O}$. Όμως αυτό είναι άτοπο, λόγω της ελαχιστότητας του n. ♠

Το παραπάνω θεώρημα δείχνει πολύ αφηρημένο, όμως το παρακάτω (σχεδόν) άμεσο πόρισμα είναι ιδιαίτερα χρήσιμο.

ΠΟΡΙΣΜΑ 1.2.15. *Έστω F/K σώμα συναρτήσεων και $z \in F$ υπερβατικό πάνω από το K. Τότε το z έχει τουλάχιστον ένα πόλο και μια ρίζα.*

ΑΠΟΔΕΙΞΗ. Θεωρούμε τον δακτύλιο $R = K[z]$ και το ιδεώδες $I = zK[z]$. Από το θεώρημα 1.2.14 υπάρχει $P \in \mathbb{P}_F$ με $z \in P$, δηλαδή ο P είναι ρίζα του z και ομοίως υπάρχει $Q \in \mathbb{P}_F$ ρίζα του z^{-1}, δηλαδή πόλος του z. ♠

Το τελευταίο πόρισμα μας δείχνει (μεταξύ άλλων) ότι $\mathbb{P}_F \neq \emptyset$. Στην πραγματικότητα ισχύει κάτι πολύ ισχυρότερο, ότι δηλαδή $|\mathbb{P}_F| = \infty$ (δες [Sti, §I.3]). Όμως και πάλι μέχρι στιγμής δεν είδαμε κάποιο στοιχείο του $\mathbb{P}_F$ και για ποιό λόγο τα στοιχεία αυτά παρομοιάζονται με τους πρώτους αριθμούς.

Για να κάνουμε κάτι τέτοιο θα πάμε στην περίπτωση του σώματος συναρτήσεων $K(x)/K$, δηλαδή του ρητού σώματος συναρτήσεων. Για κάθε ανάγωγο $p(x) \in K[x]$ ορίζουμε ως

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

και βλέπουμε εύκολα ότι αυτό είναι δακτύλιος αποτίμησης του $K(x)/K$, με αντίστοιχο μεγιστικό ιδεώδες το

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

Ένας άλλος δακτύλιος αποτίμησης του $K(x)/K$ είναι ο

$$\mathcal{O}_\infty := \left\{ \frac{f(x)}{g(x)} \,\middle|\, f(x), g(x) \in K[x],\, \deg f(x) \leq \deg g(x) \right\}$$

με μεγιστικό ιδεώδες το

$$P_\infty = \left\{ \frac{f(x)}{g(x)} \,\middle|\, f(x), g(x) \in K[x],\, \deg f(x) < \deg g(x) \right\},$$

που καλείται και *πρώτος του απείρου* ή *Αρχιμήδειος πρώτος*. Το παρακάτω θεώρημα μας δείχνει ότι στο ρητό σώμα συναρτήσεων υπάρχουν μόνο οι παραπάνω πρώτοι.

Θεωρημα 1.2.16. *Στο ρητό σώμα συναρτήσεων $K(x)/K$ αν $P \in \mathbb{P}_{K(x)}$, τότε $P = P_\infty$ ή $P = P_{p(x)}$ για κάποιο $p(x) \in K[x]$ ανάγωγο.*

Απόδειξη. Έστω $P \in \mathbb{P}_{K(x)}$ με $P \neq P_\infty$. Διακρίνουμε περιπτώσεις. Αν $x \in \mathcal{O}_P$, τότε $K[x] \subseteq \mathcal{O}_P$ και θέτουμε $I := K[x] \cap P$, το οποίο εύκολα βλέπουμε ότι είναι πρώτο ιδεώδες του $K[x]$. Όμως $K[x]$ είναι περιοχή κυρίων ιδεωδών (γιατί το K είναι σώμα) και το I είναι πρώτο ιδεώδες, άρα υπάρχει $p(x) \in K[x]$ ανάγωγο, τέτοιο ώστε $I = p(x)K[x]$. Έτσι, αν το $g(x) \in K[x]$ δεν διαιρείται από το $p(x)$, τότε $g(x) \notin I$, άρα $g(x) \notin P$, άρα $1/g(x) \in \mathcal{O}_P$. Συνοψίζοντας, έχουμε ότι

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

Όμως, από το θεώρημα 1.2.10(γ′) ισχύει ότι $\mathcal{O}_P = \mathcal{O}_{p(x)}$.

Αν τώρα $x \notin \mathcal{O}_P$, τότε όπως πριν $K[x^{-1}] \subseteq \mathcal{O}_P$, $x^{-1} \in P \cap K[x^{-1}]$ και $P \cap K[x^{-1}] = x^{-1}K[x^{-1}]$, άρα

$$\begin{aligned}
\mathcal{O}_P &\supseteq \left\{ \frac{f(x^{-1})}{g(x^{-1})} \;\middle|\; f(x^{-1}), g(x^{-1}) \in K[x^{-1}],\, x^{-1} \nmid g(x^{-1}) \right\} \\
&= \left\{ \frac{a_0 + a_1 x^{-1} + \cdots + a_n x^{-n}}{b_0 + b_1 x^{-1} + \cdots + b_m x^{-m}} \;\middle|\; b_0 \neq 0 \right\} \\
&= \left\{ \frac{a_0 x^{m+n} + \cdots + a_n x^m}{b_0 x^{m+n} + \cdots + b_m x^n} \;\middle|\; b_0 \neq 0 \right\} \\
&= \left\{ \frac{u(x)}{v(x)} \;\middle|\; u(x), v(x) \in K[x],\, \deg u(x) \leq \deg v(x) \right\} \\
&= \mathcal{O}_\infty.
\end{aligned}$$

Έτσι, και πάλι, $\mathcal{O}_P = \mathcal{O}_\infty$. ♠

1.3. Διαιρέτες και $\mathcal{L}$ χώροι

Η έννοια του διαιρέτη έχει τις ρίζες του στην αλγεβρική γεωμετρία και όχι στην κλασική θεωρία αριθμών. Παρ' όλα αυτά είναι αναπόσπαστο κομμάτι της θεωρίας μας, μιας που χάρη σε αυτήν θα αποδείξουμε το θεώρημα Riemann-Roch στο κεφάλαιο 2, που είναι ένα καταλυτικής σημασίας αποτέλεσμα, όπως θα δούμε αργότερα.

Ορισμος 1.3.1. Η ελεύθερη αβελιανή ομάδα που παράγεται από τους πρώτους ενός σώματος συναρτήσεων, ονομάζεται *ομάδα διαιρετών* (group of divisors) και συμβολίζεται ως $\mathcal{D}_F$. Τα στοιχεία της ομάδας διαιρετών, ονομάζονται *διαιρέτες* (divisors).

Έτσι, ο τυχαίος διαιρέτης είναι ένα τυπικό άθροισμα της μορφής

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

με $a_P \in \mathbb{Z}$ και $a_P = 0$ για σχεδόν όλους τους P. Τα a_P του παραπάνω τύπου συμβολίζονται ως $\mathrm{ord}_P(D)$ και ονομάζονται *τάξη* του διαιρέτη. Ένας ειδικός διαιρέτης είναι ο

$$0 := \sum_{P \in \mathbb{P}_F} 0 \cdot P,$$

ενώ αν $D = P \in \mathbb{P}_F$, τότε λέμε ότι ο D είναι *πρώτος διαιρέτης*.

Ήδη βλέπουμε ότι στο $\mathcal{D}_F$ μπορεί να οριστεί μερική διάταξη ($D_1 \leq D_2 \iff \mathrm{ord}_P(D_1) \leq \mathrm{ord}_P(D_2)\ \forall\, P \in \mathbb{P}_F$). Μάλιστα, αν $D > 0$, τότε λέμε ότι ο D είναι *αποτελεσματικός* (effective). Κάποιοι ακόμα χρήσιμοι ορισμοί είναι οι παρακάτω.

Ορισμος 1.3.2. Έστω D διαιρέτης. Ως *στήριγμα* (support) του D ορίζουμε το σύνολο

$$\mathrm{supp}(D) := \{P \in \mathbb{P}_F \mid \mathrm{ord}_P(D) \neq 0\}.$$

ΟΡΙΣΜΟΣ 1.3.3. Ως *βαθμό* του διαιρέτη D ορίζουμε τον αριθμό

$$\deg_F D := \sum_{P\in\mathbb{P}_F} \operatorname{ord}_P(D)\cdot \deg P.$$

Αν δεν υπάρχει κίνδυνος σύγχυσης, συμβολίζουμε τον $\deg_F D$ απλά ως $\deg D$. Ακόμα, εύκολα βλέπει κανείς ότι από τον βαθμό των διαιρετών προκύπτει ένας ομομορφισμός $(\deg : \mathcal{D}_F \to \mathbb{Z})$.

Επίσης, εύκολα αποδεικνύεται (δες [STI, §I.3]) ότι ένα $x \in F\setminus\{0\}$ έχει μόνο πεπερασμένες το πλήθος ρίζες και πόλους, άρα ο παρακάτω ορισμός έχει νόημα.

ΟΡΙΣΜΟΣ 1.3.4. Έστω $x \in F\setminus\{0\}$. Ορίζουμε ως

$$(x)_0 := \sum_{\substack{P\in\mathbb{P}_F\\ \operatorname{ord}_P(x)>0}} \operatorname{ord}_P(x)P, \text{ τον } \textit{διαιρέτη των ριζών} \text{ του } x,$$

$$(x)_\infty := \sum_{\substack{P\in\mathbb{P}_F\\ \operatorname{ord}_P(x)<0}} (-\operatorname{ord}_P(x))P, \text{ τον } \textit{διαιρέτη των πόλων} \text{ του } x \text{ και}$$

$$(x) := (x)_0 - (x)_\infty \text{ τον } \textit{κύριο διαιρέτη} \text{ (principal divisor) του } x.$$

Ένα ενδιαφέρον λήμμα είναι το παρακάτω.

ΛΗΜΜΑ 1.3.5. *Ισχύει ότι* $x \in \overline{K}^F \iff (x) = 0$.

ΑΠΟΔΕΙΞΗ. ($\Rightarrow$) Έστω $x \in \overline{K}^F\setminus\{0\}$ και P πρώτος. Από το λήμμα 1.2.5 έχουμε ότι $P\cap\overline{K}^F = \{0\}$, άρα $x\notin P$ και από το θεώρημα 1.2.10 $\operatorname{ord}_P(x)\le 0$. Ομοίως $\operatorname{ord}_P(x^{-1})\le 0$, δηλαδή $\operatorname{ord}_P(x)\ge 0$. Συνοψίζοντας καταλήγουμε ότι $\operatorname{ord}_P(x) = 0$.

($\Leftarrow$) Άμεσο από το πόρισμα 1.2.15. ♠

Μια ειδική υποομάδα ιδιαίτερης σημασίας είναι η παρακάτω.

ΟΡΙΣΜΟΣ 1.3.6. Το σύνολο

$$\mathcal{P}_F := \{\,(x) \mid x \in F\setminus\{0\}\,\}$$

ονομάζεται *ομάδα κύριων διαιρετών* (group of princpal divisors) του F/K.

Είναι προφανές ότι το $\mathcal{P}_F$ είναι υποομάδα της $\mathcal{D}_F$. Έτσι έχει νόημα και ο παρακάτω ορισμός.

ΟΡΙΣΜΟΣ 1.3.7. Η πηλικοομάδα

$$\mathcal{C}_F := {}^{\mathcal{D}_F}\!/_{\mathcal{P}_F}$$

ονομάζεται *ομάδα κλάσεων διαιρετών*. Αν $D\in\mathcal{D}_F$ η αντίστοιχη κλάση συμβολίζεται με $[D]$. Δύο διαιρέτες $D, D'\in\mathcal{D}_F$ ονομάζονται *ισοδύναμοι* αν $[D] = [D']$ (συμβολικά $D\sim D'$).

Στη συνέχεια ορίζουμε τους $\mathcal{L}$ χώρους που θα παίξουν κι αυτοί πρωταγωνιστικό ρόλο στη θεωρία μας και στο θεώρημα Riemann-Roch.

ΟΡΙΣΜΟΣ 1.3.8. Έστω $A \in \mathcal{D}_F$, έχουμε ότι

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

Μια πολύ χρήσιμη παρατήρηση είναι ότι $\mathcal{L}(A) \neq \{0\}$ ανν υπάρχει $A' \sim A$, με $A' \geq 0$. Η παρακάτω πρόταση μας δείχνει κάποιες πολύ σημαντικές ιδιότητες των $\mathcal{L}$ χώρων.

ΠΡΟΤΑΣΗ 1.3.9. *Έστω $A \in \mathcal{D}_F$. Τότε*

(α΄) το $\mathcal{L}(A)$ είναι διανυσματικός χώρος πάνω από το K,
(β΄) αν $A' \in \mathcal{D}_F$ με $A' \sim A$, τότε $\mathcal{L}(A) \cong \mathcal{L}(A')$ ως διανυσματικοί χώροι,
(γ΄) $\mathcal{L}(0) = K$ και
(δ΄) αν $A < 0$ τότε $\mathcal{L}(A) = \{0\}$.

ΑΠΟΔΕΙΞΗ. **α΄)** Έστω $x, y \in \mathcal{L}(A)$ και $a \in K$. Τότε για κάθε $P \in \mathbb{P}_F$ ισχύει ότι

$$\operatorname{ord}_P(x+y) \geq \min\{\operatorname{ord}_P(x), \operatorname{ord}_P(y)\} \geq -\operatorname{ord}_P(A),$$

δηλαδή $x + y \in \mathcal{L}(A)$ και

$$\operatorname{ord}_P(ax) = \operatorname{ord}_P(a) + \operatorname{ord}_P(x) \geq -\operatorname{ord}_P(A),$$

δηλαδή $ax \in \mathcal{L}(A)$.

β΄) Αφού $A \sim A'$ έχουμε ότι $A = A' + (z)$ για κάποιο $z \in F \setminus \{0\}$. Θεωρούμε τις απεικονίσεις

$$\phi : \begin{array}{ccc} \mathcal{L}(A) & \to & \mathcal{L}(A') \\ x & \mapsto & xz \end{array} \quad \text{και} \quad \phi' : \begin{array}{ccc} \mathcal{L}(A') & \to & \mathcal{L}(A) \\ x & \mapsto & xz^{-1} \end{array}$$

και παρατηρούμε ότι είναι καλά ορισμένες, K-γραμμικές και η μια αντίστροφη της άλλης. Έτσι η ϕ είναι ισομορφισμός.

γ΄) Προφανώς $K \subseteq \mathcal{L}(0)$. Έστω τώρα $x \in \mathcal{L}(0) \setminus \{0\}$, τότε $(x) \geq 0$, άρα το x δεν έχει πόλους, άρα $x \in K$ από το πόρισμα 1.2.15.

δ΄) Έστω $x \in \mathcal{L}(A) \setminus \{0\}$, τότε $(x) \geq -A > 0$, δηλαδή το x έχει ρίζες αλλά όχι πόλους, άτοπο. ♠

Στην παραπάνω πρόταση είδαμε ότι ένας $\mathcal{L}$ χώρος είναι διανυσματικός χώρος πάνω από το K. Στη συνέχεια, θα μελετήσουμε τις ιδιότητες του ως διανυσματικού χώρου και θα καταλήξουμε ότι έχει πεπερασμένη διάσταση.

ΛΗΜΜΑ 1.3.10. *Έστω $A, B \in \mathcal{D}_F$ και $A \leq B$. Τότε $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ και*

$$\dim_K \left({}^{\mathcal{L}(B)}/_{\mathcal{L}(A)} \right) \leq \deg B - \deg A.$$

ΑΠΟΔΕΙΞΗ. Το ότι $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ είναι προφανές. Για να αποδείξουμε την άλλη σχέση είναι αρκετό να υποθέσουμε ότι $B = A + P$, με $P \in \mathbb{P}_F$, και η γενική περίπτωση συνεπάγεται επαγωγικά.

Έστω λοιπόν ότι $B = A + P$, με $P \in \mathbb{P}_F$, και[4] $t \in F$ με $\operatorname{ord}_P(t) = \operatorname{ord}_P(B) = \operatorname{ord}_P(A) + 1$. Για $x \in \mathcal{L}(B)$ έχουμε ότι

$$\operatorname{ord}_P(x) \geq -\operatorname{ord}_P(B) = -\operatorname{ord}_P(t),$$

[4]Η ύπαρξη τέτοιου t εξασφαλίζεται από το θεώρημα 1.2.6.

άρα $\mathrm{ord}_P(xt) \geq 0$, δηλαδή $xt \in \mathcal{O}_P$. Επομένως έχει νόημα να μιλάμε για την παρακάτω απεικόνιση

$$\psi : \begin{array}{ccc} \mathcal{L}(B) & \to & {}^{\mathcal{O}_P}\!/_P \\ x & \mapsto & \bar{xt} \end{array},$$

η οποία είναι K-γραμμική και $x \in \ker\psi \iff \mathrm{ord}_P(xt) > 0$, δηλαδή $\mathrm{ord}_P(x) \geq -\mathrm{ord}_P(A)$. Έτσι καταλήγουμε ότι $\ker\psi = \mathcal{L}(A)$, άρα από το 1^o θεώρημα ισομορφισμών

$$\dim_K \left({}^{\mathcal{L}(B)}\!/_{\mathcal{L}(A)}\right) \leq \dim_K \left({}^{\mathcal{O}_P}\!/_P\right) = \deg P = \deg B - \deg A. \quad \spadesuit$$

ΠΡΟΤΑΣΗ 1.3.11. *Για κάθε $A \in \mathcal{D}_F$, ο $\mathcal{L}(A)$ είναι πεπερασμένης διάστασης διανυσματικός χώρος πάνω από το K.*

ΑΠΟΔΕΙΞΗ. Θεωρούμε ότι $A = A_+ + A_-$ (με A_+ και A_- τα προφανή). Αφού $\mathcal{L}(A) \subseteq \mathcal{L}(A_+)$ αρκεί να δείξουμε ότι

$$\dim_K \mathcal{L}(A_+) \leq \deg A_+ + 1.$$

Όμως $0 \leq A_+$, άρα από το λήμμα 1.3.10 ισχύει ότι

$$\dim_K \left({}^{\mathcal{L}(A_+)}\!/_{\mathcal{L}(0)}\right) \leq \deg A_+.$$

Ακόμα από την πρόταση 1.3.9(γ′) έχουμε ότι $\mathcal{L}(0) = K$, άρα

$$\dim_K \mathcal{L}(A_+) = \dim_K \left({}^{\mathcal{L}(A_+)}\!/_{\mathcal{L}(0)}\right) + 1$$

και συνδυάζοντας τα δύο παραπάνω έχουμε το ζητούμενο. $\spadesuit$

Στη τελευταία πρόταση είδαμε ότι ένας $\mathcal{L}$ χώρος είναι ένας πεπερασμένης διάστασης διανυσματικός χώρος πάνω από το K. Έτσι ο παρακάτω ορισμός έχει νόημα.

ΟΡΙΣΜΟΣ 1.3.12. Για έναν $A \in \mathcal{D}_F$ ο ακέραιος $l(A) := \dim_K \mathcal{L}(A)$ ονομάζεται η *διάσταση* του A.

Αποδεικνύεται (δες [STI, §I.3]) ότι για $x \in F \setminus K$ ισχύει ότι τα $\deg(x)_0$ και $\deg(x)_\infty$ είναι το πολύ ίσα με $[F : K(x)]$. Στο παρακάτω θεώρημα θα δούμε ότι στην πραγματικότητα ισχύει η ισότητα.

ΘΕΩΡΗΜΑ 1.3.13. *Για $x \in F \setminus K$ ισχύει ότι*

$$\deg(x)_0 = \deg(x)_\infty = [F : K(x)].$$

ΑΠΟΔΕΙΞΗ. Θέτουμε $n := [F : K(x)]$ και $B := (x)_\infty$ και σύμφωνα με τα παραπάνω αρκεί να δείξουμε ότι $\deg B \geq n$. Επιλέγουμε $\{u_1, \ldots, u_n\}$ μια βάση της επέκτασης $F/K(x)$ και $C \in \mathcal{D}_F$ τέτοιο ώστε $C \geq 0$ και $(u_i) \geq -C$ για κάθε $i = 1, \ldots, n$. Ακόμα, έπεται άμεσα από τους ορισμούς ότι $\forall\, k \geq 0$ ισχύει ότι $x^i u_j \in \mathcal{L}(kB + C)$ για $0 \leq i \leq k$ και $1 \leq j \leq n$. Επίσης, εύκολα βλέπουμε ότι τα παραπάνω στοιχεία είναι γραμμικά ανεξάρτητα πάνω από το K άρα

$$l(kB + C) \geq n(k + 1) \tag{1.7}$$

για κάθε $k \geq 0$. Θέτουμε $c := \deg C$ και από την απόδειξη της 1.3.11 παίρνουμε ότι $n(k+1) \leq l(kB+C) \leq k \cdot \deg B + c + 1$. Έτσι

$$k(\deg B - n) \geq n - c - 1 \tag{1.8}$$

για κάθε $k \in \mathbb{N}$. Όμως $c > n$, αφού από την απόδειξη της 1.3.11 έχουμε ότι $c > l(C)$ αφού $C \geq 0$ και $l(C) \geq n$ από (1.7) για $k = 0$. Έτσι η (1.8) δίνει άτοπο αν $\deg B < n$, άρα $\deg B \geq n$. ♠

Το παραπάνω θεώρημα αποδεικνύεται ευκολότερα αν υποθέσουμε ότι το K είναι τέλειο σώμα και χρησιμοποιήσουμε τις ιδιότητες του $K[x]$ ως δακτυλίου Dedekind[5] (δες [Ros, σελ. 47]), όμως εδώ προτιμήσαμε μια πιο συγκεκριμένη προσέγγιση. Τέλος, πριν κλείσουμε το κεφάλαιο ας δούμε μερικά άμεσα πορίσματα του τελευταίου θεωρήματος.

ΠΟΡΙΣΜΑ 1.3.14. *Αν $x \in F \setminus \{0\}$, τότε $\deg(x) = 0$.*

ΑΠΟΔΕΙΞΗ. Άμεσο από το θεώρημα 1.3.13 και τον ορισμό 1.3.4. ♠

ΠΟΡΙΣΜΑ 1.3.15. *Έστω $A, A' \in \mathcal{D}_F$ με $A \sim A'$. Τότε $l(A) = l(A')$ και $\deg A = \deg A'$.*

ΑΠΟΔΕΙΞΗ. Το ζητούμενο έπεται άμεσα από το πόρισμα 1.3.14 και την πρόταση 1.3.9(β′). ♠

ΠΟΡΙΣΜΑ 1.3.16. *Αν $A \in \mathcal{D}_F$ με $\deg A \leq 0$ τότε $l(A) = 0$ εκτός αν $A \sim 0$, οπότε $l(A) = 1$.*

ΑΠΟΔΕΙΞΗ. Αν $\deg A < 0$ και $\exists\, x \in \mathcal{L}(A) \setminus \{0\}$, τότε $\deg((x)+A) = \deg A < 0$, από το πόρισμα 1.3.14, και $\deg((x)+A) \geq 0$, από τον ορισμό του $\mathcal{L}(A)$, άτοπο, άρα $\mathcal{L}(A) = \{0\}$ και $l(A) = 0$. Αν $\deg A = 0$ και $\exists\, x \in \mathcal{L}(A) \setminus \{0\}$, τότε $(x)+A \geq 0$ και $\deg((x)+A) = 0$, άρα $(x)+A = 0$, άρα $A \sim 0$. Τέλος, αν $A \sim 0$ τότε από πόρισμα 1.3.15 $l(A) = l(0)$ και, μιας που $\mathcal{L}(0) = K$ από την πρόταση 1.3.9(γ′), $l(0) = 1$. ♠

[5]Για τον ορισμό του δακτυλίου Dedekind δες [Neu, σελ. 18].

ΚΕΦΑΛΑΙΟ 2

Το θεώρημα Riemann-Roch

Το κεντρικό αποτέλεσμα του κεφαλαίου αυτού είναι το θεώρημα Riemann-Roch. Το θεώρημα Riemann-Roch έχει τις ρίζες του στην Αλγεβρική Γεωμετρία, ενώ κάτι αντίστοιχο δεν υπάρχει στην κλασική Θεωρία Αριθμών.

Αναφέρουμε το θεώρημα Riemann-Roch διότι είναι ένα πανίσχυρο εργαλείο, το οποίο μας βοηθάει να έχουμε αποτελέσματα στη Θεωρία Αριθμών σε σώματα συναρτήσεων, ευκολότερα απ᾽ ότι στην κλασική Θεωρία Αριθμών, όπως θα δούμε και στα επόμενα κεφάλαια. Η ισχύς του θεωρήματος Riemann-Roch είναι τόσο μεγάλη που κατά πολλούς πρόκειται για το σημαντικότερο αποτέλεσμα της θεωρίας των σωμάτων συναρτήσεων.

Στο κεφάλαιο αυτό θα θεωρούμε πάντα ότι το F/K είναι σώμα συναρτήσεων και ότι $\overline{K}^F = K$.

2.1. Προαπαιτούμενες έννοιες

Στην παράγραφο αυτή το βασικό μας μέλημα είναι να ορίσουμε το *γένος* ενός σώματος συναρτήσεων, καθώς αυτό θα παίξει καθοριστικό ρόλο. Ας ξεκινήσουμε λοιπόν από μια βοηθητική πρόταση.

ΠΡΟΤΑΣΗ 2.1.1. *Υπάρχει κάποια σταθερά $\gamma \in \mathbb{Z}$ τέτοια ώστε για κάθε $A \in \mathcal{D}_F$ να ισχύει*

$$\deg A - l(A) \leq \gamma.$$

ΑΠΟΔΕΙΞΗ. Κατ᾽ αρχάς παρατηρούμε από το λήμμα 1.3.10 έχουμε ότι αν A_1, A_2 είναι διαιρέτες, τότε

$$A_1 \leq A_2 \Rightarrow \deg A_1 - l(A_1) \leq \deg A_2 - l(A_2). \tag{2.1}$$

Θεωρώ ένα αυθαίρετο $x \in F \setminus K$, το οποίο θα παίξει βοηθητικό ρόλο στην απόδειξη, και έστω $B := (x)_\infty$. Τότε, ακολουθώντας την ίδια διαδικασία με εκείνη της απόδειξης του θεωρήματος 1.3.13, καθώς και το 1.3.13 καταλήγουμε ότι υπάρχει κάποιο $C \in \mathcal{D}_F$, που εξαρτάται από το x, τέτοιο ώστε $C \geq 0$ και για κάθε $k \geq 0$ ισχύει ότι

$$l(kB + C) \geq (k+1)\deg B. \tag{2.2}$$

Ακόμα, από το λήμμα 1.3.10 έχουμε ότι για κάθε $k \geq 0$ ισχύει ότι

$$\begin{aligned} & l(kB + C) - l(kB) \leq \deg(kB + C) - \deg(kB) \\ \Rightarrow \quad & l(kB + C) \leq \deg C + l(kB). \end{aligned} \tag{2.3}$$

Συνδυάζοντας τις (2.2) και (2.3) καταλήγουμε ότι για κάθε $k \geq 0$

$$l(kB) \geq (k+1)\deg B - \deg C = \deg(kB) + (\deg B - \deg C)$$

δηλαδή για κάποιο $\gamma \in \mathbb{Z}$ ισχύει ότι

$$\deg(kB) - l(kB) \leq \gamma. \tag{2.4}$$

Θέλουμε να δείξουμε ότι η (2.4) ισχύει ακόμα κι αν αντικαταστήσουμε το kB με το τυχαίο στοιχείο του $\mathcal{D}_F$.

Ισχυριζόμαστε ότι για κάθε $A \in \mathcal{D}_F$ υπάρχουν $A_1, D \in \mathcal{D}_F$ και $k \in \mathbb{Z}_{\geq 0}$ τέτοιοι ώστε $A \leq A_1$, $A_1 \sim D$ και $D \leq kB$. Πράγματι, αν επιλέξουμε κάποιο $A_1 \in \mathcal{D}_F$ τέτοιο ώστε $A_1 \geq A$ και $A_1 \geq 0$, τότε για k αρκετά μεγάλο

$$\begin{array}{rcll} l(kB - A_1) & \geq & l(kB) - \deg A_1 & (\text{από το λήμμα 1.3.10}) \\ & \geq & \deg(kB) - \gamma - \deg A_1 & (\text{από την (2.4)}) \\ & > & 0 & (\text{για αρκετά μεγάλο } k)\ . \end{array}$$

Άρα υπάρχει $z \in \mathcal{L}(kB - A_1) \setminus \{0\}$ και θέτοντας $D := A_1 - (z)$ παίρνουμε ότι $A_1 \sim D$ και $D \leq A_1 - (A_1 - kB) = kB$.

Έτσι, υποθέτουμε ότι A_1 και D όπως παραπάνω και έχουμε ότι

$$\begin{array}{rcll} \deg A - l(A) & \leq & \deg A_1 - l(A_1) & (\text{από την (2.1)}) \\ & = & \deg D - l(D) & (\text{από πόρισμα 1.3.15}) \\ & \leq & \deg(kB) - l(kB) & (\text{από την (2.1)}) \\ & \leq & \gamma & (\text{από την (2.4)})\ , \end{array}$$

δηλαδή το ζητούμενο. ♣

Σύμφωνα με την παραπάνω πρόταση έχει νόημα ο παρακάτω ορισμός.

Ορισμος 2.1.2. Το *γένος* (genus) του σώματος συναρτήσεων F/K ορίζεται ως

$$g := \max\{\deg A - l(A) + 1 \mid A \in \mathcal{D}_F\}.$$

Το γένος ενός σώματος συναρτήσεων είναι καθοριστικής σημασίας, όμως εν γένει ο υπολογισμός του δεν είναι εύκολος. Ακόμα ισχύει ότι

$$g \geq 0. \tag{2.5}$$

Το αποτέλεσμα αυτό το λαμβάνουμε αν θεωρήσουμε τον μηδενικό διαιρέτη και παρατηρήσουμε ότι $\deg 0 = 0$ και $l(0) = 1$, οπότε $\deg 0 - l(0) + 1 = 0$ και άρα, από τον ορισμό του γένους, $g \geq 0$. Μια άλλη σχέση που απορρέι άμεσα από τον ορισμό του γένους είναι ότι για κάθε $A \in \mathcal{D}_F$ ισχύει ότι

$$l(A) \geq \deg A + 1 - g, \tag{2.6}$$

ή αλλιώς η *ανισότητα Riemann*. Ακόμα ισχύει το παρακάτω θεώρημα.

Θεωρημα 2.1.3 (Riemann). *Αν g το γένος του F/K τότε υπάρχει κάποιο $c \in \mathbb{Z}$ που εξαρτάται από το F/K τέτοιο ώστε αν $A \in \mathcal{D}_F$ με $\deg A \geq c$ ισχύει ότι*

$$l(A) = \deg A + 1 - g.$$

ΑΠΟΔΕΙΞΗ. Έστω $A_0 \in \mathcal{D}_F$ τέτοιο ώστε[1] $\deg A_0 - l(A_0) + 1 = g$ και $c := \deg A_0 + g$. Αν $A \in \mathcal{D}_F$ με $\deg A \geq c$, τότε από την ανισότητα Riemann ισχύει ότι

$$l(A - A_0) \geq \deg(A - A_0) + 1 - g \geq c - \deg A_0 + 1 - g = 1.$$

Επομένως, υπάρχει $z \in \mathcal{L}(A - A_0) \setminus \{0\}$. Θεωρούμε λοιπόν τον διαιρέτη $A' := A + (z)$, για τον οποίο ισχύει ότι $A' \geq A_0$. Έτσι έχουμε

$$\begin{array}{rcll} \deg A - l(A) & = & \deg A' - l(A') & \text{(από πόρισμα 1.3.15)} \\ & \geq & \deg A_0 - l(A_0) & \text{(από λήμμα 1.3.10)} \\ & = & g - 1\ . & \end{array}$$

Επομένως, $l(A) \leq \deg A + 1 - g$ και συνδυάζοντας με την ανισότητα Riemann ολοκληρώνουμε την απόδειξη. ♣

2.2. Το θεώρημα Riemann-Roch

Τονίζουμε στον αναγνώστη ότι ακόμα και για την διατύπωση του θεωρήματος Riemann-Roch χρειάζεται αρκετή ακόμα προπαρασκευή. Στην ενότητα αυτή θα διατυπώσουμε και θα αποδείξουμε το θεώρημα Riemann-Roch (θεώρημα 2.2.16). Σε ολόκληρη την ενότητα με g θα συμβολίζουμε το γένος του σώματος συναρτήσεων F/K. Θα ξεκινήσουμε δίνοντας κάποιους χρήσιμους ορισμούς.

ΟΡΙΣΜΟΣ 2.2.1. Για $A \in \mathcal{D}_F$, ο ακέραιος

$$i(A) := l(A) - \deg A + g - 1$$

ονομάζεται *ιδιαιτερότητα* (index of speciality) του A.

Η ανισότητα Riemann (σχέση (2.6)) μας εξασφαλίζει ότι για κάθε $A \in \mathcal{D}_F$ ισχύει ότι $i(A) \geq 0$, ενώ από το θεώρημα Riemann (θεώρημα 2.1.3) έχουμε ότι αν $\deg A$ είναι αρκετά μεγάλο, τότε $i(A) = 0$.

ΟΡΙΣΜΟΣ 2.2.2. Το σύνολο

$$\mathcal{A}_F := \left\{ (\alpha_P)_{P \in \mathbb{P}_F} \in \prod_{P \in \mathbb{P}_F} F \;\middle|\; \alpha_P \in \mathcal{O}_P \text{ για σχεδόν όλα τα } P \in \mathbb{P}_F \right\}$$

ονομάζεται *δακτύλιος διαχωρισμών* (adele space, repartition space, adele ring ή idèle ring).

Εύκολα μπορούμε να δούμε ότι ο δακτύλιος διαχωρισμών ενός σώματος συναρτήσεων έχει πράγματι δομή δακτυλίου, αλλά αυτό δε θα μας απασχολήσει ιδιαίτερα. Αντίθετα, σημαντικό ρόλο στη θεωρία θα παίξει το γεγονός ότι έχει και δομή K-διανυσματικού χώρου.

Επίσης, κάθε $x \in F$ έχει πεπερασμένες το πλήθος ρίζες και πόλους [STI, σελ. 14], άρα η εμβύθιση

$$\phi : \begin{array}{ccc} F & \hookrightarrow & \mathcal{A}_F \\ z & \mapsto & (z)_{P \in \mathbb{P}_F} \end{array}$$

[1] Η ύπαρξη τέτοιου A_0 εξασφαλίζεται από τον ορισμό του γένους.

είναι καλά ορισμένη, κι έτσι μπορούμε να δούμε το F ως K-υπόχωρο του $\mathcal{A}_F$. Επίσης, μπορούμε να επεκτείνουμε κατά φυσικό τρόπο και την τάξη ενός πρώτου από το F στο $\mathcal{A}_F$, οπότε για κάθε $P_1 \in \mathbb{P}_F$ ορίζουμε

$$\mathrm{ord}_{P_1} : \begin{array}{ccc} \mathcal{A}_F & \to & \mathbb{Z} \cup \{\infty\} \\ (\alpha_P)_{P\in\mathbb{P}_F} & \mapsto & \mathrm{ord}_{P_1}(\alpha_{P_1}) \end{array}$$

και το γεγονός ότι αν $\alpha \in \mathcal{A}_F$, τότε $\mathrm{ord}_P(\alpha) \geq 0$ για σχεδόν όλα τα $P \in \mathbb{P}_F$ είναι άμεσο από τους ορισμούς.

Ας δούμε τώρα μια πολύ σημαντική οικογένεια K-υπόχωρων του $\mathcal{A}_F$.

Ορισμος 2.2.3. Για $A \in \mathcal{D}_F$ ορίζουμε

$$\mathcal{A}_F(A) := \{\alpha \in \mathcal{A}_F \mid \mathrm{ord}_P(\alpha) \geq -\mathrm{ord}_P(A)\ \forall\, P \in \mathbb{P}_F\}.$$

Το παρακάτω θεώρημα θα μας βοηθήσει να έχουμε μια πρώτη «εκδοχή» του θεωρήματος Riemann-Roch καθώς και έναν ακόμα χαρακτηρισμό του γένους.

Θεωρημα 2.2.4. *Για κάθε $A \in \mathcal{D}_F$ ισχύει ότι*

$$i(A) = \dim_K \left({}^{\mathcal{A}_F}\!/_{\mathcal{A}_F(A)+F} \right).$$

Αποδειξη. Κατ' αρχάς, θα αποδείξουμε ότι αν $A_1, A_2 \in \mathcal{D}_F$ με $A_1 \leq A_2$, τότε $\mathcal{A}_F(A_1) \subseteq \mathcal{A}_F(A_2)$ και

$$\dim_K \left({}^{\mathcal{A}_F(A_2)}\!/_{\mathcal{A}_F(A_1)} \right) = \deg A_2 - \deg A_1. \tag{2.7}$$

Το ότι $\mathcal{A}_F(A_1) \subseteq \mathcal{A}_F(A_2)$ είναι προφανές. Για την απόδειξη της (2.7) αρκεί να δείξουμε την περίπτωση $A_2 = A_1 + P_1$ με $P_1 \in \mathbb{P}_F$, και η γενική περίπτωση έπεται με επαγωγή. Επιλέγουμε[2] $t \in F$ με $\mathrm{ord}_{P_1}(t) = \mathrm{ord}_{P_1}(A_1) + 1$ και ομοίως με την απόδειξη του λήμματος 1.3.10 η απεικόνηση

$$\phi : \begin{array}{ccc} \mathcal{A}_F(A_2) & \to & {}^{\mathcal{O}_{P_1}}\!/_{P_1} \\ (\alpha_P)_{P\in\mathbb{P}_F} & \mapsto & t\bar{\alpha}_{P_1} \end{array}$$

είναι καλά ορισμένη, K-γραμμική και $\ker\phi = \mathcal{A}_F(A_1)$. Ακόμα, παρατηρούμε ότι για κάθε $x \in \mathcal{O}_{P_1}$ αν $(\beta_P)_{P\in\mathbb{P}_F} \in \mathcal{A}_F$ με β_P τέτοια ώστε $\mathrm{ord}_P(\beta_P) = -\mathrm{ord}_P(A_2)$ για $P \neq P_1$ και $\beta_{P_1} = t^{-1}x$, τότε $(\beta_P)_{P\in\mathbb{P}_F} \in \mathcal{A}_F(A_2)$ και $\phi((\beta_P)_{P\in\mathbb{P}_F}) = \bar{x}$, δηλαδή η ϕ είναι επί. Έτσι, από το 1^o θεώρημα ισομορφισμών παίρνουμε την (2.7).

Στη συνέχεια θα αποδείξουμε ότι αν A_1, A_2 όπως πριν, τότε

$$\begin{aligned} &\dim_K \left({}^{\mathcal{A}_F(A_2)+F}\!/_{\mathcal{A}_F(A_1)+F} \right) \\ &\qquad = (\deg A_2 - l(A_2)) - (\deg A_1 - l(A_1)). \end{aligned} \tag{2.8}$$

Πράγματι, θεωρούμε την ακολουθία

$$\begin{aligned} 0 \xrightarrow{\sigma_1} {}^{\mathcal{L}(A_2)}\!/_{\mathcal{L}(A_1)} &\xrightarrow{\sigma_2} {}^{\mathcal{A}_F(A_2)}\!/_{\mathcal{A}_F(A_1)} \\ &\xrightarrow{\sigma_3} {}^{\mathcal{A}_F(A_2)+F}\!/_{\mathcal{A}_F(A_1)+F} \xrightarrow{\sigma_4} 0 \end{aligned} \tag{2.9}$$

[2]Η ύπαρξη τέτοιου t εξασφαλίζεται από τον ορισμό της τάξης ενός πρώτου.

με σ_i τα προφανή. Έχουμε ότι προφανώς $\operatorname{im}\sigma_1 = \ker\sigma_2$, $\operatorname{im}\sigma_3 = \ker\sigma_4$ και $\operatorname{im}\sigma_2 \subseteq \ker\sigma_3$. Έστω τώρα $\alpha \in \mathcal{A}_F(A_2)$ με $\sigma_3(\alpha + \mathcal{A}_F(A_1)) = 0$, τότε $\alpha \in \mathcal{A}_F(A_1) + F$ οπότε υπάρχει κάποιο $x \in F$ με $\alpha - x \in \mathcal{A}_F(A_1)$. Καθώς $\mathcal{A}_F(A_1) \subseteq \mathcal{A}_F(A_2)$ καταλήγουμε ότι $x \in \mathcal{A}_F(A_2) \cap F = \mathcal{L}(A_2)$. Έτσι $\alpha + \mathcal{A}_F(A_1) = x + \mathcal{A}_F(A_1) = \sigma_2(x + \mathcal{L}(A_1))$, δηλαδή $\ker\sigma_3 \subseteq \operatorname{im}\sigma_2$, δηλαδή συνολικά $\operatorname{im}\sigma_2 = \ker\sigma_3$. Έτσι η ακολουθία στην (2.9) είναι βραχέια ακριβής (δες [Rei, σελ. 45]) και άρα χρησιμοποιώντας και την (2.7) παίρνουμε:

$$\begin{aligned}\dim_K \left({}^{\mathcal{A}_F(A_2)+F}\!/_{\mathcal{A}_F(A_1)+F}\right) &= \dim_K \left({}^{\mathcal{A}_F(A_2)}\!/_{\mathcal{A}_F(A_1)}\right) - \dim_K \left({}^{\mathcal{L}(A_2)}\!/_{\mathcal{L}(A_1)}\right)\\ &= (\deg A_2 - \deg A_1) - (l(A_2) - l(A_1)).\end{aligned}$$

Ακόμα, θα δείξουμε ότι αν $B \in \mathcal{D}_F$ με $l(B) = \deg B + 1 - g$ τότε

$$\mathcal{A}_F = \mathcal{A}_F(B) + F. \tag{2.10}$$

Πράγματι, κατ᾽ αρχάς παρατηρούμε ότι από το λήμμα 1.3.10 αν $B_1 \geq B$, τότε

$$l(B_1) \leq \deg B_1 + l(B) - \deg B = \deg B_1 + 1 - g.$$

Ταυτόχρονα από την ανισότητα Riemann (σχέση (2.6)) $l(B_1) \geq \deg B_1 + 1 - g$, άρα συνολικά

$$l(B_1) = \deg B_1 + 1 - g \quad \text{για κάθε} \quad B_1 \geq B. \tag{2.11}$$

Έστω τώρα $\alpha \in \mathcal{A}_F$. Προφανώς υπάρχει $B_1 \geq B$ τέτοιο ώστε $\alpha \in \mathcal{A}_F(B_1)$. Από τις (2.8) και (2.11) έχουμε

$$\begin{aligned}\dim_K \left({}^{\mathcal{A}_F(B_1)+F}\!/_{\mathcal{A}_F(B)+F}\right) &= (\deg B_1 - l(B_1)) - (\deg B - l(B))\\ &= (g-1) - (g-1) = 0,\end{aligned}$$

δηλαδή $\mathcal{A}_F(B) + F = \mathcal{A}_F(B_1) + F$ και εφόσον $\alpha \in \mathcal{A}_F(B_1)$ καταλήγουμε ότι $\alpha \in \mathcal{A}_F(B) + F$, δηλαδή δείξαμε την (2.10).

Τέλος, έστω A διαιρέτης. Από το θεώρημα Riemann (θ. 2.1.3) υπάρχει κάποιος διαιρέτης $A_1 \geq A$ τέτοιος ώστε $l(A_1) = \deg A_1 + 1 - g$. Από την (2.10), $\mathcal{A}_F = \mathcal{A}_F(A_1) + F$ και έτσι η (2.8) δίνει

$$\begin{aligned}\dim_K \left({}^{\mathcal{A}_F}\!/_{\mathcal{A}_F(A)+F}\right) &= \dim_K \left({}^{\mathcal{A}_F(A_1)+F}\!/_{\mathcal{A}_F(A)+F}\right)\\ &= (\deg A_1 - l(A_1)) - (\deg A - l(A))\\ &= (g-1) + l(A) - \deg A = i(A).\end{aligned}$$ ♣

Το παραπάνω θεώρημα μας δείχνει ότι για κάθε $A \in \mathcal{D}_F$ ισχύει ότι

$$l(A) = \deg A + 1 - g + \dim_K \left({}^{\mathcal{A}_F}\!/_{\mathcal{A}_F(A)+F}\right), \tag{2.12}$$

που είναι μια προκαταρκτική διατύπωση του θεωρήματος Riemann-Roch. Ακόμα, μας δίνει έναν ακόμη τρόπο υπολογισμού του γένους, όπως βλέπουμε στο παρακάτω πόρισμα.

ΠΟΡΙΣΜΑ 2.2.5. *Ισχύει ότι*

$$g = \dim_K \left({}^{\mathcal{A}_F}/_{\mathcal{A}_F(0)+F} \right).$$

ΑΠΟΔΕΙΞΗ. Από το θεώρημα 2.2.4 ισχύει ότι

$$\dim_K \left({}^{\mathcal{A}_F}/_{\mathcal{A}_F(0)+F} \right) = i(0) := l(0) - \deg 0 + g - 1 = g. \qquad \clubsuit$$

Στη συνέχεια θα δούμε την έννοια του διαφορικού Weil.

ΟΡΙΣΜΟΣ 2.2.6. Ένα *διαφορικό Weil* του σώματος συναρτήσεων F/K είναι μια K-γραμμική απεικόνιση $\omega : \mathcal{A}_F \to K$, που μηδενίζεται στο $\mathcal{A}_F(A) + F$ για κάποιο $A \in \mathcal{D}_F$. Το σύνολο των διαφορικών Weil του F/K συμβολίζεται με Ω_F.

Εύκολα βλέπει κανείς ότι το Ω_F είναι K-διανυσματικός χώρος (με την προφανή πρόσθεση και για πολλαπλασιασμό αν $x \in K$, $\xi \in \mathcal{A}_F$ και $\omega \in \Omega_F$ ορίζουμε ως $(x\omega)(\xi) := \omega(x\xi)$). Εύκολα βλέπει κανείς ακόμα ότι μια οικογένεια K-υπόχωρων του Ω_F περιγράφεται στον παρακάτω ορισμό.

ΟΡΙΣΜΟΣ 2.2.7. Για $A \in \mathcal{D}_F$ ορίζουμε

$$\Omega_F(A) := \{\omega \in \Omega_F \mid \text{ το } \omega \text{ μηδενίζεται στο } \mathcal{A}_F(A) + F\}.$$

Είμαστε πλέον σε θέση να δώσουμε έναν ακόμη τρόπο υπολογισμού της ιδιαιτερότητας ενός διαιρέτη.

ΛΗΜΜΑ 2.2.8. *Για κάθε $A \in \mathcal{D}_F$ έχουμε ότι* $\dim_K \Omega_F(A) = i(A)$.

ΑΠΟΔΕΙΞΗ. Κάθε στοιχείο του $\Omega_F(A)$ είναι K-γραμμική απεικόνιση $\mathcal{A}_F \to K$ και, άρα, δεδομένου ότι το $\mathcal{A}_F$ είναι K-διανυσματικός χώρος, χαρακτηρίζεται πλήρως από την εικόνα των στοιχείων της K-βάσης του $\mathcal{A}_F$. Ταυτόχρονα όμως, ακριβώς όσα από αυτά αποτελούν την K-βάση του $\mathcal{A}_F(A) + F$ είναι δεσμευμένα καθώς πρέπει από τον ορισμό 2.2.7 να ισούνται με μηδέν. Έτσι καταλήγουμε ότι

$$\dim_K \Omega_F(A) = \dim_K \left({}^{\mathcal{A}_F}/_{\mathcal{A}_F(A)+F} \right)$$

και από το θεώρημα 2.2.4 το ζητούμενο έπεται άμεσα. $\clubsuit$

Από το τελευταίο λήμμα βλέπουμε ότι αν πάρουμε έναν διαιρέτη A έχουμε

$$\dim_K \Omega_F(A) = i(A) = l(A) - \deg A + g - 1, \tag{2.13}$$

έτσι αν $\deg A \leq -2$, τότε (λαμβάνοντας υπ᾽ όψην το πόρισμα 1.3.16) $\dim_K \Omega_F(A) \geq 1$, δηλαδή $\Omega_F(A) \supsetneqq \{0\}$, οπότε και $\Omega_F \supsetneqq \{0\}$.

Μια ακόμα πολύ σημαντική παρατήρηση είναι ότι από το λήμμα 2.2.8, τον ορισμό 2.2.1 και το πόρισμα 1.3.16 έχουμε ότι για το γένος ισχύει ότι

$$g = \dim_K \Omega_F(0), \tag{2.14}$$

δηλαδή το γένος μπορεί να υπολογιστεί μέσω των διαφορικών Weil.

Τέλος, παρατηρούμε ότι ο K-βαθμωτός πολλαπλασιασμός που ορίσαμε παραπάνω, για να δείξουμε ότι το Ω_F είναι K-διανυσματικός χώρος, επεκτείνεται φυσιολογικά και στο F. Έτσι το Ω_F είναι και F-διανυσματικός χώρος, με τη διαφορά όμως ότι τώρα αν $x \in F$ και $\omega \in \Omega_F$, με το ω να μηδενίζεται στο $\mathcal{A}_F(A) + F$, το $x\omega$ μηδενίζεται στο $\mathcal{A}_F(A + (x)) + F$. Έτσι τα $\Omega_F(A)$ με $A \in \mathcal{D}_F$ δεν είναι F-υπόχωροι του Ω_F.

Μια επίσης χρήσιμη παρατήρηση, που απορρέει από το παραπάνω είναι ότι αν $x \in F$, $\omega \in \Omega_F \setminus \{0\}$ και $x\omega = 0$, τότε $x = 0$, ενώ (προφανώς) ισχύει και το αντίστροφο.

Η διάσταση του Ω_F ως F-διανυσματικού χώρου θα μας απασχολήσει, αφού είναι καθοριστικής σημασίας στην απόδειξη του θεωρήματος Riemann-Roch· πρώτα όμως, θα ορίσουμε το διαιρέτη ενός διαφορικού Weil. Το παρακάτω λήμμα θα μας βοηθήσει να είναι καλά ορισμένη η έννοια αυτή.

Λημμα 2.2.9. *Έστω $\omega \in \Omega_F \setminus \{0\}$. Τότε υπάρχει κάποιος μοναδικός $A \in \mathcal{D}_F$ τέτοιος ώστε $\omega(\mathcal{A}_F(A) + F) = \{0\}$ και ο A να είναι μεγιστικός ως προς αυτήν την ιδιότητα.*

Αποδειξη. Από το θεώρημα Riemann (θ. 2.1.3) υπάρχει κάποιο c τέτοιο ώστε $i(A) = 0$ για κάθε $A \in \mathcal{D}_F$ με $\deg A \geq c$. Όμως από το θεώρημα 2.2.4 έχουμε ότι αν $\deg A \geq c$, τότε $\mathcal{A}_F = \mathcal{A}_F(A) + F$, άρα το ω μηδενίζεται σε ολόκληρο το $\mathcal{A}_F$, δηλαδή $\omega = 0$, άτοπο. Έτσι αν θέσουμε $\mathcal{T} := \{A \in \mathcal{D}_F \mid \omega(\mathcal{A}_F(A) + F) = \{0\}\}$ έχουμε ότι οι βαθμοί όλων των στοιχείων του $\mathcal{T}$ φράσσονται από το c.

Έστω λοιπόν $A \in \mathcal{T}$ μέγιστου βαθμού. Θα δείξουμε ότι ο A είναι ο ζητούμενος διαιρέτης. Έστω λοιπόν $A' \in \mathcal{T}$, τότε προφανώς $\operatorname{lcm}(A, A') \in \mathcal{T}$, όπου

$$\operatorname{lcm}(A, A') := \sum_{P \in \mathbb{P}_F} \max\{\operatorname{ord}_P(A), \operatorname{ord}_P(A')\} P \in \mathcal{D}_F.$$

Όμως $\deg \operatorname{lcm}(A, A') \geq \deg A$, άρα από την μεγιστότητα του $\deg A$ έπεται ότι $\deg \operatorname{lcm}(A, A') = \deg A$, δηλαδή θα πρέπει $\operatorname{lcm}(A, A') = A$, δηλαδή $A' \leq A$. Η μοναδικότητα του A είναι τετριμμένη. ♣

Από το παραπάνω λήμμα έχει νόημα ο παρακάτω ορισμός.

Ορισμος 2.2.10. Ο διαιρέτης που περιγράφεται στο λήμμα 2.2.9 ονομάζεται *διαιρέτης του διαφορικού Weil* ω και συμβολίζεται ως (ω). Ακόμα αν $W \in \mathcal{D}_F$ τέτοιο ώστε $W = (\omega)$ για κάποιο $\omega \in \Omega_F \setminus \{0\}$, τότε ο W ονομάζεται *κανονικός διαιρέτης*.

Μια σχεδόν προφανής ιδιότητα των διαιρετών Weil διατυπώνεται στο παρακάτω λήμμα.

Λημμα 2.2.11. *Αν $A \in \mathcal{D}_F$ και $\omega \in \Omega_F$, τότε το ω μηδενίζεται στο $\mathcal{A}_F(A) + F$ αν $A \leq (\omega)$.*

ΑΠΟΔΕΙΞΗ. Άμεσο από τους ορισμούς 2.2.3 και 2.2.10. ♣

Άλλη μια ιδιότητα των διαιρετών διαφορικών Weil δίνεται στην παρακάτω πρόταση.

ΠΡΟΤΑΣΗ 2.2.12. *Αν* $x \in F^*$ *και* $\omega \in \Omega_F \setminus \{0\}$ *ισχύει ότι*

$$(x\omega) = (x) + (\omega).$$

ΑΠΟΔΕΙΞΗ. Αν το ω μηδενίζεται στο $\mathcal{A}_F(A) + F$ το $x\omega$ μηδενίζεται στο $\mathcal{A}_F(A + (x)) + F$, άρα μιας που το ω μηδενίζεται στο $\mathcal{A}_F((\omega)) + F$, το $x\omega$ θα μηδενίζεται στο $\mathcal{A}_F((x) + (\omega)) + F$, άρα, από τη μεγιστική ιδιότητα του $(x\omega)$,

$$(\omega) + (x) \leq (x\omega).$$

Ομοίως $(x\omega) + (x^{-1}) \leq (x^{-1}x\omega) = (\omega)$. Έτσι, συνδυάζοντας τα δύο παραπάνω παίρνουμε ότι

$$(\omega) + (x) \leq (x\omega) \leq -(x^{-1}) + (\omega) = (\omega) + (x).$$ ♣

Είμαστε πλέον σε θέση να υπολογίσουμε τη διάσταση του Ω_F ως διανυσματικού χώρου πάνω από το F.

ΠΡΟΤΑΣΗ 2.2.13. *Ισχύει ότι* $\dim_F \Omega_F = 1$.

ΑΠΟΔΕΙΞΗ. Κατ' αρχάς θα δείξουμε ότι αν $\omega \in \Omega_F \setminus \{0\}$ και $x \in \mathcal{L}((\omega) - A)$, με $A \in \mathcal{D}_F$, τότε ισχύει ότι $x\omega \in \Omega_F(A)$. Πράγματι, αφού $x \in \mathcal{L}((\omega) - A)$ έχουμε ότι $(x) \geq A - (\omega)$, ενώ από την πρόταση 2.2.12 $(x\omega) = (x) + (\omega)$. Έτσι παίρνουμε ότι $(x\omega) \geq A$, δηλαδή $x\omega \in \Omega_F(A)$.

Στη συνέχεια θα δείξουμε ότι αν $\omega \in \Omega_F \setminus \{0\}$ και $A \in \mathcal{D}_F$, τότε το $\mathcal{L}((\omega) - A)\omega$ είναι K-υπόχωρος του $\Omega_F(A)$. Πράγματι από την πρόταση 1.3.9(α') το $\mathcal{L}((\omega) - A)$ είναι K-διανυσματικός χώρος, άρα εύκολα μπορεί να δει κανείς ότι και το $\mathcal{L}((\omega) - A)\omega$ θα είναι K-διανυσματικός χώρος, ενώ από την παραπάνω παρατήρηση έπεται άμεσα ότι θα είναι και υποσύνολο του $\Omega_F(A)$.

Το επόμενο βήμα μας θα είναι να δείξουμε ότι αν $\omega, \omega' \in \Omega_F \setminus \{0\}$, τότε υπάρχει κάποιο $A \in \mathcal{D}_F$ τέτοιο ώστε

$$\mathcal{L}((\omega) - A)\omega \cap \mathcal{L}((\omega') - A)\omega' \neq \{0\}.$$

Πράγματι θεωρούμε καποιο $P \in \mathbb{P}_F$ και θέτουμε $D_n := -nP$ $(n \in \mathbb{N})$. Από τη σχέση (2.13) και το πόρισμα 1.3.16 έχουμε ότι

$$\dim_K \Omega_F(D_n) = l(D_n) - \deg D_n + g - 1 = n \deg P + g - 1. \tag{2.15}$$

Από την ανισότητα Riemann (σχέση (2.6)) και το γεγονός ότι[3]

$$\dim_K \mathcal{L}((\omega) - D_n)\omega = \dim_K \mathcal{L}((\omega) - D_n),$$

ισχύει ότι

$$\dim_K \mathcal{L}((\omega) - D_n)\omega = l((\omega) + nP) \geq \deg(\omega) + n \deg P - g + 1,$$

[3]Αυτό ισχύει διότι αν $\omega \in \Omega_F \setminus \{0\}$ και $x \in F$, τότε: $x\omega = 0 \iff x = 0$, όπως είδαμε στα σχόλια μετά το λήμμα 2.2.8.

ενώ το ίδιο ισχύει και για το ω'. Έτσι παίρνουμε ότι

$$\dim_K \mathcal{L}((\omega) - D_n)\omega + \dim_K \mathcal{L}((\omega) - D_n)\omega' \geq 2n \deg P + \deg(\omega) + \deg(\omega') - 2g + 2.$$

Έτσι, για n αρκετά μεγάλο το παραπάνω άθροισμα θα γίνει μεγαλύτερο από το $n \deg P + g - 1$ που από την σχέση (2.13) ισούται με $\dim_K \Omega_F(D_n)$. Δηλαδή αν θέσουμε ως n_1 το παραπάνω περιγραφόμενο n και $A := D_{n_1}$, τότε

$$\dim_K \mathcal{L}((\omega) - A)\omega + \dim_K \mathcal{L}((\omega) - A)\omega \geq \dim_K \Omega_F(A).$$

Έτσι το τελευταίο, από στοιχειώδη γραμμική άλγεβρα και μιας που, όπως είδαμε παραπάνω, τα $\mathcal{L}((\omega) - A)\omega$ και $\mathcal{L}((\omega') - A)\omega'$ είναι K-υπόχωροι του $\Omega_F(A)$ μας δίνει το ζητούμενο αποτέλεσμα.

Είμαστε πλέον σε θέση να αποδείξουμε το θεώρημα. Δεδομένου λοιπόν, ότι $\Omega_F \neq \{0\}$ αρκεί να δείξουμε ότι για κάθε $\omega_1, \omega_2 \in \Omega_F \setminus \{0\}$, τότε υπάρχει $z \in F$ τέτοιο ώστε $\omega_1 = z\omega_2$. Πράγματι, από την προηγούμενη παράγραφο υπάρχει κάποιος $A \in \mathcal{D}_F$ τέτοιος ώστε

$$M := (\mathcal{L}((\omega_1) - A)\omega_1 \cap \mathcal{L}((\omega_2) - A)\omega_2) \setminus \{0\} \neq \emptyset.$$

Έτσι αν $m \in M$ υπάρχουν $x, y \in F^*$ τέτοια ώστε $m = x\omega_1 = y\omega_2$, δηλαδή για $z := x^{-1}y$ έχουμε το ζητούμενο. ♣

Η παραπάνω πρόταση στην ουσία μας δίνει το θεώρημα Riemann-Roch, όμως θα πρέπει να δείξουμε πρώτα μερικά πορίσματά της.

ΠΟΡΙΣΜΑ 2.2.14. *Αν $\omega \in \Omega_F \setminus \{0\}$ και $A \in \mathcal{D}_F$ τότε*

$$\mathcal{L}((\omega) - A) = \Omega_F(A).$$

ΑΠΟΔΕΙΞΗ. Έχουμε δει παραπάνω ότι και τα δύο σύνολα είναι K-διανυσματικοί χώροι, ενώ στην απόδειξη της προηγούμενης πρότασης δείξαμε ότι $\mathcal{L}((\omega) - A) \subseteq \Omega_F(A)$. Έτσι, αρκεί να δείξουμε ότι $\mathcal{L}((\omega) - A) \supseteq \Omega_F(A)$.

Έστω λοιπόν $\omega' \in \Omega_F(A)$. Από την πρόταση 2.2.13 υπάρχει $x \in F$ τέτοιο ώστε $\omega' = x\omega$. Εφόσον το ω' μηδενίζεται στο $\mathcal{A}_F(A) + F$ έχουμε (λαμβάνοντας υπ᾽ όψιν και την πρόταση 2.2.12) ότι $A \leq (\omega') = (x) + (\omega)$, δηλαδή $(x) \geq -((\omega) - A)$, δηλαδή $x \in \mathcal{L}((\omega) - A)$. ♣

ΠΟΡΙΣΜΑ 2.2.15. *Οι κανονικοί διαιρέτες αποτελούν μια κλάση διαιρετών ως προς την υποομάδα των κύριων διαιρετών $\mathcal{P}_F$.*

ΑΠΟΔΕΙΞΗ. Το ότι δύο κανονικοί διαιρέτες είναι ισοδύναμοι έπεται άμεσα από τις προτάσεις 2.2.12 και 2.2.13. Έστω τώρα $\omega \in \Omega_F \setminus \{0\}$ και $A \in [(\omega)]$. Τότε για κάποιο $x \in F^*$ θα έχουμε ότι $A = (x) + (\omega) = (x\omega)$, δηλαδή ο A είναι κανονικός διαιρέτης. ♣

Έτσι έχει νόημα να μιλάμε για την κλάση των κανονικών διαιρετών, η οποία ονομάζεται *κανονική κλάση* (canonical class) του F/K και συμβολίζεται με $\mathcal{W}_F$. Είμαστε πλέον σε θέση να αποδείξουμε το θεώρημα Riemann-Roch.

ΘΕΩΡΗΜΑ 2.2.16 (Riemann-Roch). *Αν $W \in \mathcal{W}_F$ τότε για κάθε $A \in \mathcal{D}_F$ ισχύει ότι*

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

ΑΠΟΔΕΙΞΗ. Άμεσο από τα πορίσματα 2.2.14 και 2.2.15 και την σχέση (2.13). ♣

2.3. Μερικές συνέπειες του θεωρήματος Riemann-Roch.

Το θεώρημα Riemann-Roch είναι ένα από τα ισχυρότερα εργαλεία στην θεωρία των σωμάτων συναρτήσεων. Εδώ θα δούμε κάποια άμεσα επακόλουθά του, κάποια εκ των οποίων θα βοηθήσουν και το ίδιο το θεώρημα να είναι πιο εύχρηστο. Ας ξεκινήσουμε λοιπόν χαρακτηρίζοντας την κανονική κλάση $\mathcal{W}_F$.

ΠΡΟΤΑΣΗ 2.3.1. *Για κάθε $W \in \mathcal{W}_F$ έχουμε ότι $\deg W = 2g - 2$ και $l(W) = g$.*

ΑΠΟΔΕΙΞΗ. Έστω $W \in \mathcal{W}_F$. Το θεώρημα Riemann-Roch για $A = 0$ δίνει ότι

$$l(0) = \deg 0 + 1 - g + l(W) \text{ άρα } l(W) = l(0) - 1 + g$$

και από το πόρισμα 1.3.16 θα έχουμε ότι $l(W) = g$. Ακόμα το Riemann-Roch για $A = W$ δίνει

$$l(W) = \deg W + 1 - g + l(0) \text{ άρα } \deg W = l(W) + g - 1 - l(0),$$

δηλαδή από το προηγούμενο και το πόρισμα 1.3.16, $\deg W = 2g - 2$. ♣

ΠΡΟΤΑΣΗ 2.3.2. *Αν $W \in \mathcal{D}_F$, με $\deg W = 2g-2$ και $l(W) \geq g$, τότε $W \in \mathcal{W}_F$.*

ΑΠΟΔΕΙΞΗ. Θεωρούμε κάποιο $A \in \mathcal{D}_F$, με $\deg A = 2g-2$ και $l(A) \geq g$, και κάποιο $W \in \mathcal{W}_F$. Τότε απο το θεώρημα Riemann-Roch έχουμε ότι

$$g \leq l(A) = \deg A + 1 - g + l(W - A) = g - 1 + l(W - A).$$

Έτσι $l(W - A) \geq 1$. Όμως $\deg(W - A) = 0$, έτσι από το πόρισμα 1.3.16 έχουμε ότι $W - A \sim 0$, δηλαδή $W \sim A$. ♣

Το επόμενο θεώρημα προσδιορίζει με ακρίβεια τη σταθερά c που αναφέρθηκε στο θεώρημα Riemann (θ. 2.1.3).

ΘΕΩΡΗΜΑ 2.3.3. *Η σταθερά c του θεωρήματος Riemann είναι $2g - 1$.*

ΑΠΟΔΕΙΞΗ. Έστω $A \in \mathcal{D}_F$ με $\deg A \geq 2g - 1$ και $W \in \mathcal{W}_F$. Τότε, από την πρόταση 2.3.1, έχουμε ότι $\deg W = 2g-2$, άρα $\deg(W-A) < 0$, οπότε, από το πόρισμα 1.3.16, έχουμε ότι $l(W - A) = 0$. Τώρα, το θεώρημα Riemann-Roch μας δίνει

$$l(A) = \deg A + 1 - g.$$

Το ότι η σταθερά αυτή δεν είναι μικρότερη από $2g-1$ έπεται άμεσα από την πρόταση 2.3.1, αφού $\deg W = 2g-2$ και δεν ισχύει η ζητούμενη σχέση. ♣

Στη συνέχεια θα αποδείξουμε την ύπαρξη στοιχείων του F που έχουν ένα και μοναδικό πόλο.

ΠΡΟΤΑΣΗ 2.3.4. *Αν $P \in \mathbb{P}_F$, τότε για κάθε $n \geq 2g$ υπάρχει κάποιο $x \in F$ τέτοιο ώστε $(x)_\infty = nP$.*

ΑΠΟΔΕΙΞΗ. Για $n \geq 2g$ από το θεώρημα 2.3.3 έχουμε ότι $l((n-1)P) = (n-1)\deg P + 1 - g$ και $l(nP) = n\deg P + 1 - g$. Έτσι $l((n-1)P) \neq l(nP)$, άρα $\mathcal{L}((n-1)P) \subsetneq \mathcal{L}(nP)$. Αν $x \in \mathcal{L}(nP) \setminus \mathcal{L}((n-1)P)$, τότε $(x)_\infty = nP$. ♣

Κλείνοντας το κεφάλαιο αυτό, θα δώσουμε έναν κομψό χαρακτηρισμό του ρητού σώματος συναρτήσεων

ΠΡΟΤΑΣΗ 2.3.5. *Έχουμε ότι το F/K είναι ρητό ανν $g = 0$ και υπάρχει κάποιος $A \in \mathcal{D}_F$ με $\deg A = 1$.*

ΑΠΟΔΕΙΞΗ. Στην απόδειξη θα χρησιμοποιήσουμε τους συμβολισμούς που χρησιμοποιήσαμε στο θεώρημα 1.2.16.

Έστω λοιπόν ότι $F = K(x)$. Η ύπαρξη διαιρέτη βαθμού 1 είναι τετριμμένη (π.χ. $D := P_\infty$). Ακόμα, από το θεώρημα Riemann (ϑ. 2.1.3) για $n > 0$ μεγάλο έχουμε ότι $l(nP_\infty) = n - g + 1$. Επιπλέον, τα K-γραμμικά ανεξάρτητα $1, x, \ldots, x^n$ προφανώς ανήκουν στο $\mathcal{L}(nP_\infty)$, δηλαδή $l(nP\infty) \geq n+1$. Έτσι, συνολικά $g \leq 0$. Όμως, όπως είδαμε στα σχόλια μετά τον ορισμό του γένους ισχύει ότι $g \geq 0$. Επομένως, συνολικά $g = 0$.

Αντίστροφα, έστω ότι $g = 0$ και $A \in \mathcal{D}_F$ με $\deg A = 1$. Επειδή $\deg A > 2g-1$, από το 2.3.3 θα έχουμε ότι $l(A) = 2 > 0$, άρα από την παρατήρηση στον ορισμό 1.3.8, υπάρχει κάποιο θετικό $A' \in \mathcal{D}_F$ με $A' \sim A$. Εφόσον τώρα $\dim_K \mathcal{L}(A') = l(A') = 2$, υπάρχει κάποιο $x \in \mathcal{L}(A') \setminus K$, άρα $(x) \neq 0$ και $(x) + A' \geq 0$. Όμως, εφόσον $A' \geq 0$ και $\deg A' = 1$ κάτι τέτοιο είναι εφικτό μόνο στην περίπτωση που $A' = (x)_\infty$. Έτσι, από το θεώρημα 1.3.13 θα έχουμε

$$[F : K(x)] = \deg(x)_\infty = \deg A' = 1,$$

δηλαδή $F = K(x)$. ♣

ΚΕΦΑΛΑΙΟ 3

Επεκτάσεις σωμάτων συναρτήσεων

Στο κεφάλαιο αυτό θα ορίσουμε κάποιες βασικές έννοιες περί των επεκτάσεων των σωμάτων συναρτήσεων και θα δούμε κάποιες απλές ιδιότητές τους. Βάσει των εννοιών που θα ορίσουμε στο κεφάλαιο αυτό, θα μπορούσαμε να αποδείξουμε σχετικά εύκολα τα αντίστοιχα μεγάλων προβλημάτων της κλασικής Θεωρίας Αριθμών, όπως το θεώρημα Riemann-Hurwitz ή την εικασία ABC, όμως κάτι τέτοιο ξεφεύγει από τους σκοπούς μας. Για τις αποδείξεις των παραπάνω παραπέμπουμε στο [Ros, κεφ. 7].

Ακόμα, στο κεφάλαιο αυτό θα εξακολουθήσουμε να χρησιμοποιούμε τους συμβολισμούς και τις παραδοχές των προηγούμενων κεφαλαίων και επίσης θα δεχόμαστε ότι το K είναι τέλειο[1], όπου αυτό είναι απαραίτητο.

3.1. Γενικές ιδιότητες

Στην παράγραφο αυτή θα δούμε κάποιες βασικές έννοιες και ιδιότητες των πεπερασμένων επεκτάσεων σωμάτων συναρτήσεων. Ας ξεκινήσουμε λοιπόν ορίζοντας την έννοια της επέκτασης.

Ορισμος 3.1.1. Αν F/K σώμα συναρτήσεων, L αλγεβρική επέκταση του F και $E := \overline{K}^L$, τότε το L/E είναι *επέκταση* του F/K (συμβ. $F \leq L$). Αν $[L : F] < \infty$, τότε η $F \leq L$ είναι *πεπερασμένη επέκταση*, αν $L = EF$, τότε έχουμε μια *επέκταση σταθερού σώματος* και αν $E = K$, τότε έχουμε μια *γεωμετρική επέκταση*.

Δεν είναι προφανές ότι το L/E του παραπάνω ορισμού είναι πράγματι σώμα συναρτήσεων. Αποδεικνύεται όμως (βλέπε [Mor, π. 19.18]) ότι αν $F_1/F_2/F_3$ είναι ένας πύργος επεκτάσεων σωμάτων και $\mathrm{trdeg}(F_i/F_j)$ ο βαθμός υπερβατικότητας[2] της επέκτασης σωμάτων F_i/F_j, τότε

$$\mathrm{trdeg}(F_1/F_3) = \mathrm{trdeg}(F_1/F_2) + \mathrm{trdeg}(F_2/F_3), \tag{3.1}$$

και (βλέπε [Mor, π. 19.9 & ο. 19.16]) ότι $\mathrm{trdeg}(F_i/F_j) = 0$ ανν η επέκταση F_i/F_j είναι αλγεβρική.

Έτσι, έχουμε ότι αν F, K, L και E όπως στον ορισμό 3.1.1, τότε $\mathrm{trdeg}(F/K) = 1$, $\mathrm{trdeg}(L/F) = 0$ και $\mathrm{trdeg}(E/K) = 0$. Τέλος, από

[1] Δηλαδή όλες οι αλγεβρικές επεκτάσεις του είναι διαχωρίσιμες.

[2] Για τον γενικό ορισμό του βαθμού υπερβατικότητας μιας επέκτασης βλέπε [Mor, σελ. 173–179]. Τονίζουμε ότι στην περίπτωση που $\mathrm{trdeg}(F_i/F_j) = 1$ ο γενικός ορισμός και ο ορισμός 1.1.1 ταυτίζονται, κατά προφανή τρόπο.

τη σχέση (3.1) παίρνουμε ότι $\mathrm{trdeg}(L/E) = 1$, δηλαδή το L/E είναι πράγματι σώμα συναρτήσεων και ο ορισμός 3.1.1 είναι καλός.

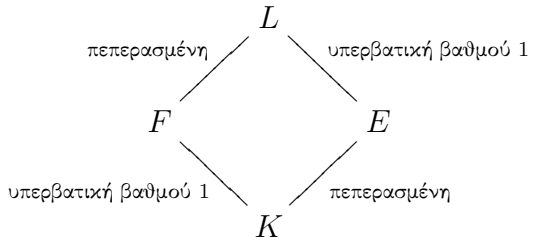
Ακόμα, ένα άμεσο συμπέρασμα του ορισμού 3.1.1 είναι το παρακάτω λήμμα.

Λημμα 3.1.2. *Αν το L/E είναι πεπερασμένη επέκταση του F/K, τότε*

$$[E : K] < \infty.$$

Απόδειξη. Θεωρούμε το σώμα συναρτήσεων L/K και το ζητούμενο έπεται άμεσα από το λήμμα 1.1.3. ♢

Ο ορισμός 3.1.1 δείχνει πολύπλοκος, αλλά το σχήμα 3.1 (που περιλαμβάνει και το λήμμα 3.1.2) τον δίνει σχηματικά και είναι διαφωτιστικό. Μια ακόμα χρήσιμη παρατήρηση είναι ότι $F \leq EF \leq L$, με $F \leq EF$ ε-



Σχημα 3.1. Το L/E είναι πεπερασμένη επέκταση του F/K.

πέκταση σταθερού σώματος και $EF \leq L$ γεωμετρική. Από εδώ και πέρα θα θεωρούμε ότι το L/E είναι πεπερασμένη επέκταση του F/K χωρίς να γίνεται αναφορά.

Στη συνέχεια, θα δούμε πώς σχετίζονται οι πρώτοι του L/E με εκείνους του F/K.

Ορισμος 3.1.3. Έστω $P \in \mathbb{P}_F$ και $\mathfrak{P} \in \mathbb{P}_L$. Λέμε ότι ο $\mathfrak{P}$ *βρίσκεται πάνω* (lies above) από τον P (συμβ. $\mathfrak{P} \mid P$) αν $\mathcal{O}_P = \mathcal{O}_{\mathfrak{P}} \cap F$ και $P = \mathfrak{P} \cap \mathcal{O}_P$.

Ας δούμε τώρα κάποια μεγέθη που χαρακτηρίζουν την περιγραφόμενη από τον παραπάνω ορισμό σχέση. Ξεκινάμε με ένα λήμμα που θα κάνει τα μεγέθη καλά ορισμένα.

Λημμα 3.1.4. *Αν P και $\mathfrak{P}$ όπως πριν, τότε*

(α′) το ${}^{\mathcal{O}_{\mathfrak{P}}}/_{\mathfrak{P}}$ είναι διανυσματικός χώρος πεπερασμένης διάστασης πάνω από το ${}^{\mathcal{O}_P}/_P$ και

(β′) $P\mathcal{O}_{\mathfrak{P}} = \mathfrak{P}^e$ για κάποιον ακέραιο $e \geq 1$.

Απόδειξη. **α′)** Από τα σχόλια πριν τον ορισμό 1.2.11 και το θεώρημα 1.2.12, τα ${}^{\mathcal{O}_P}/_P$ και ${}^{\mathcal{O}_{\mathfrak{P}}}/_{\mathfrak{P}}$ είναι διανυσματικοί χώροι πεπερασμένης διάστασης πάνω από τα K και E αντίστοιχα, ενώ λαμβάνοντας υπ᾽ όψιν το

λήμμα 3.1.2 θα πάρουμε ότι το ${}^{\mathcal{O}_\mathfrak{P}}/_{\mathfrak{P}}$ θα είναι και αυτό K-διανυσματικός χώρος πεπερασμένης διάστασης.

Έτσι, μένει να δείξουμε ότι το ${}^{\mathcal{O}_P}/_{P}$ είναι υπόχωρος του ${}^{\mathcal{O}_\mathfrak{P}}/_{\mathfrak{P}}$. Αυτό είναι άμεσο, αν παρατηρήσει κανείς ότι η απεικόνιση

$$\phi : \begin{array}{ccc} {}^{\mathcal{O}_P}/_{P} & \hookrightarrow & {}^{\mathcal{O}_\mathfrak{P}}/_{\mathfrak{P}} \\ \alpha + P & \mapsto & \alpha + \mathfrak{P} \end{array}$$

είναι μονομορφισμός.

β′) Έχουμε ότι το $P\mathcal{O}_\mathfrak{P}$ είναι μη μηδενικό γνήσιο ιδεώδες του $\mathcal{O}_\mathfrak{P}$, άρα αρκεί να δείξουμε ότι το ζητούμενο ισχύει για κάθε μη μηδενικό γνήσιο ιδεώδες του $\mathcal{O}_\mathfrak{P}$. Πράγματι, αν I μη μηδενικό γνήσιο ιδεώδες του $\mathcal{O}_\mathfrak{P}$ και[3] $\mathfrak{P} = t\mathcal{O}_\mathfrak{P}$, τότε το σύνολο $A := \{r \in \mathbb{N} \mid t^r \in I\}$ είναι μη κενό, γιατί το I θα περιέχει κάποιο μη μηδενικό και μη αντιστρέψιμο στοιχείο, δηλαδή στοιχείο του $t\mathcal{O}_\mathfrak{P}^*$, έστω $t^r u$ (με $r \geq 1$ και $u \in \mathcal{O}_\mathfrak{P}^*$), οπότε και $u^{-1}t^r u = t^r \in I$. Θέτουμε $n := \min(A)$ και έχουμε ότι $I \supseteq t^n\mathcal{O}_\mathfrak{P}$ κατά προφανή τρόπο και αν $y \in I \setminus \{0\}$, τότε $y = t^m w$ με $m \geq 1$ και $w \in \mathcal{O}_\mathfrak{P}^*$, άρα και $t^m \in I$, άρα θα πρέπει $n \leq m$ λόγω ελαχιστότητας του n, επομένως $y \in t^n\mathcal{O}_\mathfrak{P}$, δηλαδή συνολικά $I = t^n\mathcal{O}_\mathfrak{P} = \mathfrak{P}^n$. ♢

Έτσι ο παρακάτω ορισμός έχει νόημα.

Ορισμος 3.1.5. Αν $\mathfrak{P} \mid P$ ως *σχετικό βαθμό* (relative degree ή inertia degree) των $\mathfrak{P}$ και P ορίζουμε τον αριθμό

$$f(\mathfrak{P}/P) := \left[{}^{\mathcal{O}_\mathfrak{P}}/_{\mathfrak{P}} \ : \ {}^{\mathcal{O}_P}/_{P}\right]$$

και ως *δείκτη διακλάδωσης* (ramification index) των $\mathfrak{P}$ και P (συμβ. $e(\mathfrak{P}/P)$) τον ακέραιο e εκείνο που $P\mathcal{O}_\mathfrak{P} = \mathfrak{P}^e$. Αν $e(\mathfrak{P}/P) = 1$, τότε λέμε ότι ο $\mathfrak{P}$ *αδρανεί* (inerts) πάνω από τον P, αλλιώς λέμε ότι *διακλαδώνεται* (ramifies) πάνω από τον P.

Αν δεν υπάρχει κίνδυνος σύγχυσης, θα γράφουμε απλά f και e αντίστοιχα. Ακόμα, είναι προφανές ότι και τα δύο παραπάνω μεγέθη είναι πάντα ≥ 1. Επίσης μια άμεση συνέπεια των ορισμών είναι ότι για κάθε $a \in F$ έχουμε ότι

$$\operatorname{ord}_\mathfrak{P}(a) = e \cdot \operatorname{ord}_P(a). \tag{3.2}$$

Ας δούμε τώρα την πολλαπλασιατική ιδιότητα των παραπάνω μεγεθών.

Προταση 3.1.6. *Αν $K \leq L \leq M$ και $P \in \mathbb{P}_K$, $\mathfrak{P} \in \mathbb{P}_L$ και $\mathfrak{p} \in \mathbb{P}_M$ τέτοια ώστε $\mathfrak{p} \mid \mathfrak{P} \mid P$, τότε*

$$e(\mathfrak{p}/P) = e(\mathfrak{p}/\mathfrak{P}) \cdot e(\mathfrak{P}/P) \quad \text{και} \quad f(\mathfrak{p}/P) = f(\mathfrak{p}/\mathfrak{P}) \cdot f(\mathfrak{P}/P).$$

Αποδειξη. Άμεσο από τους ορισμούς. ♢

Μέχρι στιγμής όμως δεν είδαμε ούτε αν υπάρχουν $\mathfrak{P}$ και P που να ικανοποιούν τη σχέση $\mathfrak{P} \mid P$, ούτε πόσα είναι αυτά αν εμείς σταθεροποιήσουμε το ένα από τα δύο. Η επόμενη πρόταση απαντάει (εν μέρει) σε αυτό το ερώτημα.

[3] Αυτό γίνεται από το θεώρημα 1.2.6(α′).

ΠΡΟΤΑΣΗ 3.1.7. *Αν $F \leq L$, τότε*

(α′) για κάθε $\mathfrak{P} \in \mathbb{P}_L$ υπάρχει κάποιο μοναδικό $P \in \mathbb{P}_F$ τέτοιο ώστε $\mathfrak{P} \mid P$ και

(β′) για κάθε $P \in \mathbb{P}_F$ υπάρχει τουλάχιστον ένα, αλλά πεπερασμένα το πλήθος στοιχεία του $\mathbb{P}_L$ που βρίσκονται πάνω από αυτό.

ΑΠΟΔΕΙΞΗ. **α′)** Άμεσο από τον ορισμό 3.1.3.

β′) Από την πρόταση 2.3.4 υπάρχει κάποιο $x \in F \setminus K$, τέτοιο ώστε ο P να είναι η μοναδική του ρίζα. Θα δείξουμε ότι

$$\mathfrak{P} \mid P \iff \operatorname{ord}_{\mathfrak{P}}(x) > 0. \tag{3.3}$$

Πράγματι, από την (3.2) αν $\mathfrak{P} \mid P$, τότε $\operatorname{ord}_{\mathfrak{P}}(x) = e \operatorname{ord}_P(x) > 0$. Αντίστροφα, αν $\operatorname{ord}_{\mathfrak{P}}(x) > 0$ και Q ο μοναδικός πρώτος του F/K με $\mathfrak{P} \mid Q$, τότε από την (3.2) θα ισχύει ότι $\operatorname{ord}_Q(x) > 0$. Όμως, το x έχει ως μοναδική ρίζα στο F/K τον P, άρα $P = Q$.

Έτσι, η (3.3) μας λέει ότι ο $\mathfrak{P}$ βρίσκεται πάνω από τον P ανν είναι ρίζα του x στο L/E. Όμως, το x στο L/E έχει το πολύ τουλάχιστον μία, αλλά πεπερασμένες το πλήθος ρίζες στο L/E. ♢

Σύμφωνα με την παραπάνω πρόταση, έχει νόημα να μιλάμε για το σύνολο των πρώτων του L/E που βρίσκονται πάνω από έναν πρώτο του F/K.

Επόμενος στόχος μας είναι να δείξουμε ότι αν πολλαπλασιάσουμε τον δείκτη διακλάδωσης με τον σχετικό βαθμό για κάθε $\mathfrak{P} \in \mathbb{P}_L$ που βρίσκεται πάνω από το $P \in \mathbb{P}_F$ και προσθέσουμε τα παραπάνω γινόμενα, το αποτέλεσμα που θα πάρουμε είναι $[L : F]$. Ξεκινάμε με μια απλή πρόταση.

ΠΡΟΤΑΣΗ 3.1.8. *Αν $P \in \mathbb{P}_F$, $\mathfrak{P} \in \mathbb{P}_L$ και $\mathfrak{P} \mid P$, τότε $ef \leq [L : F]$.*

ΑΠΟΔΕΙΞΗ. Εφόσον $f = \left[{}^{\mathcal{O}_{\mathfrak{P}}}/_{\mathfrak{P}} \,:\, {}^{\mathcal{O}_P}/_P\right]$, έχουμε ότι θα υπάρχουν κάποια $\omega_1, \ldots, \omega_f \in \mathcal{O}_{\mathfrak{P}}$ τέτοια ώστε τα $\bar{\omega_1}, \ldots, \bar{\omega_f} \in {}^{\mathcal{O}_{\mathfrak{P}}}/_{\mathfrak{P}}$ να είναι γραμμικά ανεξάρτητα πάνω από το ${}^{\mathcal{O}_P}/_P$. Ακόμα, από το θεώρημα 1.2.6(α′) θα υπάρχει κάποιο $T \in L$ τέτοιο ώστε $\mathfrak{P} = T\mathcal{O}_{\mathfrak{P}}$. Θα δείξουμε ότι τα ($ef$ το πλήθος) $\omega_i T^j$, με $1 \leq i \leq f$ και $0 \leq j < e$, είναι γραμμικά ανεξάρτητα πάνω από το F. Έστω λοιπόν ότι

$$\sum_{j=0}^{e-1} \sum_{i=1}^{f} a_{ij} \omega_i T^j = 0$$

ένας μη τετριμμένος γραμμικός συνδυασμός με $a_{ij} \in F$. Επίσης, χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι $a_{ij} \in \mathcal{O}_P$ (γιατί το σώμα κλασμάτων του $\mathcal{O}_P$ είναι το F) και ότι τουλάχιστον κάποιο από αυτά δεν ανήκει στο P (πολλαπλασιάζοντας όσες φορές χρειαστεί την σχέση με t^{-1}, όπου $t \in F$ τέτοιο ώστε $P = t\mathcal{O}_P$). Θεωρούμε τώρα τα στοιχεία

$$A_j := \sum_{i=1}^{f} a_{ij} \omega_i$$

για $0 \leq j < e$. Αν λοιπόν για κάποιο j υπάρχει κάποιο $a_{ij} \notin P$, τότε $\bar{a_{ij}} \neq \bar{0}$ και άρα (από τη γραμμική ανεξαρτησία των $\bar{\omega_i}$) έχουμε ότι $\bar{A_j} \neq \bar{0}$, δηλαδή $A_j \notin \mathfrak{P}$, δηλαδή $A_j \in \mathcal{O}_{\mathfrak{P}}^*$. Αντίθετα, αν $a_{ij} \in P$ για κάθε i, τότε $t \mid A_j$ και άρα, μιας που $t = T^e$ από την απόδειξη του λήμματος 3.1.4(β′), $\mathrm{ord}_{\mathfrak{P}}(A_j) \geq e$.

Έτσι, από την ισχυρή τριγωνική ανισότητα (αφού για όλα τα j που υπάρχει κάποιο $a_{ij} \notin P$ τα $\mathrm{ord}_{\mathfrak{P}} A_j T^j$ είναι διαφορετικό ανα δύο, αλλά πάντα $< e$ και για εκείνα που δεν ισχύει αυτό τα $\mathrm{ord}_{\mathfrak{P}} A_j t^j$ είναι $\geq e$) θα έχουμε ότι $\mathrm{ord}_{\mathfrak{P}} \left(\sum_{j=0}^{e-1} A_j T^j \right) < e$. Όμως $\sum_{j=0}^{e-1} A_j T^j = 0$ και $\mathrm{ord}_{\mathfrak{P}}(0) = \infty$, άτοπο. ♢

Στη συνέχεια, θα δούμε τον ισχυρισμό μας για την ειδική περίπτωση, όπου η επέκταση L/F είναι διαχωρίσιμη.

Πρόταση 3.1.9. *Αν η επέκταση L/F είναι διαχωρίσιμη, τότε, για κάθε $P \in \mathbb{P}_F$, αν $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_k\}$ είναι το σύνολο των πρώτων του L που βρίσκονται πάνω από το P, $e_i := e(\mathfrak{P}_i/P)$ και $f_i := f(\mathfrak{P}_i/P)$, τότε*

$$\sum_{i=1}^{k} e_i f_i = [L : F].$$

Απόδειξη. Η πρόταση ισχύει γενικά για δακτυλίους Dedekind, για την απόδειξη δες [Neu, κεφ. I, π. (8.2)]. ♢

Ας δούμε τώρα τι συμβαίνει στην περίπτωση που η επέκταση L/F είναι πλήρως μη διαχωρίσιμη.

Πρόταση 3.1.10. *Έστω ότι L/F πλήρως μη διαχωρίσιμη επέκταση βαθμού p και $p = \mathrm{char}\, F$. Αν $F = L^p$ και $P \in \mathbb{P}_F$, τότε υπάρχει μοναδικός $\mathfrak{P} \in \mathbb{P}_L$ τέτοιος ώστε $\mathfrak{P} \mid P$. Ακόμα $e = p$ και $f = 1$, οπότε $ef = [L : F]$.*

Απόδειξη. Θέτουμε $R := \{r \in L \mid r^p \in \mathcal{O}_P\}$ και $\mathfrak{P} := \{r \in L \mid r^p \in P\}$. Δεδομένης της ταυτότητας $(a \pm b)^p = a^p \pm b^p$ σε σώματα χαρακτηριστικής p, εύκολα βλέπουμε ότι το R είναι δακτύλιος, το $\mathfrak{P}$ πρώτο ιδεώδες του και ότι $\mathfrak{P} \cap \mathcal{O}_P = P$. Θα δείξουμε ότι ο R είναι δακτύλιος αποτίμησης του L/E.

Έστω t γεννήτορας του P. Εφόσον $L^p = F$ υπάρχει κάποιο $T \in L$ τέτοιο ώστε $T^p = t$. Προφανώς, $T \in \mathfrak{P}$. Έστω $x \in L$, οπότε $x^p \in F$, άρα $x^p = ut^s$, όπου $u \in \mathcal{O}_P^*$ και $s \in \mathbb{Z}$. Θα ισχύει ότι $(x/T^s)^p = u$, δηλαδή $x/T^s \in R$ και μιας που $u^{-1} \in \mathcal{O}_P$ και $u^{-1} = (T^s/x)^p$ θα έχουμε και ότι $T^s/x \in R$. Έτσι, καταλήγουμε ότι κάθε στοιχείο του L είναι γινόμενο κάποιας δύναμης του T με κάποιο στοιχείο του R^*. Εύκολα λοιπόν καταλήγουμε ότι $\mathfrak{P} = TR$ και ότι πράγματι το R είναι δακτύλιος αποτίμησης.

Δείξαμε λοιπόν ότι $\mathfrak{P} \in \mathbb{P}_L$ και $\mathfrak{P} \mid P$. Έστω $\mathfrak{P}'$ ένας άλλος πρώτος του L που βρίσκεται πάνω από το P. Αν $x \in \mathcal{O}_{\mathfrak{P}'}$, τότε $x^p \in F \cap \mathcal{O}_P$, άρα

$x \in R$, δηλαδή $\mathcal{O}_{\mathfrak{P}'} \subseteq R$. Έτσι από το 1.2.10(γ′) θα ισχύει ότι $\mathcal{O}_{\mathfrak{P}'} = R$, άρα $\mathfrak{P} = \mathfrak{P}'$.

Μας μένει λοιπόν να δείξουμε τους ισχυρισμούς για τα e και f. Πράγματι από την (3.2), μιας που $\mathrm{ord}_{\mathfrak{P}}(t) = p$, θα έχουμε ότι $e = p$ και από την 3.1.8 θα έχουμε ότι $ef \leq p$, άρα $f = 1$. ♢

Ας δούμε τώρα κάποιες γενικές αλγεβρικές προτάσεις που θα μας βοηθήσουν αργότερα. Υπενθυμίζουμε ότι ένα σώμα λέγεται *τέλειο*, αν κάθε αλγεβρική του επέκταση είναι διαχωρίσιμη ή ισοδύναμα αν κάθε ανάγωγο πολυώνυμό του είναι διαχωρίσιμο.

Λημμα 3.1.11. *Αν το F είναι σώμα με $\mathrm{char}\, F = p > 0$, τότε το F είναι τέλειο ανν $F = F^p$.*

Απόδειξη. Θα χρησιμοποιήσουμε το γεγονός ότι αν $\mathrm{char}\, F = p > 0$ και $f \in F[X]$ ανάγωγο, τότε f μη διαχωρίσιμο ανν $f \in F[X^p]$ (δες [Ash, π. 3.4.3(2)]).

($\Rightarrow$) Αφού F τέλειο, θα έχουμε ότι για κάθε $\alpha \in F$ το $X^p - \alpha$ δεν θα είναι ανάγωγο. Όμως $X^p - \alpha = (X - \sqrt[p]{\alpha})^p$ και άρα πρέπει $X - \sqrt[p]{\alpha} \in F[X]$, δηλαδή $\sqrt[p]{\alpha} \in F$. Έτσι $F \subset F^p$ και άρα $F = F^p$.

($\Leftarrow$) Αν $f \in F[X^p]$, τότε $f \in F^p[X^p]$ και άρα το f είναι της μορφής

$$\begin{aligned} f(X) &= \alpha_0^p + \alpha_1^p X^p + \cdots + \alpha_n^p X^p n \\ &= (\alpha_0 + \alpha_1 X + \cdots + \alpha_n X^n)^p, \end{aligned}$$

άρα f όχι ανάγωγο. ♢

Προταση 3.1.12. *Αν το K είναι τέλειο σώμα χαρακτηριστικής $p > 0$, τότε $[F : F^p] = p$.*

Απόδειξη. Έστω $x \in F \setminus K$, τότε $[F : K(x)], [F : K(x^p)] < \infty$. Κατ᾽ αρχάς, παρατηρούμε ότι $K(x)^p = K^p(x^p) = K(x^p)$. Ακόμα, είναι εμφανές ότι το σύνολο $\{1, x, x^2, \ldots, x^{p-1}\}$ είναι μια $K(x^p)$-βάση του $K(x)$ έτσι έχουμε ότι

$$[K(x) : K(x^p)] = p. \tag{3.4}$$

Στη συνέχεια, αν πάρουμε $\{\omega_1, \ldots, \omega_m\}$ μια $K(x)$-βάση του F βλέπουμε εύκολα ότι το σύνολο $\{\omega_1^p, \ldots, \omega_m^p\}$ είναι μια $K(x)^p$-βάση του F^p, έτσι συνολικά θα έχουμε ότι

$$[F : K(x)] = [F^p : K(x^p)]. \tag{3.5}$$

Ακόμα, παρατηρούμε ότι

$$[F : K(x^p)] = [F : K(x)] \cdot [K(x) : K(x^p)] \text{ και} \tag{3.6}$$

$$[F : K(x^p)] = [F : F^p] \cdot [F^p : K(x^p)], \tag{3.7}$$

έτσι από τις (3.4), (3.5), (3.6) και (3.7) καταλήγουμε στο ζητούμενο. ♢

Πορισμα 3.1.13. *Αν το K είναι τέλειο σώμα χαρακτηριστικής $p > 0$ και η επάκταση L/F είναι πλήρως μη διαχωρίσιμη, βαθμού p, τότε $E = K$ και $L^p = F$.*

Απόδειξη. Έστω $a \in E$. Εξ ορισμού το a είναι αλγεβρικό πάνω από το K και εφόσον η επέκταση L/F είναι πλήρως μη διαχωρίσιμη βαθμού p έχουμε ότι $a^p \in F$ και είναι αλγεβρικό πάνω από το K, οπότε $a^p \in K$. Έτσι, από το λήμμα 3.1.11 θα έχουμε και $a \in K$, δηλαδή $E \subseteq K$, οπότε τελικά $E = K$.

Εφόσον η επέκταση E/K είναι αλγεβρική, το E θα είναι και αυτό τέλειο. Έτσι από την πρόταση 3.1.12 θα έχουμε ότι $[L : L^p] = p$. Όμως, αφού η επέκταση L/F είναι πλήρως μη διαχωρίσιμη θα ισχύει ότι $L^p \subseteq F$ και έτσι συνολικά $[F : L^p] = 1$, οπότε $L^p = F$. ♢

Πρόταση 3.1.14. *Έστω K τέλειο σώμα και $F \leq M \leq L$, με M τη μέγιστη διαχωρίσιμη επέκταση του F. Τότε το γένος του M είναι ίσο με το γένος του L. Ακόμα, για κάθε $\mathfrak{p} \in \mathbb{P}_M$ υπάρχει μοναδικό $\mathfrak{P} \in \mathbb{P}_L$ τέτοιο ώστε $\mathfrak{P} \mid \mathfrak{p}$ και ακόμα $e(\mathfrak{P}/\mathfrak{p}) = [L : M]$ και $f(\mathfrak{P}/\mathfrak{p}) = 1$.*

Απόδειξη. Αν N το σώμα σταθερών του M, τότε το N είναι τέλειο ως αλγεβρική επέκταση του K. Εφόσον τώρα η επέκταση είναι πλήρως μη διαχωρίσιμη από στοιχειώδη άλγεβρα, θα υπάρχουν σώματα $K_0, K_1, \ldots, K_n$ τετοια ώστε

$$F \subseteq M = K_0 \subset K_1 \subset \cdots \subset K_{n-1} \subset K_n = L$$

και για κάθε $i \leq 1$ να ισχύει ότι η επέκταση K_i/K_{i-1} είναι πλήρως μη διαχωρίσιμη βαθμού p. Με επαγωγή και το πόρισμα 3.1.13 καταλήγουμε ότι $K_{i-1} = K_i^p$. Έτσι οι απεικονίσεις

$$\phi_i : \begin{array}{ccc} K_i & \to & K_{i-1} \\ \alpha & \mapsto & \alpha^p \end{array}$$

είναι ισομορφισμοί, δηλαδή όλα τα K_i θα έχουν το ίδιο γένος.

Όλοι οι υπόλοιποι ισχυρισμοί έπονται άμεσα με επαγωγή κάνοντας χρήση του πορίσματος 3.1.13, της πρότασης 3.1.10 και της πρότασης 3.1.6. ♢

Πλέον είμαστε σε θέση να δείξουμε τον ισχυρισμό που κάναμε στη σελίδα 30.

Θεώρημα 3.1.15 (Θεμελιώδης Ταυτότητα). *Έστω F/K σώμα συναρτήσεων, K τέλειο και L σώμα τέτοιο ώστε $[L : F] = n \leq \infty$. Αν $P \in \mathbb{P}_F$, $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_m\} \subseteq \mathbb{P}_L$ οι πρώτοι του L που βρίσκονται πάνω από τον P, $e_i := e(\mathfrak{P}_i/P)$ και $f_i := f(\mathfrak{P}_i/P)$, τότε*

$$\sum_{i=1}^{m} e_i f_i = n.$$

Απόδειξη. Έστω M η μέγιστη (μέσα στο L) διαχωρίσιμη επέκταση του F. Για κάθε i θέτουμε $\mathfrak{p}_i$ τον πρώτο του M που βρίσκεται κάτω από τον $\mathfrak{P}_i$ και ακόμα θέτουμε $e_i' := e(\mathfrak{p}_i/P)$ και $f_i' := f(\mathfrak{p}_i/P)$. Από την

πρόταση 3.1.9 ισχύει ότι

$$\sum_{i=1}^{m} e'_i f'_i = [M : F].$$

Ακόμα από τις προτάσεις 3.1.6 και 3.1.14 θα ισχύει ότι $e_i = e'_i[L : M]$ και $f_i = f'_i$. Έτσι το παραπάνω άθροισμα δίνει

$$\sum_{i=1}^{m} e_i f_i = [L : M] \cdot [M : F] = n. \qquad \diamondsuit$$

Η θεμελιώδης ταυτότητα αποδεικνύεται και χωρίς να υποθέσουμε ότι το K είναι τέλειο με χρήση ιδιοτήτων των σωμάτων συναρτήσεων. Παρ' όλα αυτά, εμείς εδώ το δείξαμε με γενικές μεθόδους που θα μπορούσαν να χρησιμοποιηθούν σε οποιοδήποτε δακτύλιο Dedekind. Αυτή η οδός πέραν της γενικότητας της μεθόδου μας έδωσε και μερικά ενδιαφέροντα ενδιάμεσα αποτελέσματα, όπως την πρόταση 3.1.14. Για την ειδική απόδειξη παραπέμπουμε στο [Sti, §III.1].

Στη συνέχεια, θα δούμε κάποιες σημαντικές απεικονίσεις και μερικές απλές ιδιότητές τους. Τονίζουμε ότι οι παρακάτω έννοιες είναι καλά ορισμένες χάρη στην πρόταση 3.1.7.

Ορισμος 3.1.16. Αν $F \leq L$, τότε η απεικόνηση $N_{L/F} : \mathcal{D}_L \to \mathcal{D}_F$ με

$$N_{L/F}(\mathfrak{P}) = f(\mathfrak{P}/P)P,$$

όπου $\mathfrak{P} \in \mathbb{P}_L$ και P ο (μοναδικός) πρώτος του F που βρίσκεται κάτω από τον $\mathfrak{P}$, επεκτεινόμενη γραμμικά σε όλο το $\mathcal{D}_L$, ονομάζεται *νόρμα* ή *στάθμη* (norm).

Επίσης, η απεικόνιση $i_{L/F} : \mathcal{D}_F \to \mathcal{D}_L$ με

$$i_{L/F}(P) = \sum_{\mathfrak{P}|P} e(\mathfrak{P}/P)\mathfrak{P},$$

όπου $P \in \mathbb{P}_F$, επεκτεινόμενη γραμμικά σε όλο το $\mathcal{D}_F$, ονομάζεται *συνόρμα* (conorm).

Είναι άμεσο από τους ορισμούς ότι η νόρμα είναι επιμορφισμός και η συνόρμα μονομορφισμός. Ακόμα από τον ορισμό της νόρμας και της συνόρμας και την θεμελιώδη ταυτότητα εύκολα βλέπουμε ότι

$$(N_{L/F} \circ i_{L/F})(D) = [L : F] \cdot D. \tag{3.8}$$

Ακόμα από τον ορισμό της νόρμας και της συνόρμας και την πρόταση 3.1.6 έχουμε ότι αν $F \leq M \leq L$, $A \in \mathcal{D}_F$ και $\mathfrak{A} \in \mathcal{D}_L$, τότε

$$i_{L/F}(\mathfrak{A}) = i_{L/M}(i_{M/F}(\mathfrak{A})) \text{ και} \tag{3.9}$$

$$N_{L/F}(A) = N_{L/M}(N_{M/F}(A)). \tag{3.10}$$

Η επόμενη πρόταση μας δείχνει πώς σχετίζονται οι βαθμοί των προεικόνων με εκείνους των εικόνων των εν λόγω απεικονίσεων.

ΠΡΟΤΑΣΗ 3.1.17. *Αν* $\mathfrak{A} \in \mathcal{D}_L$ *και* $A \in \mathcal{D}_F$, *τότε*

$$\deg_F(N_{L/F}(\mathfrak{A})) = [E:K]\deg_L \mathfrak{A} \quad \textit{και}$$
$$\deg_L(i_{L/F}(A)) = \frac{[L:F]}{[E:K]}\deg_F A.$$

ΑΠΟΔΕΙΞΗ. Αρκεί να δείξουμε τους ισχυρισμούς μας για την περίπτωση που οι διαιρέτες $\mathfrak{A}$ και A είναι κάποιοι πρώτοι $\mathfrak{P}$ και P αντίστοιχα.

Έτσι παρατηρούμε κατ᾽ αρχάς ότι

$$\left[\mathcal{O}_{\mathfrak{P}}/_{\mathfrak{p}} : K\right] = \left[\mathcal{O}_{\mathfrak{P}}/_{\mathfrak{p}} : E\right]\cdot[E:K] = \left[\mathcal{O}_{\mathfrak{P}}/_{\mathfrak{p}} : \mathcal{O}_P/_P\right]\cdot\left[\mathcal{O}_P/_P : K\right],$$

δηλαδή

$$[E:K]\deg_L \mathfrak{P} = f(\mathfrak{P}/P)\deg_F P, \tag{3.11}$$

απ᾽ όπου έπεται άμεσα η πρώτη προς απόδειξη εξίσωση.

Στη συνέχεια παρατηρούμε ότι

$$\begin{aligned}\deg_L(i_{L/F}(P)) &= \sum_{\mathfrak{P}|P} e(\mathfrak{P}/P)\deg_L \mathfrak{P}\\ &= \frac{1}{[E:K]}\sum_{\mathfrak{P}|P} e(\mathfrak{P}/P)f(\mathfrak{P}/P)\deg_F P\\ &= \frac{[L:F]}{[E:K]}\deg_F P,\end{aligned}$$

όπου η πρώτη εξίσωση έπεται από τον ορισμό 3.1.16, η δεύτερη από την (3.11) και η τρίτη από το θεώρημα 3.1.15. ♢

Κλείνοντας την παράγραφο αυτή θα δούμε μια πρόταση σχετικά με τη συμπεριφορά της συνόρμας στα $\mathcal{P}_F$ και $\mathcal{P}_L$, τις ομάδες των κύριων διαιρετών.

ΠΡΟΤΑΣΗ 3.1.18. *Αν* $a \in F^*$, *τότε*[4] $i_{L/F}((a)_F) = (a)_L$.

ΑΠΟΔΕΙΞΗ. Έχουμε ότι

$$\begin{aligned}i_{L/F}((a)_F) &= i_{L/F}\left(\sum_{P\in\mathbb{P}_F}\operatorname{ord}_P(a)P\right)\\ &= \sum_{p\in\mathbb{P}_F}\operatorname{ord}_P(a)\sum_{\mathfrak{P}|P} e(\mathfrak{P}/P)\mathfrak{P}\\ &= \sum_{\mathfrak{P}\in\mathbb{P}_L} e(\mathfrak{P}/P)\operatorname{ord}_P(a)\mathfrak{P}\\ &= \sum_{\mathfrak{P}\in\mathbb{P}_L}\operatorname{ord}_{\mathfrak{P}}(a)\mathfrak{P} =: (a)_L.\end{aligned}$$ ♢

[4]Εδώ εννοούμε $(a)_F := \sum_{P\in\mathbb{P}_F}\operatorname{ord}_P(a)P$ και $(a)_L := \sum_{\mathfrak{P}\in\mathbb{P}_L}\operatorname{ord}_{\mathfrak{P}}(a)\mathfrak{P}$.

Από την τελευταία πρόταση παρατηρούμε ότι η συνόρμα επάγει φυσιολογικά έναν ομομορφισμό $\mathcal{C}_F \to \mathcal{C}_L$, τον οποίο επίσης θα συμβολίζουμε με $i_{L/F}$.

3.2. Επεκτάσεις σταθερού σώματος

Στην παράγραφο αυτή θα ασχοληθούμε με επεκτάσεις σταθερού σώματος, όπως αυτές ορίστηκαν στον ορισμό 3.1.1. Οι επεκτάσεις αυτές είναι ιδιαίτερα σημαντικές και βάσει της θεωρίας αυτής της παραγράφου, θα αποδείξουμε το θεώρημα των πρώτων αριθμών στα σώματα συναρτήσεων στην ασθενή του μορφή. Τέλος, στην παράγραφο αυτή θα κάνουμε όσες παραδοχές κάναμε στην προηγούμενη παράγραφο και επίσης θα θεωρούμε ότι το σώμα K είναι τέλειο, χωρίς να γίνεται ιδιαίτερη αναφορά.

Ας ξεκινήσουμε με κάποιες βασικές ιδιότητες των επεκτάσεων σταθερού σώματος.

ΠΡΟΤΑΣΗ 3.2.1. *Ισχύει ότι* $[FE : F] = [E : K]$ *και ότι κάθε* K*-βάση του* E *είναι και* F*-βάση του* FE*.*

ΑΠΟΔΕΙΞΗ. Αν η επέκταση E/K είναι Galois, τότε μιας που E/K πεπερασμένη και $E \cap F = K$ (αφού το K είναι το σώμα σταθερών του F), θα έχουμε ότι η επέκταση FE/F είναι Galois και $\mathrm{Gal}(FE/F) \cong \mathrm{Gal}(E/K)$, από το [Ash, θ. 6.2.2]. Έτσι, $|\mathrm{Gal}(FE/F)| = |\mathrm{Gal}(E/K)|$, δηλαδή $[FE : F] = [E : K]$.

Έστω ότι η επέκταση E/K είναι διαχωρίσιμη. Θέτουμε[5] ως E_1 την ελάχιστη επέκταση του K στο $\bar{E}$, που είναι Galois πάνω από το K. Τότε, δεδομένου και του προηγούμενου, έχουμε ότι

$$[E_1 : K] = [FE_1 : F] = [FE_1 : FE][FE : F] \quad \text{και}$$
$$[E_1 : K] = [E_1 : E][E : K],$$

δηλαδή συνολικά

$$[FE_1 : FE][FE : F] = [E_1 : E][E : K]. \tag{3.12}$$

Όμως προφανώς $[FE_1 : FE] \leq [E_1 : E]$ και $[FE : F] \leq [E : K]$, έτσι από την (3.12) παίρνουμε ότι $[FE_1 : FE] = [E_1 : E]$ και $[FE : F] = [E : K]$.

Έστω τώρα ότι $\{\alpha_1, \ldots, \alpha_n\}$ μια K-βάση του E. Τότε κάθε στοιχείο e του E θα γράφεται ως $e = \sum_{i=1}^{n} k_i \alpha_i$ με $k_i \in K$, άρα κάθε στοιχείο r του FE γράφεται ως $r = \sum_{j=1}^{m} f_j e_j$ με $f_j \in F$ και $e_j \in E$, οπότε

$$r = \sum_{j=1}^{m} f_j e_j = \sum_{j=1}^{m} f_j \sum_{i=1}^{n} k_{ij} \alpha_i = \sum_{i=1}^{n} \left(\sum_{j=1}^{m} f_j k_{ij} \right) \alpha_i = \sum_{i=1}^{n} f_i' \alpha_i.$$

Έτσι βλέπουμε ότι, μιας που $f_i' \in F$, το $\{\alpha_1, \ldots, \alpha_n\}$ παράγει το FE ως F-διανυσματικό χώρο και από τα προηγούμενα $[E : K] = [FE : F]$, άρα θα έχουμε ότι το $\{\alpha_1, \ldots, \alpha_n\}$ είναι και F-βάση του FE. ♢

[5] Η ύπαρξη τέτοιου E_1 είναι προφανής.

Το παρακάτω λήμμα θεωρίας σωμάτων θα μας φανεί χρήσιμο σε διάφορες περιπτώσεις[6].

ΛΗΜΜΑ 3.2.2. *Έστω L/F πεπερασμένη επέκταση σωμάτων.*

(α΄) Αν το K είναι υπόσωμα του F, αλγεβρικά κλειστό στο F και το $\beta \in L$ είναι αλγεβρικό πάνω από το K, τότε $\mathrm{tr}_{L/F}(\beta) \in K$.

(β΄) Αν ο O είναι υποδακτύλιος του F, ακέραια κλειστός στο F και το $b \in L$ είναι ακέραιο πάνω από τον O, τότε $\mathrm{tr}_{L/F}(b) \in O$.

ΑΠΟΔΕΙΞΗ. Αν $x_1, \ldots, x_n$ οι ρίζες του $\mathrm{Irr}(\beta, F)$ στην αλγεβρική θήκη του F, τότε προφανώς $\mathrm{Irr}(\beta, F) \mid \mathrm{Irr}(\beta, K)$ στο $F[X]$, έτσι τα $x_1, \ldots x_n$ είναι αλγεβρικά πάνω από το K. Άρα και $\sum_{i=1}^{n} x_i$ αλγεβρικό πάνω από το K. Όμως από το [Ash, π. 7.3.5] βλέπουμε ότι για κάποιο $k \in \mathbb{Z}$ έχουμε ότι

$$\mathrm{tr}_{L/F}(\beta) = k \sum_{i=1}^{n} x_i,$$

δηλαδή συνολικά $\mathrm{tr}_{L/F}(\beta)$ αλγεβρικό πάνω από το K και μιας που (γενικά) $\mathrm{tr}_{L/F}(\beta) \in F$ και K αλγεβρικά κλειστό πάνω από το F καταλήγουμε ότι $\mathrm{tr}_{L/F}(\beta) \in K$. Ομοίως αποδεικνύεται και η περίπτωση (β΄). ♢

Η επόμενη πρόταση μας δείχνει ποιό ακριβώς είναι το σώμα σταθερών του FE.

ΠΡΟΤΑΣΗ 3.2.3. *Το E είναι το σώμα σταθερών του FE.*

ΑΠΟΔΕΙΞΗ. Αρκεί να δείξουμε ότι κάθε στοιχείο του FE που είναι αλγεβρικό πάνω από το E ανήκει στο E.

Έστω[7] $\{\alpha_1, \ldots, \alpha_n\}$ μια K-βάση του E και $\beta \in FE$ αλγεβρικό πάνω από το E. Από την πρόταση 3.2.1 υπάρχουν μοναδικά $x_i \in F$ τέτοια ώστε

$$\beta = \sum_{i=1}^{n} x_i \alpha_i. \tag{3.13}$$

Έτσι για κάθε $j = 1, \ldots, n$ θα έχουμε ότι

$$\mathrm{tr}_{FE/F}(\alpha_j \beta) = \mathrm{tr}_{FE/F}\left(\sum_{i=1}^{n} \alpha_j \alpha_i x_i \right),$$

και αφού το $\mathrm{tr}_{FE/F}$ είναι F-γραμμική απεικόνιση θα έχουμε ότι

$$\mathrm{tr}_{FE/F}(\alpha_j \beta) = \sum_{i=1}^{n} \mathrm{tr}_{FE/F}(\alpha_j \alpha_i) x_i.$$

Εφόσον τώρα το β είναι αλγεβρικό πάνω από το E και E/K αλγεβρική, το β θα είναι αλγεβρικό πάνω από το K, άρα και $\alpha_j \beta$ αλγεβρικό πάνω από το K, δηλαδή από το λήμμα 3.2.2(α΄) θα έχουμε ότι $\mathrm{tr}_{FE/F}(\alpha_j \beta) \in K$.

[6] Το λήμμα αυτό δεν απαιτεί την ισότητα $L = EF$, ισχύει γενικότερα.

[7] Μια τέτοια βάση υπάρχει αφού $[E : K] = n < \infty$.

Ακόμα, $\alpha_j\alpha_i$ αλγεβρικό πάνω από το K, άρα και $\mathrm{tr}_{FE/F}(\alpha_j\alpha_i) \in K$. Έτσι μαζεύοντας τα παραπάνω, έχουμε το παρακάτω $n \times n$ γραμμικό σύστημα επί του F

$$\begin{cases} \mathrm{tr}_{FE/F}(\alpha_1\beta) & = & \mathrm{tr}_{FE/F}(\alpha_1\alpha_1)x_1 & + & \cdots & + & \mathrm{tr}_{FE/F}(\alpha_1\alpha_n)x_n \\ \vdots & & \vdots & & \ddots & & \vdots \\ \mathrm{tr}_{FE/F}(\alpha_n\beta) & = & \mathrm{tr}_{FE/F}(\alpha_n\alpha_1)x_1 & + & \cdots & + & \mathrm{tr}_{FE/F}(\alpha_n\alpha_n)x_n \end{cases}$$

και παρατηρούμε ότι από [Neu, σελ. 11], μιας που $\det(\mathrm{tr}_{FE/F}(\alpha_i\alpha_j) = \det(\mathrm{tr}_{E/K}(\alpha_i\alpha_j)$ από την πρόταση 3.2.1, $D := \det(\mathrm{tr}_{FE/F}(\alpha_i\alpha_j) \neq 0$. Από τον κανόνα του Cramer (δες [Ανδ, σελ. 165]), θα έχουμε ότι $x_i \in K$ για κάθε $i = 1, \ldots, n$. Έτσι η (3.13), σε συνδυασμό με το γεγονός ότι $\{\alpha_1, \ldots, \alpha_n\}$ μια K-βάση του E, μας δίνει ότι $\beta \in E$. ♢

Ας δούμε τώρα ένα ακόμα χρήσιμο λήμμα.

Λημμα 3.2.4. *Έστω $\{\alpha_1, \ldots, \alpha_n\}$ μια K-βάση του E, $P \in \mathbb{P}_F$ και $\mathcal{O}_P$ ο αντίστοιχος δακτύλιος αποτίμησης. Αν $\mathcal{R}_P$ η ακέραια θήκη του $\mathcal{O}_P$ στο FE, τότε το $\{\alpha_1, \ldots, \alpha_n\}$ είναι μια ακέραια βάση του $\mathcal{R}_P$ πάνω από το $\mathcal{O}_P$.*

Απόδειξη. Εφόσον $K \subset \mathcal{O}_P$ εξ ορισμού και κάθε α_i αλγεβρικό πάνω από το K, τότε κάθε α_i είναι ακέραιο πάνω από τον $\mathcal{O}_P$.

Έστω τώρα $\beta \in \mathcal{R}_P$. Από την πρόταση 3.2.1 υπάρχουν $x_i \in F$ τέτοια ώστε

$$\beta = \sum_{i=1}^{n} x_i\alpha_i.$$

Έτσι, ομοίως με την αποδειξη της 3.2.3 για κάθε $j = 1, \ldots, n$ έχουμε ότι

$$\mathrm{tr}_{FE/F}(\alpha_j\beta) = \sum_{i=1}^{n} \mathrm{tr}_{FE/F}(\alpha_j\alpha_i)x_i$$

και με χρήση του λήμματος 3.2.2(β′) και πανομοιότυπων με εκείνους της απόδειξης της πρότασης 3.2.3 συλλογισμών καταλήγουμε ότι $x_i \in \mathcal{O}_P$. Επομένως, το $\{\alpha_1, \ldots, \alpha_n\}$ παράγει το $\mathcal{R}_P$ πάνω από το $\mathcal{O}_P$.

Ακόμα, αφού το $\{\alpha_1, \ldots, \alpha_n\}$ είναι F-βάση του FE, τα $\alpha_1, \ldots, \alpha_n$ θα είναι γραμμικά ανεξάρτητα πάνω από το $\mathcal{O}_P$, άρα θα είναι μια ελεύθερη βάση του $\mathcal{R}_P$ ως $\mathcal{O}_P$-διανυσματική περιοχή[8]. ♢

Το επόμενο μέλημά μας είναι να μελετήσουμε τη συμπεριφορά του βαθμού και της διάστασης ενός διαιρέτη, όταν επεκτείνουμε το σώμα συναρτήσεων μέσω μιας επέκτασης σταθερού σώματος. Για την ακρίβεια, για $D \in \mathcal{D}_F$ θα συγκρίνουμε τα $\deg_F D$ και $l(D)$ με τα $\deg_{FE}(i_{FE/F}(D))$ και $l(i_{FE/F}(D))$. Ξεκινάμε με δύο χρήσιμα λήμματα. Από εδώ και πέρα, θα θεωρούμε ότι η επέκταση $F \leq L$ είναι επέκταση σταθερού σώματος.

Λημμα 3.2.5. *Αν $x_1, \ldots, x_m \in F$ γραμμικά ανεξάρτητα πάνω από το K, τότε τα $x_1, \ldots, x_m$ είναι γραμμικά ανεξάρτητα πάνω από το E.*

[8]Ως *διανυσματική περιοχή* εννοούμε τον διεθνή όρο *module*.

Απόδειξη. Έστω

$$\sum_{i=1}^{m} \beta_i x_i = 0, \tag{3.14}$$

με $\beta_i \in E$. Αρκεί να δείξουμε ότι $\beta_i = 0$ για κάθε i. Αν $\{\alpha_1, \ldots, \alpha_n\}$ μια K-βάση του E, τότε $\beta_i = \sum_{j=1}^{n} c_{ij}\alpha_j$, με $c_{ij} \in K$, και η (3.14) δίνει

$$\sum_{i=1}^{m} \left(\sum_{j=1}^{n} c_{ij}\alpha_j \right) x_i = \sum_{j=1}^{n} \left(\sum_{i=1}^{m} c_{ij} x_i \right) \alpha_j = 0.$$

Το τελευταίο από την πρόταση 3.2.1 μας δίνει ότι για κάθε j έχουμε ότι

$$\sum_{i=1}^{m} c_{ij} x_i = 0.$$

Όμως, τα $x_1, \ldots, x_m$ είναι K-γραμμικά ανεξάρτητα και $c_{ij} \in K$, άρα $c_{ij} = 0$ για κάθε i και j, άρα και $\beta_i = 0$ για κάθε i. ♢

Λημμα 3.2.6. *Αν $P \in \mathbb{P}_F$ και $\mathfrak{P}_1, \ldots, \mathfrak{P}_m$ οι πρώτοι του L/E που βρίσκονται πάνω από τον P, τότε οι $\mathfrak{P}_1, \ldots, \mathfrak{P}_m$ αδρανούν πάνω από τον P. Ακόμα, αν για κάποια $n \in \mathbb{Z}$ και $b \in L$ ισχύει ότι $\mathrm{ord}_{\mathfrak{P}_i}(b) \geq -n$ για κάθε i, τότε $\mathrm{ord}_P(\mathrm{tr}_{L/F}(b)) \geq -n$.*

Απόδειξη. Για την απόδειξη του πρώτου ισχυρισμού παραπέμπουμε στο [Ros, π. 8.5]. Έστω τώρα $t \in F$ τέτοιο ώστε $\mathrm{ord}_P(t) = 1$. Τότε για κάθε i, αφού ο $\mathfrak{P}_i$ αδρανεί πάνω από τον P, η (3.2) θα μας δώσει ότι $\mathrm{ord}_{\mathfrak{P}_i}(t) = 1$. Έτσι, για κάθε i έχουμε ότι $\mathrm{ord}_{\mathfrak{P}_i}(b) \geq -n$, δηλαδή $\mathrm{ord}_{\mathfrak{P}_i}(t^n b) \geq 0$. Επομένως, $t^n b \in \mathcal{O}_{\mathfrak{P}_i}$ για κάθε i, δηλαδή

$$t^n b \in \bigcap_{i=1}^{m} \mathcal{O}_{\mathfrak{P}_i}.$$

Όμως από [Sti, π. III.3.5] έχουμε ότι το $\bigcap_{i=1}^{m} \mathcal{O}_{\mathfrak{P}_i}$ είναι η ακέραια θήκη του $\mathcal{O}_P$ στο L, άρα το $t^n b$ είναι ακέραιο πάνω από το $\mathcal{O}_P$. Ακόμα το γεγονός ότι το $\bigcap_{i=1}^{m} \mathcal{O}_{\mathfrak{P}_i}$ είναι η ακέραια θήκη του $\mathcal{O}_P$ στο L, σε συνδυασμό με τον ορισμό 3.1.3, μας δίνει ότι η ακέραια θήκη του $\mathcal{O}_P$ στο F είναι η $\bigcap_{i=1}^{m} \mathcal{O}_{\mathfrak{P}_i} \cap F = \mathcal{O}_P$, δηλαδή το $\mathcal{O}_P$ είναι ακέραια κλειστός στο F. Επομένως, από το λήμμα 3.2.2(β′) έχουμε ότι $\mathrm{tr}_{L/F}(b) \in \mathcal{O}_P$. Έτσι έχουμε ότι $\mathrm{ord}_P(t^n \mathrm{tr}_{L/F}(b)) \geq 0$, δηλαδή $\mathrm{ord}_P(\mathrm{tr}_{L/F}(b)) \geq -n$. ♢

Είμαστε πλέον σε θέση να κάνουμε την προαναφερθείσα σύγκριση.

Πρόταση 3.2.7. *Αν $D \in \mathcal{D}_F$ και $L := EF$, τότε*

$$\deg_L(i_{L/F}(D)) = \deg_F D \quad \text{και} \quad l(i_{L/F}(D)) = l(D).$$

Απόδειξη. Από την πρόταση 3.2.3 το E είναι το σώμα σταθερών του L. Έτσι, δεδομένου ότι $[L : F] = [E : K]$ (πρόταση 3.2.1), από την πρόταση 3.1.17 έχουμε την πρώτη εξίσωση.

Από την πρόταση 3.1.18, έχουμε ότι αν $x \in F^*$ τότε $i_{L/F}((x)_F) = (x)_L$ και έτσι βλέπουμε άμεσα ότι $\mathcal{L}(D) \subseteq \mathcal{L}(i_{L/F}(D))$. Έστω τώρα $\{x_1, \ldots, x_d\}$ μια K-βάση του $\mathcal{L}(D)$. Τα $x_1, \ldots, x_d$ είναι K-γραμμικά ανεξάρτητα, επομένως από το λήμμα 3.2.5 θα είναι και E-γραμμικά ανεξάρτητα. Έτσι έχουμε ότι

$$l(D) \leq l(i_{L/F}(D))$$

και πλεόν αρκεί να δείξουμε ότι το σύνολο $\{x_1, \ldots, x_d\}$ παράγει τον $\mathcal{L}(i_{L/F}(D))$ πάνω από το E.

Θα ξεκινήσουμε αποδεικνύοντας ότι αν $u \in \mathcal{L}(i_{L/F}(D))$, τότε ισχύει ότι $\mathrm{tr}_{L/F}(u) \in \mathcal{L}(D)$. Από τον ορισμό του $\mathcal{L}$ χώρου έχουμε ότι $u \in \mathcal{L}(i_{L/F}(D))$ ανν για κάθε $\mathfrak{P} \in \mathbb{P}_L$ ισχύει ότι

$$\mathrm{ord}_{\mathfrak{P}}(u) \geq -\mathrm{ord}_{\mathfrak{P}}(i_{L/F}(D)).$$

Έστω τώρα $\mathfrak{P} \in \mathbb{P}_L$ και P ο πρώτος του F/K που βρίσκεται κάτω από τον $\mathfrak{P}$. Από το λήμμα 3.2.6, ο $\mathfrak{P}$ αδρανεί πάνω από τον P και έτσι από τον ορισμό 3.1.16 θα έχουμε ότι $\mathrm{ord}_{\mathfrak{P}}(i_{L/F}(D)) = \mathrm{ord}_P(D)$. Έτσι συνδυάζοντας τα παραπάνω, έχουμε ότι $u \in \mathcal{L}(i_{L/F}(D))$ ανν για κάθε $P \in \mathbb{P}_F$ έχουμε ότι

$$\mathrm{ord}_{\mathfrak{P}}(u) \geq -\mathrm{ord}_P(D)$$

για κάθε $\mathfrak{P} \in \mathbb{P}_L$ με $\mathfrak{P} \mid P$. Το τελευταίο από το λήμμα 3.2.6 μας δίνει ότι $\mathrm{ord}_P(\mathrm{tr}_{L/F}(u)) \geq -\mathrm{ord}_P(D)$ για κάθε $P \in \mathbb{P}_F$, δηλαδή $\mathrm{tr}_{L/F}(u) \in \mathcal{L}(D)$.

Τώρα είμαστε σε θέση να αποδείξουμε ότι το σύνολο $\{x_1, \ldots, x_d\}$ παράγει τον $\mathcal{L}(i_{L/F}(D))$ πάνω από το E. Έστω λοιπόν $z \in \mathcal{L}(i_{L/F}(D))$ και $\{\alpha_1, \ldots, \alpha_n\}$ μια K-βάση του E. Από την πρόταση 3.2.1 θα έχουμε ότι το $\{\alpha_1, \ldots, \alpha_n\}$ είναι μια F-βάση του L, άρα υπάρχουν $y_i \in F$ τέτοια ώστε

$$z = \sum_{i=1}^{n} y_i \alpha_i. \tag{3.15}$$

Η τελευταία σχέση, όπως στην απόδειξη της 3.2.3, μας δίνει ότι για $j = 1, \ldots, n$ ισχύει ότι

$$\mathrm{tr}_{L/F}(\alpha_j z) = \sum_{i=1}^{n} \mathrm{tr}_{L/F}(\alpha_j \alpha_i) y_i.$$

Ακόμα, μιας και $z \in \mathcal{L}(i_{L/F}(D))$, θα έχουμε και $\alpha_j z \in \mathcal{L}(i_{L/F}(D))$ και άρα σύμφωνα με τον προηγούμενο ισχυρισμό $\mathrm{tr}_{L/F}(\alpha_j z) \in \mathcal{L}(D)$. Έτσι, παρομοίως με την απόδειξη της πρότασης 3.2.3, από τον κανόνα του Cramer θα έχουμε ότι $y_i \in \mathcal{L}(D)$ για κάθε i. Έτσι, τα y_i ανήκουν στον χώρο που παράγουν K-γραμμικά τα $x_1, \ldots, x_d$, δηλαδή $y_i = \sum_{j=1}^{d} c_{ij} x_j$, με $c_{ij} \in K$. Έτσι η (3.15) γίνεται

$$z = \sum_{i=1}^{n} \left(\sum_{j=1}^{d} c_{ij} x_j \right) \alpha_i = \sum_{j=1}^{d} \left(\sum_{i=1}^{n} c_{ij} \alpha_i \right) x_j = \sum_{j=1}^{d} r_j x_j,$$

με $r_j \in E$. ♢

Η επόμενη πρόταση μας περιγράφει το γένος σε μια επέκταση σταθερού σώματος.

ΠΡΟΤΑΣΗ 3.2.8. *Το γένος του F/K είναι ίσο με το γένος του FE/E.*

ΑΠΟΔΕΙΞΗ. Θέτουμε $L := FE$, g το γένος του F/K και g' του L/E. Έστω $D \in \mathcal{D}_F$ με $\deg_F D > \max\{2g-1, 2g'-1\}$. Από την πρόταση 3.2.7 θα έχουμε ότι $\deg_L(i_{L/F}(D)) = \deg_F D$. Έτσι από το θεώρημα 2.3.3 και το θεώρημα Riemann θα έχουμε ότι

$$l(D) = \deg_F(D) - g + 1 \quad \text{και} \quad l(i_{L/F}(D)) = \deg_L(i_{L/F}(D)) - g' + 1.$$

Το τελευταίο σε συνδυασμό με την πρόταση 3.2.7, μας δίνει ότι $-g+1 = -g'+1$, δηλαδή $g = g'$. ♢

Είδαμε στην πρόταση 3.1.7 ότι υπάρχουν πεπερασμένοι το πλήθος πρώτοι του L/E που βρίσκονται πάνω από έναν πρώτο του F/K. Οι επόμενες δύο προτάσεις θα μας δείξουν ότι αν η επέκτασή μας είναι επέκταση σταθερού σώματος, τότε μπορούμε να βρούμε ακριβώς αυτό το πλήθος.

ΠΡΟΤΑΣΗ 3.2.9. *Έστω $\mathfrak{P} \in \mathbb{P}_L$ και P ο πρώτος του F/K που βρίσκεται κάτω από τον $\mathfrak{P}$. Αν $E_{\mathfrak{P}} := {}^{\mathcal{O}_{\mathfrak{P}}}/_{\mathfrak{P}}$ και $F_P := {}^{\mathcal{O}_P}/_P$, τότε $E_{\mathfrak{P}} = F_P E$.*

ΑΠΟΔΕΙΞΗ. Προφανώς $F_P E \subseteq E_{\mathfrak{P}}$. Έστω τώρα $\bar{\omega} \in E_{\mathfrak{P}}$ και $\omega \in \mathcal{O}_{\mathfrak{P}}$ ένας αντιπρόσωπος του $\bar{\omega}$. Αν $\{\mathfrak{P} = \mathfrak{P}_1, \mathfrak{P}_2, \ldots, \mathfrak{P}_m\}$ οι πρώτοι του L/E που βρίσκονται πάνω από τον P. Από το [Sti, θ. I.3.1][9] έχουμε ότι υπάρχει κάποιο $\omega' \in L$, τέτοιο ώστε $\mathrm{ord}_{\mathfrak{P}}(\omega' - \omega) > 0$ και $\mathrm{ord}_{\mathfrak{P}_i}(\omega') > 0$ για $i = 2, \ldots, m$. Τότε, προφανώς $\omega' \in \bigcap_{i=1}^{m} \mathcal{O}_{\mathfrak{P}_i}$, δηλαδή (όπως στην απόδειξη του λήμματος 3.2.6) το ω' είναι ακέραιο πάνω από το $\mathcal{O}_P$. Έτσι αν $\{\alpha_1, \ldots, \alpha_n\}$ μια K-βάση του E από το λήμμα 3.2.4 είναι και $\mathcal{O}_P$-ακέραια βάση της ακέραιας θήκης του $\mathcal{O}_P$ στο L. Έτσι υπάρχουν $x_1, \ldots, x_n \in \mathcal{O}_P$ τέτοια ώστε

$$\omega' = \sum_{i=1}^{n} x_i \, \alpha_i.$$

Η τελευταία σχέση αναγόμενη modulo $\mathfrak{P}$ μας δίνει ότι $\bar{\omega'} \in F_P E$. Όμως $\mathrm{ord}_{\mathfrak{P}}(\omega' - \omega) > 0$, οπότε $\omega' - \omega \in \mathfrak{P}$, άρα $\bar{\omega'} = \bar{\omega}$, δηλαδή $\bar{\omega} \in F_P E$. ♢

---

[9] Το θεώρημα αυτό λέγεται *ασθενές προσεγγιστικό θεώρημα* (weak approximation theorem) και αναφέρει ότι αν $P_1, \ldots, P_n$ ανά δύο ξένοι πρώτοι του F/K, $x_1, \ldots, x_n \in F$ και $r_1, \ldots, r_n \in \mathbb{Z}$, τότε υπάρχει κάποιο $x \in F$ τέτοιο ώστε $\mathrm{ord}_{P_i}(x - x_i) = r_i$ για κάθε i.

Μια ισχυρότερη εκδοχή του είναι το *ισχυρό προσεγγιστικό θεώρημα* (strong approximation theorem), που είναι επακόλουθο του θεωρήματος Riemann-Roch και επεκτείνει την ασθενή εκδοχή σε άπειρο γνήσιο υποσύνολο S του $\mathbb{P}_F$. Σύμφωνα με αυτό η ισότητα του ασθενούς να ισχύει μόνο για πεπερασμένο το πλήθος στοιχεία του S και για τα υπόλοιπα ισχύει ότι $\mathrm{ord}_P(x) \geq 0$. Για την απόδειξη δες [Sti, σελ. 31].

ΠΡΟΤΑΣΗ 3.2.10. *Έστω* $P \in \mathbb{P}_F$ *και* $F_P := {}^{\mathcal{O}_P}/_P$. *Αν* $F_P = K[\theta]$, $h(X) := \operatorname{Irr}(\theta, K)$ *και*

$$h(X) = h_1(X) \cdots h_m(X)$$

η ανάλυση του $h(X)$ *σε ανάγωγα στο* $E[X]$, *τότε υπάρχουν ακριβώς* m *το πλήθος πρώτοι του* L/E *που βρίσκονται πάνω από τον* P. *Ακόμα αν* $\{\mathfrak{P}_1, \ldots, \mathfrak{P}_m\}$ *είναι το σύνολο αυτών των πρώτων, τότε (ενδεχομένως μετά από κάποια αναδιάταξή τους)* $\deg_L \mathfrak{P}_i = \deg h_i(X)$ *για* $i = 1, \ldots, m$. *Τέλος, ισχύει ότι*

$$\deg_K P = \sum_{i=1}^{m} \deg_L \mathfrak{P}_i.$$

ΑΠΟΔΕΙΞΗ. Για την απόδειξη δες [Ros, σελ. 107]. ♢

Από την τελευταία πρόταση βλέπουμε ότι αν ${}^{\mathcal{O}_P}/_P \cong {}^{K[X]}/_{h(X)K[X]}$, τότε μπορούμε να περιγράψουμε με ακρίβεια τους πρώτους του L/E που βρίσκονται πάνω από τον P. Ακόμα, είναι εμφανές ότι αν $[E : K] = n$ και το $h(X)$ αναλύεται πλήρως στο $E[X]$, τότε υπάρχουν n το πλήθος πρώτοι του L/E που βρίσκονται πάνω από τον P βαθμού 1.

ΚΕΦΑΛΑΙΟ 4

Η συνάρτηση ζήτα του Riemann

Στο κεφάλαιο αυτό θα ασχολούμαστε αποκλειστικά με το ολικό σώμα συναρτήσεων $F/\mathbb{F}$, καθώς εκεί έχουμε τα προαναφερθέντα αποτελέσματα. Επίσης με g θα συμβολίζουμε το γένος του σώματος συναρτήσεων $F/\mathbb{F}$.

Στο κεφάλαιο αυτό θα ασχοληθούμε με τη συνάρτηση ζ του Riemann στα σώματα συναρτήσεων. Στην πρώτη παράγραφο θα δούμε τον ορισμό της και κάποιες βασικές ιδιότητές της. Στη δεύτερη παράγραφο θα δούμε την απόδειξη της ασθενούς μορφής του θεωρήματος των πρώτων αριθμών σε σώματα συναρτήσεων, η οποία βασίζεται στη θεωρία του κεφαλαίου 3. Στην τρίτη και τελευταία παράγραφο θα δούμε την απόδειξη του θεωρήματος Hasse-Weil, που είναι η υπόθεση Riemann σε σώματα συναρτήσεων· από αυτή θα αποδείξουμε και μια ισχυρότερη μορφή του θεωρήματος των πρώτων αριθμών σε σώματα συναρτήσεων.

4.1. Ορισμοί – Βασικές ιδιότητες

Πριν προχωρήσουμε στον ορισμό της συνάρτησης ζ θα δούμε κάποια αποτελέσματα που καθιστούν τη συνάρτηση ζ καλά ορισμένη.

Λημμα 4.1.1. *Το πλήθος των αποτελεσματικών διαιρετών βαθμού $n \geq 0$ είναι πεπερασμένο.*

Απόδειξη. Από τον ορισμό του διαιρέτη και του αποτελεσματικού διαιρέτη, προφανώς, αρκεί να δείξουμε ότι το σύνολο

$$S := \{P \in \mathbb{P}_F \mid \deg P \leq n\}$$

είναι πεπερασμένο.

Επιλέγουμε x υπερβατικό πάνω από το $\mathbb{F}$. Όπως είδαμε στο θεώρημα 1.2.16, οι πρώτοι του $\mathbb{F}(x)/\mathbb{F}$ βρίσκονται σε αντιστοιχία ένα προς ένα με τα μονικά ανάγωγα του $\mathbb{F}[x]$ (εκτός του απείρου πρώτου). Ακόμα, εύκολα βλέπει κανείς ότι ο βαθμός κάθε πρώτου ισούται με το βαθμό του αντίστοιχου πολυωνύμου (και ο βαθμός του P_∞ είναι 1), οπότε για κάθε $m \geq 0$ υπάρχουν πεπερασμένοι το πλήθος πρώτοι βαθμού m.

Έτσι από την πρόταση 3.1.17 θα υπάρχουν και πεπερασμένοι το πλήθος πρώτοι του $F/\mathbb{F}$ βαθμού n. ♡

Ας δούμε τώρα τον ορισμό δύο σημαντικών αριθμών.

Ορισμος 4.1.2. Θέτουμε

$$a_{F,n} := |\{P \in \mathbb{P}_F \mid \deg P = n\}|$$

και

$$b_{F,n} := |\{A \in \mathcal{D}_F \mid \deg A = n \text{ και } A \geq 0\}|.$$

Αν δεν υπάρχει κίνδυνος σύγχυσης γράφουμε απλά a_n και b_n αντίστοιχα. Ακόμα, σύμφωνα με το λήμμα 4.1.1 έχουμε ότι οι a_n και b_n είναι φυσικοί αριθμοί. Στη συνέχεια θα δούμε κάποιους ακόμα χρήσιμους ορισμούς.

Ορισμος 4.1.3. Το σύνολο

$$\mathcal{D}_F^0 := \{A \in \mathcal{D}_F \mid \deg A = 0\}$$

ονομάζεται *ομάδα διαιρετών βαθμού μηδέν* και το σύνολο

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

ονομάζεται *ομάδα κλάσεων διαιρετών βαθμού μηδέν*.

Τονίζουμε ότι ο ορισμός του $\mathcal{C}_F^0$ είναι σωστός από το πόρισμα 1.3.14. Στη συνέχεια θα δούμε μια πολύ σημαντική ιδιότητα του $\mathcal{C}_F^0$.

Προταση 4.1.4. *Η ομάδα κλάσεων διαιρετών βαθμού μηδέν είναι πεπερασμένη.*

Αποδειξη. Έστω $B \in \mathcal{D}_F$ με $\deg B =: n \geq g$ και

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

Η απεικόνιση

$$\phi : \begin{array}{ccc} \mathcal{C}_F^0 & \to & \mathcal{C}_F^n \\ [A] & \mapsto & [A+B] \end{array}$$

είναι, προφανώς, ένα προς ένα και επί, επομένως αρκεί να δείξουμε ότι $|\mathcal{C}_F^n| < \infty$. Όμως από το λήμμα 4.1.1 αρκεί να δείξουμε ότι για κάθε $[C] \in \mathcal{C}_F^n$ υπάρχει κάποιος $A \in [C]$ με $A \geq 0$.

Πράγματι, έστω $[C] \in \mathcal{C}_F^n$. Από το θεώρημα Riemann-Roch έχουμε ότι

$$l(C) \geq \deg C + 1 - g = n + 1 - g > 0.$$

Έτσι $\mathcal{L}(C) \neq \{0\}$ και από την παρατήρηση μετά τον ορισμό 1.3.8 έπεται ότι υπάρχει κάποιος αποτελεσματικός διαιρέτης $A \in [C]$. ♡

Ένας ακόμα σημαντικός ορισμός είναι ο παρακάτω.

Ορισμος 4.1.5. Ο αριθμός

$$h_F := |\mathcal{C}_F^0|$$

ονομάζεται *αριθμός κλάσεων* του $F/\mathbb{F}$.

Η πρόταση 4.1.4 μας δείχνει ότι ο αριθμός κλάσεων ενός ολικού σώματος συναρτήσεων είναι φυσικός αριθμός, ενώ το γιατί ο αριθμός αυτός καλείται αριθμός κλάσεων θα το δούμε αργότερα. Ένας άλλος αριθμός που θα μας απασχολήσει προσωρινά είναι ο

$$\vartheta := \min\{\deg A \mid A \in \mathcal{D}_F \text{ και } A > 0\}.$$

Είναι προφανές ότι αν $\vartheta \nmid n$, τότε $b_n = 0$. Συνεχίζουμε με ένα χρήσιμο λήμμα.

ΛΗΜΜΑ 4.1.6. *Έστω $C \in \mathcal{D}_F$. Ισχύει ότι*[1]

$$|\{A \in [C] \mid A \geq 0\}| = \frac{q^{l(C)} - 1}{q - 1}.$$

Ακόμα αν $n > 2g - 2$ και $\vartheta \mid n$, τότε

$$b_n = \frac{h_F}{q-1}(q^{n+1-g} - 1).$$

ΑΠΟΔΕΙΞΗ. Έχουμε ότι $A \in [C]$ και $A \geq 0$ ανν $A = (x) + C$ για κάποιο $x \in F \setminus \{0\}$ με $(x) \geq -C$. Το τελευταίο σημαίνει ότι $x \in \mathcal{L}(C) \setminus \{0\}$. Όμως τέτοιες δυνατές επιλογές του x είναι ακριβώς $q^{l(C)} - 1$, ενώ δύο εξ αυτών δίνουν τον ίδιο διαιρέτη ανν διαφέρουν κατά σταθερά $\alpha \in \mathbb{F}$. Έτσι προκύπτει η πρώτη σχέση.

Όπως είδαμε και στην απόδειξη της πρότασης 4.1.4 υπάρχουν ακριβώς h_F κλάσεις διαιρετών με διαιρέτες βαθμού n. Έστω $[C_1], \ldots, [C_{h_F}]$ οι κλάσεις αυτές. Από το θεώρημα 2.3.3 και το προηγούμενο έχουμε ότι, για $j = 1, \ldots, h_F$,

$$|\{A \in [C_j] \mid A \geq 0\}| = \frac{q^{l(C_j)} - 1}{q - 1} = \frac{q^{n+1-g} - 1}{q - 1}.$$

Ακόμα, κάθε διαιρέτης βαθμού n ανήκει σε ακριβώς μια από τις κλάσεις $[C_1], \ldots, [C_{h_F}]$. Έτσι προκύπτει το ζητούμενο. ♡

Πριν ορίσουμε τη συνάρτηση ζ θα δούμε έναν ορισμό μιας ακόμα βοηθητικής συνάρτησης.

ΟΡΙΣΜΟΣ 4.1.7. Αν $A \in \mathcal{D}_F$ ως NA ορίζουμε τον αριθμό $q^{\deg A}$.

Είναι προφανές ότι αν A και B διαιρέτες, τότε

$$N(A + B) = NA \cdot NB \tag{4.1}$$

Είμαστε πλέον σε θέση να ορίσουμε τη συνάρτηση ζ.

ΟΡΙΣΜΟΣ 4.1.8. Η *συνάρτηση ζήτα* του $F/\mathbb{F}$ ορίζεται ως

$$\zeta_F(s) := \sum_{\substack{A \in \mathcal{D}_F \\ A \geq 0}} NA^{-s}, \quad s \in \mathbb{C}.$$

Εύκολα βλέπει κανείς ότι η συνάρτηση ζ_F μπορεί να γραφτεί και με άλλους χρήσιμους τρόπους. Έτσι έχουμε π.χ. ότι $NA^{-s} = q^{-ns}$, όπου $n := \deg A$, άρα καταλήγουμε ότι

$$\zeta_F(s) = \sum_{n=1}^{\infty} \frac{b_n}{q^{ns}}. \tag{4.2}$$

[1] Υπενθυμίζουμε ότι $q := |\mathbb{F}|$, σύμφωνα με τις παραδοχές της σελίδας iv.

Ακόμα, αν θεωρήσουμε ένα $s \in \mathbb{C}$ τέτοιο ώστε η $\zeta_F(s)$ να είναι συγκλίνουσα, τότε από την (4.1) και τον ορισμό του $\mathcal{D}_F$ εύκολα βλέπουμε ότι

$$\zeta_F(s) = \prod_{P \in \mathbb{P}_F} \left(\sum_{j=0}^{\infty} (NP)^{-js} \right)$$

και επειδή συγκλίνει η $\zeta_F(s)$ θα συγκλίνει και η $\sum_{j=0}^{\infty}(NP)^{-js}$, και κάθε μια από τις σειρές αυτές είναι μια συγκλίνουσα γεωμετρική σειρά με άθροισμα $(1-(NP)^{-s})^{-1}$. Έτσι έχουμε ότι

$$\zeta_F(s) = \prod_{P \in \mathbb{P}_F} (1-(NP)^{-s})^{-1}. \tag{4.3}$$

Επιπροσθέτως, έχουμε άμεσα από τους ορισμούς και την (4.3) ότι

$$\zeta_F(s) = \prod_{n=1}^{\infty} (1-q^{-ns})^{-a_n}. \tag{4.4}$$

Οι δύο παραπάνω εκφράσεις της ζ_F ονομάζονται τα *γινόμενα Euler της ζήτα*. Στη συνέχεια θα δούμε μια ισοδύναμη, αλλά συχνά πιο πρακτική γραφή της ζ_F.

Ορισμος 4.1.9. Θέτουμε $u := q^{-s}$ και η συνάρτηση

$$Z_F(u) := \zeta_F(s) = \sum_{n=0}^{\infty} b_n u^n$$

ονομάζεται *συνάρτηση Ζήτα* του $F/\mathbb{F}$.

Ακόμα από τον παραπάνω ορισμό και την (4.3) έχουμε ότι

$$Z_F(u) = \prod_{P \in \mathbb{P}_F} (1-u^{\deg P})^{-1}, \tag{4.5}$$

δηλαδή το *γινόμενο Euler της Ζήτα*.

Επόμενο μέλημά μας είναι να δείξουμε ότι η συνάρτηση ζήτα συγκλίνει απόλυτα για $s \in \mathbb{C}$ με $\Re(s) > 1$. Είναι προφανές ότι αυτό είναι ισοδύναμο με τη σύγκλιση της Ζήτα για $u \in \mathbb{C}$ με $|u| < q^{-1}$.

Προταση 4.1.10. *Η δυναμοσειρά*

$$\zeta_F(s) = \sum_{n=1}^{\infty} \frac{b_n}{q^{ns}}$$

και το απειρογινόμενο

$$\zeta_F(s) = \prod_{n=1}^{\infty} (1-q^{-ns})^{-a_n}$$

συγκλίνουν απόλυτα για $s \in \mathbb{C}$ *με* $\Re(s) > 1$.

Απόδειξη. Από το λήμμα 4.1.6 και τα σχόλια μετά τον ορισμό 4.1.5 έχουμε ότι το b_n είναι το πολύ $O(q^n)$. Από αυτό η ισχύς του πρώτου ισχυρισμού έπεται άμεσα.

Για την απόδειξη του δεύτερου ισχυρισμού παρατηρούμε ότι

$$\prod_{n=1}^{\infty}(1-q^{-ns})^{-a_n}=\prod_{n=1}^{\infty}(1-A_n),$$

όπου A_n τέτοιο ώστε $A_n=q^{-ms}$ με $\sum_{j=1}^{m-1}a_j<m\leq\sum_{j=1}^{m}a_j$. Από [Για, Τόμος Ιια, σελ. 174–176] έχουμε ότι το δεύτερο μέλος της ισότητας συγκλίνει απόλυτα ανν η $\sum_{n=1}^{\infty}|A_n|$ συγκλίνει, δηλαδή ανν η $\sum_{n=1}^{\infty}a_n|q^{-ns}|$ συγκλίνει. Όμως το τελευταίο ισχύει αφού $a_n\leq b_n$ και το b_n είναι το πολύ $O(q^n)$. ♡

Πρόταση 4.1.11. *Για $s\in\mathbb{C}$ με $\Re(s)>1$ έχουμε ότι*
(α′) αν $g=0$, τότε

$$\zeta_F(s)=\frac{1}{q-1}\left(\frac{q}{1-q^{(1-s)\vartheta}}-\frac{1}{1-q^{-s\vartheta}}\right)$$

(β′) και αν $g\geq 1$, τότε $\zeta_F(s)=f_1(s)+f_2(s)$ όπου

$$f_1(s)=\frac{1}{q-1}\sum_{\substack{[C]\in\mathcal{C}_F\\ 0\leq\deg C\leq 2g-2}}q^{l(C)-s\deg C}$$

και

$$f_2(s)=\frac{h_F}{q-1}\left(\frac{q^{1-g+(1-s)(2g-2+\vartheta)}}{1-q^{\vartheta(1-s)}}-\frac{1}{1-q^{-s\vartheta}}\right).$$

Απόδειξη. Θα δείξουμε τις αντίστοιχες σχέσεις για την $Z_F(u)$, όπου $u=q^{-s}$.

α′) Έστω $[A]\in\mathcal{C}_F^0$. Τότε από το θεώρημα Riemann-Roch έχουμε ότι $l(A)=\deg A+1-g=1$, οπότε υπάρχει κάποιο $x\in F\setminus\{0\}$ με $(x)\geq -A$. Όμως από το πόρισμα 1.3.14 θα έχουμε $\deg A=\deg(-(x))=0$ και ως εκ τούτου $A=-(x)=(x^{-1})$, οπότε $A\in\mathcal{P}_F$, δηλαδή $[A]=\mathcal{P}_F$. Έτσι καταλήγουμε ότι $h_F=1$.

Στη συνέχεια από τον ορισμό 4.1.9, το λήμμα 4.1.6, τα σχόλια μετά τον ορισμό 4.1.5 και το προηγούμενο, για $|u|<q^{-1}$ θα έχουμε ότι

$$\begin{aligned}Z_F(u)&=\sum_{n=0}^{\infty}b_nu^n=\sum_{n=0}^{\infty}b_{\vartheta n}u^{\vartheta n}=\sum_{n=0}^{\infty}\frac{q^{\vartheta n+1}-1}{q-1}\cdot u^{\vartheta n}\\&=\frac{1}{q-1}\left(q\sum_{n=0}^{\infty}(qu)^{\vartheta n}-\sum_{n=0}^{\infty}u^{\vartheta n}\right)\\&=\frac{1}{q-1}\left(\frac{q}{1-(qu)^{\vartheta}}-\frac{1}{1-u^{\vartheta}}\right).\end{aligned}$$

β′) Σε αυτή την περίπτωση από το λήμμα 4.1.6 και το θεώρημα Riemann-Roch έχουμε ότι

$$\begin{aligned} Z_F(u) = \sum_{n=0}^{\infty} b_n u^n &= \sum_{\substack{[C]\in\mathcal{C}_F \\ \deg C\geq 0}} |\{A \in [C] \mid A \geq 0\}| \cdot u^{\deg C} \\ &= \sum_{\substack{[C]\in\mathcal{C}_F \\ \deg C\geq 0}} \frac{q^{l(C)}-1}{q-1} \cdot u^{\deg C} \\ &= \frac{1}{q-1} \sum_{\substack{[C]\in\mathcal{C}_F \\ 0\leq \deg C\leq 2g-2}} q^{l(C)} u^{\deg C} \\ &\quad + \frac{1}{q-1} \sum_{\substack{[C]\in\mathcal{C}_F \\ \deg C> 2g-2}} q^{\deg C+1-g} \cdot u^{\deg C} - \frac{1}{q-1} \sum_{\substack{[C]\in\mathcal{C}_F \\ \deg C\geq 0}} u^{\deg C}. \end{aligned}$$

Από το τελευταίο εύκολα βλέπουμε ότι προκύπτει το ζητούμενο για $|u| < q^{-1}$. ♡

Πορισμα 4.1.12. *Η συνάρτηση ζήτα επεκτείνεται αναλυτικά στο* $\mathbb{C}$ *με απλούς πόλους στα σημεία* $s = 0$ *και* $s = 1$.

Αποδειξη. Άμεσο από την πρόταση 4.1.11. ♡

Επόμενος στόχος μας είναι να δείξουμε ότι σε οποιοδήποτε ολικό σώμα υπάρχουν διαιρέτες βαθμού 1. Η πρώτη απόδειξη του αποτελέσματος αυτού υπάρχει στο [Sch].

Από τη θεωρία σωμάτων γνωρίζουμε ότι για κάθε $r \geq 1$ υπάρχει μοναδική επέκταση $\mathbb{F}_{q^r}/\mathbb{F}$ βαθμού r. Θέτουμε

$$F_r := F\mathbb{F}_{q^r}. \tag{4.6}$$

Είναι προφανές ότι η επέκταση σωμάτων συναρτήσεων $F \leq F_r$ είναι επέκταση σταθερού σώματος και από την πρόταση 3.2.3 έχουμε ότι το $\mathbb{F}_{q^r}$ είναι το σώμα σταθερών του $F_r/\mathbb{F}_{q^r}$, ενώ από την πρόταση 3.2.8 έχουμε ότι το γένος του $F_r/\mathbb{F}_{q^r}$ θα είναι g. Ακόμα, ισχύει το παρακάτω λήμμα.

Λημμα 4.1.13. *Έστω* $P \in \mathbb{P}_F$ *με* $\deg P = m$. *Τότε* $i_{F_r/F}(P) = \mathfrak{P}_1 + \cdots + \mathfrak{P}_d$, *με* $d := \gcd(m, r)$ *και* $\mathfrak{P}_i$ *διάφορους ανά δύο, βαθμού* m/d *πρώτους του* $F_r/\mathbb{F}_{q^r}$.

Αποδειξη. Έστω $\mathfrak{P} \in \mathbb{P}_{F_r}$ με $\mathfrak{P} \mid P$. Από το λήμμα 3.2.6 ο $\mathfrak{P}$ αδρανεί πάνω από τον P και από την πρόταση 3.2.9 θα έχουμε ότι

$$\mathcal{O}_{\mathfrak{P}} \big/ \mathfrak{P} = \mathbb{F}_{q^r} \cdot \mathcal{O}_P \big/ P.$$

Όμως από τον ορισμό 1.2.11 έχουμε ότι $\mathcal{O}_P/_P = \mathbb{F}_{q^m}$. Έτσι αν $l := \operatorname{lcm}(m,r)$, τότε $\mathcal{O}_\mathfrak{P}/_\mathfrak{P} = \mathbb{F}_{q^l}$. Δηλαδή βλέπουμε ότι

$$\deg \mathfrak{P} := \left[\mathcal{O}_\mathfrak{P}/_\mathfrak{P} : \mathbb{F}_{q^r}\right] = [\mathbb{F}_{q^l} : \mathbb{F}_{q^r}] = m/d.$$

Το αποτέλεσμα έπεται άμεσα από τα παραπάνω και το γεγονός ότι

$$\deg_{F_r}(i_{F_r/F}(P)) = \deg_F P = m,$$

από την πρόταση 3.2.7. ♡

Ένα ακόμα λήμμα που θα μας χρειαστεί είναι το παρακάτω (τεχνικό) λήμμα.

Λημμα 4.1.14. *Έστω $m, r \in \mathbb{Z}$ και $d := \gcd(m,r)$. Αν $\omega_1, \ldots, \omega_r$ είναι οι r-στές ρίζες της μονάδας στο $\mathbb{C}$ και $t \in \mathbb{C}$, τότε*

$$(1 - t^{mr/d})^d = \prod_{j=1}^{r}(1 - (\omega_j t)^m).$$

Απόδειξη. Παρατηρούμε ότι τα πολυώνυμα $f_1(X) := (X^{r/d} - 1)^d$ και $f_2(X) := \prod_{j=1}^{r}(X - \omega_j^m)$ του $\mathbb{C}[X]$ είναι αμφότερα μονικά, βαθμού r και έχουν ως ρίζες τάξης r/d τα ω_j, άρα θα έχουμε ότι $f_1(X) = f_2(X)$. Η προς απόδειξη σχέση έπεται άμεσα αν αντικαταστήσουμε το X με t^{-m}. ♡

Ας δούμε τώρα μια ενδιαφέρουσα πρόταση.

Προταση 4.1.15. *Αν $\omega_1, \ldots, \omega_r$ είναι οι r-στές ρίζες της μονάδας στο $\mathbb{C}$, τότε*

$$Z_{F_r}(u^r) = \prod_{j=1}^{r} Z_F(\omega_j u).$$

Απόδειξη. Εφόσον αμφότερες οι Z_{F_r} και Z_F είναι αναλυτικές στο $\mathbb{C} \setminus \{1, q^{-1}\}$, αρκεί να δείξουμε την προς απόδειξη σχέση για $|u| < q^{-1}$. Στην περιοχή αυτή το γινόμενο Euler της Z_{F_r} είναι

$$Z_{F_r}(u^r) = \prod_{\mathfrak{P} \in \mathbb{P}_{F_r}} (1 - u^{r \cdot \deg \mathfrak{P}})^{-1} = \prod_{P \in \mathbb{P}_F} \prod_{\mathfrak{P} | P} (1 - u^{r \cdot \deg \mathfrak{P}})^{-1}. \tag{4.7}$$

Έστω $P \in \mathbb{P}_F$. Θέτουμε $m := \deg P$ και $d := \gcd(r,m)$ και έχουμε ότι

$$\prod_{\mathfrak{P}|P}(1 - u^{r \cdot \deg \mathfrak{P}}) = (1 - u^{rm/d})^d = \prod_{j=1}^{r}(1 - (\omega_r u)^m)$$

$$= \prod_{j=1}^{r}(1 - (\omega_j u)^{\deg P})$$

από τα λήμματα 4.1.13 και 4.1.14. Έτσι η (4.7) δίνει

$$Z_{F_r}(u^r) = \prod_{j=1}^{r} \prod_{P\in\mathbb{P}_F} (1-(\omega_j u)^{\deg P})^{-1} = \prod_{j=1}^{r} Z_F(\omega_j u). \qquad \heartsuit$$

Είμαστε πλέον σε θέση να δείξουμε το θεώρημα του F. K. Schmidt.

Θεωρημα 4.1.16 (Schmidt). $\vartheta = 1$.

Αποδειξη. Εφόσον $\vartheta \mid \deg P$ για κάθε $P \in \mathbb{P}_F$, αν ω είναι μια ϑ-στη ρίζα της μονάδας στο $\mathbb{C}$, τότε

$$Z_F(\omega u) = \prod_{P\in\mathbb{P}_F} (1-(\omega u)^{\deg P})^{-1} = \prod_{P\in\mathbb{P}_F} (1-u^{\deg P})^{-1} = Z_F(u).$$

Επομένως $Z_{F_\vartheta}(u^\vartheta) = Z_F(u)^\vartheta$, από την πρόταση 4.1.15. Όμως, από το πόρισμα 4.1.12, η $Z_{F_\vartheta}(u^\vartheta)$ έχει απλό πόλο στο $u=1$, ενώ από το ίδιο πόρισμα, η $Z_F(u)^\vartheta$ έχει στο ίδιο σημείο πόλο βαθμού ϑ. Έτσι καταλήγουμε ότι $\vartheta = 1$. $\heartsuit$

Ένα άμεσο πόρισμα του θεωρήματος Scmidt και της πρότασης 2.3.5 είναι ότι, το $F/\mathbb{F}$ είναι ρητό ανν $g = 0$. Ακόμα, παρατηρούμε ότι η πρόταση 4.1.11 επαναδιατυπώνεται απλούστερα ως εξής.

Πορισμα 4.1.17. *Για $s \in \mathbb{C}$ με $\Re(s) > 1$ έχουμε ότι αν $g = 0$, τότε*

$$\zeta_F(s) = \frac{1}{(1-q^{1-s})(1-q^{-s})}$$

και αν $g \geq 1$, τότε $\zeta_F(s) = f_1(s) + f_2(s)$, με

$$f_1(s) = \frac{1}{q-1} \sum_{\substack{[C]\in\mathcal{C}_F \\ 0\leq \deg C\leq 2g-2}} q^{l(C)-s\deg C}$$

και

$$f_2(s) = \frac{h_F}{q-1} \cdot \frac{-q^g(q^{-s})^{2g} + q^g(q^{-s})^{2g-1} + q(q^{-s}) - 1}{(1-q^{1-s})(1-q^{-s})}.$$

Αποδειξη. Το αποτέλεσμα είναι άμεσο από την πρόταση 4.1.11, το θεώρημα 4.1.16 και μερικές αλγεβρικές πράξεις. $\heartsuit$

Ένα ακόμα πολύ σημαντικό πόρισμα είναι το παρακάτω.

Λημμα 4.1.18. *Υπάρχει κάποιο $L_F(u) \in \mathbb{Z}[u]$, με $\deg L_F = 2g$ τέτοιο ώστε*

$$\zeta_F(s) = \frac{L_F(q^{-s})}{(1-q^{-s})(1-q^{1-s})}.$$

Ακόμα $L_F(0) = 1$, $L_F'(0) = a_1 - 1 - q$ και $L_F(1) = h_F$.

Αποδειξη. Η ύπαρξη κάποιου πολυωνύμου του $L_F(u) \in \mathbb{Q}[u]$ με $\deg L_F = 2g$ και

$$\zeta_F(s) = \frac{L_F(q^{-s})}{(1-q^{-s})(1-q^{1-s})}$$

έπεται άμεσα από το πόρισμα 4.1.17. Ακόμα αν $u := q^{-s}$ παρατηρούμε ότι

$$L_F(u) = (1-u)(1-qu)Z_F(u) = (1-u)(1-qu)\sum_{n=0}^{\infty} b_n u^n$$
$$= \sum_{n=0}^{\infty} b_n u^n - (q+1)\sum_{n=0}^{\infty} b_n u^{n+1} + q\sum_{n=0}^{\infty} b_n u^{n+2} = \sum_{n=0}^{\infty} A_n u^n,$$

όπου

$$A_n = \begin{cases} b_0 & , \ n=0 \\ b_1 - (q+1)b_0 & , \ n=1 \\ qb_{n+2} - (q+1)b_{n+1} + b_n & , \ n \geq 2 \ . \end{cases}$$

Από το παραπάνω είναι προφανές ότι $L_F(u) \in \mathbb{Z}[u]$ και ακόμα ότι $L_F(0) = b_0$ και $L'_F(0) = b_1 - (q+1)b_0$, ενώ από τον ορισμό 4.1.2 είναι σαφές ότι $b_0 = 1$ και $b_1 = a_1$. Έτσι καταλήγουμε ότι $L_F(0) = 1$ και $L'_F(0) = a_1 - 1 - q$.

Το γεγονός ότι $L_F(1) = h_F$ είναι άμεσο στην περίπτωση που $g = 0$, αφού τότε $h_F = 1$, όπως είδαμε στην απόδειξη της πρότασης 4.1.11(α′) και από το πόρισμα 4.1.17 βλέπουμε ότι $L_F(u) = 1$ για κάθε $u \in \mathbb{C}$. Αν $g \geq 1$, τότε από το πόρισμα 4.1.17 έχουμε ότι

$$L_F(1) = \lim_{u\to 1}(1-u)(1-qu)Z_F(u) = h_F. \qquad \heartsuit$$

Το πολυώνυμο $L_F(u)$ της παραπάνω πρότασης ονομάζεται το *L-πολυώνυμο* του $F/\mathbb{F}$ και είναι καθοριστικής σημασίας, όπως θα δούμε και παρακάτω. Πριν κλείσουμε αυτήν την παράγραφο ας δούμε άλλη μια σημαντική ιδιότητα της συνάρτησης ζήτα.

Θεωρημα 4.1.19 (Συναρτησιακή Εξίσωση της ζ_F). *Για κάθε $s \in \mathbb{C}$ έχουμε ότι*

$$q^{(g-1)(1-s)}\zeta_F(1-s) = q^{(g-1)s}\zeta_F(s).$$

Απόδειξη. Αν θέσουμε $u := q^{-s}$, τότε η προς απόδειξη σχέση είναι ισοδύναμη με την

$$Z_F(u) = q^{g-1}u^{2g-2}Z_F((qu)^{-1}).$$

Για $g = 0$ η σχέση έπεται άμεσα από το πόρισμα 4.1.17. Για $g \geq 1$, το πόρισμα 4.1.17 συνεπάγεται ότι $Z_F(u) = F_1(u) + F_2(u)$ με

$$F_1(u) := \frac{1}{q-1} \sum_{\substack{[C]\in\mathcal{C}_F \\ 0\leq \deg C \leq 2g-2}} q^{l(C)} u^{\deg C}$$

και

$$F_2(u) := \frac{h_F}{q-1}\left(q^g u^{2g-1}\frac{1}{1-qu} - \frac{1}{1-u}\right).$$

Έτσι, από το θεώρημα Riemann-Roch και την πρόταση 2.3.1, αν η $\mathcal{W}_F$ είναι η κανονική κλάση του $F/\mathbb{F}$ και $W \in \mathcal{W}_F$, τότε

$$\begin{aligned}(q-1)F_1(u) &= \sum_{\substack{[C]\in\mathcal{C}_F\\ 0\le\deg C\le 2g-2}} q^{l(C)}u^{\deg C}\\ &= \sum_{\substack{[C]\in\mathcal{C}_F\\ 0\le\deg C\le 2g-2}} q^{\deg C+1-g+l(W-C)}u^{\deg C}\\ &= q^{g-1}u^{2g-2}\sum_{\substack{[C]\in\mathcal{C}_F\\ 0\le\deg C\le 2g-2}} q^{\deg C-(2g-2)+l(W-C)}u^{\deg C-(2g-2)}\\ &= q^{g-1}u^{2g-2}\sum_{\substack{[C]\in\mathcal{C}_F\\ 0\le\deg C\le 2g-2}} q^{l(W-C)}((qu)^{-1})^{\deg(W-C)}\\ &= q^{g-1}u^{2g-2}(q-1)F_1((qu)^{-1}),\end{aligned}$$

δηλαδή[2]

$$F_1(u) = q^{g-1}u^{2g-2}F_1((qu)^{-1}). \tag{4.8}$$

Ακόμα έχουμε ότι

$$\begin{aligned}&q^{g-1}u^{2g-2}F_2((qu)^{-1})\\ &\quad= \frac{h_F}{q-1}q^{g-1}u^{2g-2}\left(q^g\left(\frac{1}{qu}\right)^{2g-1}\frac{1}{1-q\frac{1}{qu}}-\frac{1}{1-\frac{1}{qu}}\right)\\ &\quad= \frac{h_F}{q-1}\left(\frac{1}{u}\frac{1}{1-\frac{1}{u}}-\frac{q^gu^{2g-1}}{qu\left(1-\frac{1}{qu}\right)}\right)\\ &\quad= \frac{h_F}{q-1}\left(q^gu^{2g-1}\frac{1}{1-qu}-\frac{1}{1-u}\right),\end{aligned}$$

δηλαδή

$$F_2(u) = q^{g-1}u^{2g-2}F_2((qu)^{-1}). \tag{4.9}$$

Από τις (4.8) και (4.9) έχουμε την προς απόδειξη σχέση. ♡

4.2. Το θεώρημα των πρώτων αριθμών ασθενής μορφή)

Το θεώρημα των πρώτων αριθμών στην κλασική του μορφή, αναφέρει ότι, αν $\pi(x)$ είναι το πλήθος των πρώτων που είναι μικρότεροι από x, τότε

$$\lim_{x\to\infty}\frac{\pi(x)\log x}{x} = 1.$$

[2]Στις παραπάνω πράξεις χρησιμοποιήσαμε την ταυτότητα

$$-\deg(W-C) = \deg C-(2g-2).$$

Η ταυτότητα αυτή προκύπτει εφαρμόζοντας το θεώρημα Riemann-Roch αρχικά για τον C και μετά για τον $W-C$, και, εν τέλει, συνδυάζοντας τις δύο σχέσεις.

Το θεώρημα αυτό αποδείχθηκε ανεξάρτητα από τους Hadamard και de la Vallée Poussin το 1896, ενώ ως πρόβλημα ήταν ανοιχτό για περίπου 100 χρόνια. Ακόμα, στην απόδειξη συνέβαλαν σχεδόν όλοι οι μεγάλοι μαθηματικοί του $19^{ου}$ αιώνα και έτσι δικαίως θεωρήθηκε ως ένα από τα μεγαλύτερα μαθηματικά επιτεύγματα του αιώνα αυτού. Στο [Jam] υπάρχουν δύο αποδείξεις του θεωρήματος, ιστορικά στοιχεία και εφαρμογές.

Ένα ανάλογο θεώρημα, σύμφωνα με την αντιστοιχία του $\mathbb{Z}$ με το $\mathbb{F}[x]$ που αναφέραμε στον πρόλογο, υπάρχει στο [Ros, κεφ. 2]. Βάσει αυτού, αν με a_n συμβολίσουμε το πλήθος των μονικών ανάγωγων πολυωνύμων βαθμού n του $\mathbb{F}_q[x]$, τότε

$$a_n = \frac{q^n}{n} + O\left(\frac{q^{n/2}}{n}\right).$$

Αν και η απόδειξη είναι σαφώς ευκολότερη, είναι ισχυρότερο από το αντίστοιχο του κλασικού θεωρήματος των πρώτων αριθμών και το αντίστοιχο αποτέλεσμα στην κλασική Θεωρία Αριθμών συνεπάγεται την υπόθεση Riemann (βλέπε [Jam, §5.2]).

Στην παράγραφο αυτή θα δείξουμε ένα θεώρημα, το οποίο, αν και φαινομενικά ασθενέστερο από το θεώρημα των πρώτων αριθμών στα πολυώνυμα, είναι γενικότερο, από την άποψη ότι ισχύει για επεκτάσεις. Στην αποδεικτική διαδικασία δεν θα χρειαστούμε την υπόθεση Riemann για σώματα συναρτήσεων.

Στην επόμενη παράγραφο, αφού πρώτα αποδείξουμε την υπόθεση Riemann για σώματα συναρτήσεων, θα δούμε ένα ακόμα ισχυρότερο αποτέλεσμα, που μοιάζει σαν ανάλογο του θεωρήματος των πρώτων αριθμών στα πολυώνυμα.

Τέλος, για κάθε $r > 0$ θα ορίζουμε το σώμα F_r όπως ορίστηκε στην (4.6). Θα ξεκινήσουμε με κάποια αποτελέσματα σχετικά με επεκτάσεις σταθερού σώματος πάνω από ολικά σώματα συναρτήσεων, τα οποία θα μας οδηγήσουν σε κάποια αποτελέσματα για τη συνάρτηση ζήτα.

Πρόταση 4.2.1. *Αν $P \in \mathbb{P}_F$, τότε υπάρχουν ακριβώς $\gcd(n, \deg_F P)$ πρώτοι του F_n, που βρίσκονται πάνω από τον P. Ακόμα αν $\mathfrak{P} \in \mathbb{P}_{F_n}$ και $\mathfrak{P} \mid P$, τότε*

$$\deg_{F_n} \mathfrak{P} = \frac{\deg_F P}{\gcd(n, \deg_F P)} \quad \text{και} \quad f(\mathfrak{P}/P) = \frac{n}{\gcd(n, \deg_F P)}.$$

Απόδειξη. Έστω $\mathfrak{P} \in \mathbb{P}_{F_n}$ με $\mathfrak{P} \mid P$. Έχουμε ότι $\deg_F P := \left[{}^{\mathcal{O}_P}\!/_P : \mathbb{F}\right]$, άρα ${}^{\mathcal{O}_P}\!/_P = \mathbb{F}_{q^{\deg_F P}}$. Έτσι από γνωστό αποτέλεσμα της θεωρίας πεπερασμένων σωμάτων θα έχουμε ότι

$$\mathcal{O}_P \big/ P \cdot \mathbb{F}_{q^n} = \mathbb{F}_{q^{\deg_F P}} \cdot \mathbb{F}_{q^n} = \mathbb{F}_{q^{\mathrm{lcm}(n, \deg_F P)}}.$$

Έτσι από την πρόταση 3.2.9 θα έχουμε ότι ${}^{O_{\mathfrak{P}}}\!/_{\mathfrak{P}} = \mathbb{F}_{q^{\mathrm{lcm}(n, \deg_F P)}}$, οπότε

$$\deg_{F_n} \mathfrak{P} := \left[\mathcal{O}_{\mathfrak{P}} \big/ \mathfrak{P} : \mathbb{F}_{q^n}\right] = \frac{\mathrm{lcm}(n, \deg_F P)}{n} = \frac{\deg_F P}{\gcd(n, \deg_F P)}.$$

Ακόμα θα έχουμε ότι

$$f(\mathfrak{P}/P) := \left[\mathcal{O}_{\mathfrak{P}}\big/\mathfrak{P} : \mathcal{O}_P\big/P\right] = \frac{\operatorname{lcm}(n, \deg_F P)}{\deg_F P} = \frac{n}{\gcd(n, \deg_F P)} .$$

Επιπροσθέτως, έχουμε ήδη δει ότι η επέκταση $F \leq F_n$ είναι επέκταση σταθερού σώματος, άρα από το λήμμα 3.2.6 έχουμε ότι ο $\mathfrak{P}$ αδρανεί πάνω από τον P. Έτσι από τη θεμελιώδη ταυτότητα θα έχουμε ότι υπάρχουν ακριβώς $\gcd(n, \deg_F P)$ πρώτοι του $F_n/\mathbb{F}_{q^n}$ που βρίσκονται πάνω από τον P. ♡

Ακόμα θα μας χρειαστεί μια στοιχειώδης ταυτότητα.

Λημμα 4.2.2. *Έστω $\omega_n \in \mathbb{C}$ μια πρωταρχική n-στή ρίζα της μονάδας, $u \in \mathbb{C}$ και $m \in \mathbb{Z}_{>0}$. Τότε*

$$\prod_{j=0}^{n-1}(1 - \omega_n^{jm}u^m) = (1 - u^{\operatorname{lcm}(m,n)})^{\gcd(m,n)}.$$

Απόδειξη. Έχουμε ότι $X^n - 1 = \prod_{j=0}^{n-1}(X - \omega_n^j)$, αφού και τα δύο πολυώνυμα του $\mathbb{C}[X]$ είναι μονικά, βαθμού n και έχουν τις ίδιες ρίζες, με τάξη 1. Έτσι για $X = u^{-1}$ καταλήγουμε ότι

$$u^{-n} - 1 = \prod_{j=0}^{n-1}(u^{-1} - \omega_n^j) \;\Rightarrow\; 1 - u^n = \prod_{j=0}^{n-1}(1 - u\omega_n^j),$$

δηλαδή δείξαμε το ζητούμενο για $m = 1$.

Για $m > 1$ θέτουμε $m' := m/\gcd(n, m)$ και $n' := n/\gcd(m, n)$ και βλέπουμε εύκολα ότι το ω_n^m είναι μια πρωταρχική n'-στη ρίζα της μονάδας, την οποία ονομάζουμε $\omega_{n'}$. Από τον τύπο της Ευκλείδειας διαίρεσης έχουμε ότι για κάθε $j = 0, 1, \ldots, n-1$ υπάρχουν μοναδικά k και r, με $0 \leq k < \gcd(n, m)$ και $0 \leq r < n'$, τέτοια ώστε $j = kn' + r$. Επομένως, έχουμε

$$\begin{aligned}\prod_{j=0}^{n-1}(1 - \omega_n^{jm}u^m) = \prod_{j=0}^{n-1}(1 - \omega_{n'}^{j}u^m) &= \prod_{k=0}^{\gcd(n,m)-1}\left(\prod_{r=0}^{n'-1}(1 - \omega_{n'}^{kn'+r}u^m)\right) \\ &= \prod_{k=0}^{\gcd(n,m)-1}\left(\prod_{r=0}^{n'-1}(1 - \omega_{n'}^{r}u^m)\right) = \prod_{k=0}^{\gcd(n,m)-1}(1 - u^{mn'}) \\ &= (1 - u^{mn'})^{\gcd(n,m)} .\end{aligned}$$

Όμως $mn' = \frac{mn}{\gcd(m,n)} = \operatorname{lcm}(m, n)$, οπότε έχουμε το ζητούμενο. ♡

Τώρα είμαστε σε θέση να δείξουμε τη ζητούμενη σχέση για τη ζήτα.

Θεωρημα 4.2.3. *Αν ω_n είναι μια μιγαδική πρωταρχική n-στή ρίζα της μονάδας και $u := q^{-s}$, τότε για κάθε $u \in \mathbb{C}$ έχουμε ότι*

$$\zeta_{F_n}(s) = Z_{F_n}(u^n) = \prod_{j=0}^{n-1} Z_F(\omega_n^j u).$$

ΑΠΟΔΕΙΞΗ. Εφόσον από την πρόταση 3.2.3 το σώμα σταθερών του $F_n/\mathbb{F}_{q^n}$ είναι το $\mathbb{F}_{q^n}$ που έχει q^n το πλήθος στοιχεία, από τον ορισμό 4.1.9 έχουμε ότι

$$\zeta_{F_n}(s) = Z_{F_n}((q^n)^{-s}) = Z_{F_n}((q^{-s})^n) = Z_{F_n}(u^n).$$

Στη συνέχεια, από την (4.3) περιοριζόμενοι σε κατάλληλα s, παίρνουμε

$$\zeta_{F_n}(s) = \prod_{\mathfrak{P}\in\mathbb{P}_{F_n}} (1 - (N\mathfrak{P})^{-s})^{-1}. \tag{4.10}$$

Ακόμα, θέτοντας $d_P := \gcd(n, \deg_F P)$, έχουμε από τον ορισμό 4.1.7 και την πρόταση 4.2.1

$$N\mathfrak{P} := (q^n)^{\deg_{F_n}\mathfrak{P}} = q^{n\cdot\frac{\deg_F P}{d_P}} = (q^{\deg_F P})^{\frac{n}{d_P}} = (NP)^{\frac{n}{d_P}}. \tag{4.11}$$

Από τις σχέσεις (4.10) και (4.11) και τις προτάσεις 4.2.1 και 3.1.7 θα πάρουμε ότι

$$\begin{aligned}\zeta_{F_n}(s) &= \prod_{\mathfrak{P}\in\mathbb{P}_{F_n}} (1 - (N\mathfrak{P})^{-s})^{-1} = \prod_{P\in\mathbb{P}_F}\prod_{\substack{\mathfrak{P}\in\mathbb{P}_{F_n}\\ \mathfrak{P}|P}} (1 - (NP)^{-s\frac{n}{d_P}})^{-1}\\ &= \prod_{P\in\mathbb{P}_F} (1 - (NP)^{-s\frac{n}{d_P}})^{-d_P}. \qquad (4.12)\end{aligned}$$

Στη συνέχεια, από τον ορισμό 4.1.7, το λήμμα 4.2.2 και τις σχέσεις (4.5) και (4.12) έχουμε ότι

$$\begin{aligned}\zeta_{F_n}(s) &= \prod_{P\in\mathbb{P}_F} (1 - (NP)^{-s\frac{n}{d_P}})^{-d_P} = \prod_{P\in\mathbb{P}_F} (1 - q^{-s\frac{n\deg_F P}{d_P}})^{-d_P}\\ &= \prod_{P\in\mathbb{P}_F} \left(\left(1 - u^{\operatorname{lcm}(n,\deg_F P)}\right)^{\gcd(n,\deg_F P)}\right)^{-1}\\ &= \prod_{P\in\mathbb{P}_F} \left(\prod_{j=0}^{n-1}(1 - \omega_n^{j\deg_F P}u^{\deg_F P})\right)^{-1}\\ &= \prod_{j=0}^{n-1}\prod_{P\in\mathbb{P}_F} (1 - (\omega_n^j u)^{\deg_F P})^{-1} = \prod_{j=0}^{n-1} Z_F(\omega_n^j u). \qquad \heartsuit\end{aligned}$$

Στο πόρισμα 4.1.12 είδαμε ότι η συνάρτηση ζήτα επεκτείνεται αναλυτικά σε ολόκληρο το $\mathbb{C}$ με απλούς πόλους στα σημεία $s = 0$ και $s = 1$. Ακόμα, στο λήμμα 4.1.18 δείξαμε ότι η $\zeta_F(s)$ είναι ρητή συνάρτηση του q^{-s}, οπότε είναι περιοδική με περίοδο $2\pi i/\log q$. Επομένως, η ζήτα έχει άπειρους το πλήθος πόλους στις ευθείες $\Re s = 0$ και $\Re s = 1$ και μάλιστα, στη δεύτερη ευθεία, οι πόλοι της είναι τα σημεία $s = 1 + i\cdot\frac{2\pi m}{\log q}$, $m \in \mathbb{Z}$. Ακόμα, για την ευθεία αυτή ισχύει η παρακάτω πρόταση.

ΠΡΟΤΑΣΗ 4.2.4. *Η συνάρτηση ζήτα δεν μηδενίζεται στην ευθεία* $\{s \in \mathbb{C} \mid \Re s = 1\}$.

ΑΠΟΔΕΙΞΗ. Κατ' αρχάς παρατηρούμε ότι για κάθε $\theta \in \mathbb{R}$ έχουμε ότι

$$\begin{aligned} & 2(1+\cos\theta)^2 \geq 0 \\ \Rightarrow\ & 2(1+2\cos\theta+\cos^2\theta) \geq 0 \\ \Rightarrow\ & 2+4\cos\theta+2\cos^2\theta \geq 0 \\ \Rightarrow\ & 3+4\cos\theta+\cos 2\theta \geq 0\ . \end{aligned} \tag{4.13}$$

Ακόμα από την (4.3) έχουμε ότι αν $\sigma := \Re s$, $\tau := \Im s$ και $\sigma > 1$, τότε

$$\zeta_F(s) = \prod_{P\in\mathbb{P}_F} (1-(NP)^{-s})^{-1}$$

$$\Rightarrow\ \log\zeta_F(s) = -\sum_{P\in\mathbb{P}_F} \log(1-(NP)^{-s}).$$

Όμως, περιοριζόμενοι σε κατάλληλα x, έχουμε ότι

$$-\log(1-x) = \sum_{m=1}^{\infty} \frac{x^m}{m},$$

επομένως το τελευταίο μας δίνει ότι

$$\log\zeta_F(s) = \sum_{P\in\mathbb{P}_F}\sum_{m=1}^{\infty} m^{-1}(NP)^{-ms} = \sum_{P\in\mathbb{P}_F}\sum_{m=1}^{\infty} m^{-1}e^{-s\log(NP)^m},$$

δηλαδή

$$\Re\log\zeta_F(s) = \sum_{P\in\mathbb{P}_F}\sum_{m=1}^{\infty} m^{-1}(NP)^{-m\sigma}\cos(\tau\log((NP)^m).$$

Έτσι από το παραπάνω και την (4.13) έχουμε ότι

$$3\cdot\Re\log\zeta_F(\sigma) + 4\cdot\Re\log\zeta_F(\sigma+i\tau) + \Re\log\zeta_F(\sigma+2i\tau) \geq 0,$$

δηλαδή για κάθε $\sigma > 1$ και για κάθε $\tau \in \mathbb{R}$ έχουμε ότι

$$|\zeta_F(\sigma)|^3 \cdot |\zeta_F(\sigma+i\tau)|^4 \cdot |\zeta_F(\sigma+2i\tau)| \geq 1. \tag{4.14}$$

Έστω τώρα ότι δεν ισχύει η υπόθεση, δηλαδή ότι υπάρχει $\tau \in \mathbb{R}$ τέτοιο ώστε $\zeta_F(1+i\tau) = 0$. Από την (4.14) και τα σχόλια πριν την παρούσα Πρόταση έχουμε ότι $\tau \neq \frac{2k\pi}{\log q}$ για κάθε $k \in \mathbb{Z}$. Ακόμα, έχουμε ότι

$$\lim_{\sigma\to 1^+} \frac{\zeta_F(\sigma+i\tau)}{\sigma-1} = \lim_{\sigma\to 1^+} \frac{\zeta_F(\sigma+i\tau)-\zeta_F(1+i\tau)}{(\sigma+i\tau)-(1+i\tau)} = \zeta_F'(1+i\tau)$$

και αφού η ζ_F είναι αναλυτική στο $1+i\tau$, το

$$\lim_{\sigma\to 1^+} \frac{\zeta_F(\sigma+i\tau)}{\sigma-1}$$

θα είναι φραγμένο. Από το πόρισμα 4.1.12 έχουμε ότι η ζ_F έχει απλό πόλο στο $s=1$, άρα το

$$\lim_{\sigma\to 1^+} (\sigma-1)\zeta_F(\sigma)$$

είναι επίσης φραγμένο. Τέλος, αν το τ δεν ισούται με κάποιο περιττό πολλαπλάσιο του $\pi/\log q$, τότε και το

$$\lim_{\sigma\to 1^+} \zeta_F(\sigma + 2i\tau)$$

είναι φραγμένο σύμφωνα με τα σχόλια πριν την πρόταση αυτή. Όμως τα παραπάνω έρχονται σε αντίθεση με την (4.14).

Επομένως μας απομένει να μελετήσουμε την περίπτωση που το τ είναι περιττό πολλαπλάσιο του $\pi/\log q$. Σε αυτήν την περίπτωση $q^{-(1+i\tau)} = -q^{-1}$. Έτσι είναι προφανές από τον ορισμό της Ζήτα και του προηγούμενου ότι αρκεί να δείξουμε ότι $Z_F(-q^{-1}) \neq 0$. Όμως από τον ορισμό της Ζήτα και το θεώρημα 4.1.19 έχουμε ότι $Z_F(-q^{-1}) \neq 0$ ανν $Z_F(-1) \neq 0$. Επιπροσθέτως, από τον ορισμό της Ζήτα και το λήμμα 4.1.18, θα έχουμε ότι $Z_F(-1) \neq 0$ ανν $L_F(-1) \neq 0$. Όμως από το θεώρημα 4.2.3 παίρνουμε ότι

$$L_{F_2}(1) = L_F(1)L_F(-1)$$

και βάσει του λήμματος 4.1.18 η σχέση αυτή μας δίνει

$$L_F(-1) = \frac{h_{F_2}}{h_F} \neq 0. \qquad \heartsuit$$

Η παραπάνω πρόταση ισχύει και στην περίπτωση της κλασικής συνάρτησης ζήτα (βλέπε [Apo, §13.5]) και παίζει κεντρικό ρόλο στην απόδειξη του θεωρήματος των πρώτων αριθμών. Εμείς εδώ θα τη χρησιμοποιήσουμε, ώστε να αποδείξουμε εύκολα ένα αποτέλεσμα παρόμοιο με την υπόθεση Riemann, αλλά ασθενέστερο.

Πορισμα 4.2.5. *Υπάρχει κάποιος $\theta \in \mathbb{R}$, με $\theta < 1$, τέτοιος ώστε η ζήτα να μη μηδενίζεται στο ημιεπίπεδο $\{s \in \mathbb{C} \mid \Re s > \theta\}$.*

Αποδειξη. Από την πρόταση 4.1.10 βλέπουμε ότι η ζήτα αναπαριστάται από ένα μη μηδενικό συγκλίνον απειρογινόμενο για $\Re s > 1$, δεν έχει ρίζες στην περιοχή $\{s \in \mathbb{C} \mid \Re s > 1\}$. Αυτό, σε συνδυασμό με την 4.2.4 μας λέει ότι η ζήτα δεν έχει ρίζες στην περιοχή $\{s \in \mathbb{C} \mid \Re s \geq 1\}$. Το συμπέρασμα αυτό, σε συνδυασμό με το θεώρημα 4.1.19, μας λέει ότι η ζήτα δε μηδενίζεται επίσης στην περιοχή $\{s \in \mathbb{C} \mid \Re s \leq 0\}$.

Ακόμα, όπως είδαμε στα σχόλια πριν την πρόταση 4.2.4, η ζήτα είναι περιοδική με περίοδο $2\pi i/\log q$, άρα συνδυάζοντας και το παραπάνω αρκεί να αναζητήσουμε τις ρίζες της ζήτα στο σύνολο

$$A := \{s \in \mathbb{C} \mid 0 \leq \Re s \leq 1 \text{ και } 0 \leq \Im s \leq 2\pi i/\log q\}.$$

Όμως, η ζήτα είναι μη μηδενική και αναλυτική, δηλαδή το σύνολο των ριζών της δεν μπορεί να έχει σημείο συσσώρευσης. Αυτό, σε συνδυασμό με το ότι το A είναι συμπαγές, μας δίνει ότι το πλήθος των ριζών της ζήτα στο A είναι πεπερασμένο. Έτσι το ζητούμενο έπεται άμεσα. $\heartsuit$

Πριν φτάσουμε στο κεντρικό θεώρημα της παραγράφου αυτής, ας δούμε τι ακριβώς σημαίνει το παραπάνω πόρισμα για το πολυώνυμο $L_F(u)$.

Από το λήμμα 4.1.18 έχουμε ότι υπάρχουν κάποια ρ_j, με $j = 1, \dots, 2g$ τέτοια ώστε

$$L_F(u) = \prod_{j=1}^{2g}(1 - \rho_j u) \tag{4.15}$$

και χρησιμοποιώντας το πόρισμα 4.2.5 παίρνουμε ότι

$$|\rho_j| \leq q^{\theta} \tag{4.16}$$

για κάθε $j = 1, \dots, 2g$, με θ τη σταθερά του πορίσματος 4.2.5. Ας δούμε τώρα το κεντρικό θεώρημα αυτής της παραγράφου.

Θεωρημα 4.2.6 (Πρώτων Αριθμών – Ασθενής Μορφή). *Υπάρχει κάποιος $\theta \in \mathbb{R}$, με $\theta < 1$, τέτοιος ώστε*

$$a_N = \frac{q^N}{N} + O\left(\frac{q^{\theta N}}{N}\right).$$

Αποδειξη. Συνδυάζοντας τον ορισμό της Ζήτα, το λήμμα 4.1.18 και τις σχέσεις (4.4) και (4.15) έχουμε ότι

$$\frac{\prod_{j=1}^{2g}(1 - \rho_j u)}{(1-u)(1-qu)} = \prod_{d=1}^{\infty}(1 - u^d)^{-a_d}.$$

Από την παραπάνω σχέση παίρνουμε διαδοχικά ότι

$$-\log(1-u) - \log(1-qu) + \sum_{j=1}^{2g}\log(1 - \rho_j u) = -\sum_{d=1}^{\infty} a_d \log(1 - u^d)$$

και

$$\frac{1}{1-u} + \frac{q}{1-qu} - \sum_{j=1}^{2g}\frac{\rho_j}{1 - \rho_j u} = \sum_{d=1}^{\infty} a_d \frac{du^{d-1}}{1 - u^d}$$

δηλαδή

$$\frac{u}{1-u} + \frac{qu}{1-qu} - \sum_{j=1}^{2g}\frac{\rho_j u}{1 - \rho_j u} = \sum_{d=1}^{\infty} d a_d \frac{u^d}{1 - u^d}.$$

Όμως για μικρά x ισχύει ότι $\frac{x}{1-x} = \sum_{k=1}^{\infty} x^k$. Έτσι το τελευταίο μας δίνει

$$\sum_{k=1}^{\infty} u^k + \sum_{k=1}^{\infty}(qu)^k - \sum_{j=1}^{2g}\sum_{k=1}^{\infty}(\rho_j u)^k = \sum_{d=1}^{\infty}\sum_{k=1}^{\infty} d a_d u^{dk}$$

το οποίο μας δίνει με τη σειρά του ότι για κάθε $N \geq 1$ ισχύει ότι

$$1 + q^N - \sum_{j=1}^{2g}\rho_j^N = \sum_{d|N} d a_d.$$

Από τον τύπο αντιστροφής του Möbius[3] το τελευταίο ισοδυναμεί με το

$$Na_N = \sum_{d|N} \mu(d) q^{N/d} + \sum_{d|N} \mu(d) + \sum_{d|N} \mu(d) \left(\sum_{j=1}^{2g} \rho_j^{N/d} \right),$$

όπου μ η συνάρτηση Möbius[4], και μιας που $\sum_{d|N} \mu(d) = 0$ για $N \geq 1$, από το [Apo, ϑ. 2.1], το τελευταίο μας δίνει

$$Na_N = \sum_{d|N} \mu(d) q^{N/d} + \sum_{d|N} \mu(d) \left(\sum_{j=1}^{2g} \rho_j^{N/d} \right). \tag{4.17}$$

Όμως είναι προφανές από τον ορισμό της συνάρτησης Möbius ότι

$$\sum_{d|N} \mu(d) q^{N/d} = q^N + O(q^{N/2}). \tag{4.18}$$

Ακόμα, από τον ορισμό της συνάρτησης Möbius και την (4.16) έχουμε ότι

$$\left| \sum_{d|N} \mu(d) \left(\sum_{j=1}^{2g} \rho_j^{N/d} \right) \right| \leq 2g q^{\theta N} + 2gN q^{\theta N/2}. \tag{4.19}$$

Τέλος, λαμβάνοντας υπ᾽ όψιν ότι βάσει του ϑεωρήματος 4.1.19 για τη σταθερά θ του πορίσματος 4.2.5, που ταυτίζεται με τη σταθερά θ της (4.19) και ισχύει ότι $\frac{1}{2} \leq \theta < 1$, παίρνουμε από τις σχέσεις (4.17), (4.18) και (4.19) ότι

$$Na_N = q^N + O(q^{\theta N}),$$

από το οποίο το ζητούμενο έπεται άμεσα. ♡

4.3. Το ϑεώρημα Hasse-Weil

Το κεντρικό ϑεώρημα της παραγράφου αυτής είναι το ϑεώρημα Hasse-Weil ή αλλιώς η υπόθεση Riemann για σώματα συναρτήσεων. Το ϑεώρημα εικάζεται για πρώτη φορά από τον Artin στη διατριβή του και αποδεικνύεται για μερικές μόνο περιπτώσεις, από τον Hasse τη δεκαετία του ᾽40. Στα τέλη της ίδιας δεκαετίας ο Weil στο [Wei] αποδεικνύει τη γενική περίπτωση με χρήση προχωρημένης αλγεβρικής γεωμετρίας. Μια σχετικά απλή απόδειξη δόθηκε από τον W. Schmidt που βασίστηκε σε ιδέες του Stepanov περίπου 20 χρόνια αργότερα από εκείνη του Weil. Την απόδειξη αυτή απλοποίησε ακόμα περισσότερο ο Bombieri στο [Bom]. Η

[3] Ο τύπος αντιστροφής του Möbius λέει ότι

$$f(n) = \sum_{d|n} g(d) \iff g(n) = \sum_{d|n} \mu(d) f(n/d),$$

όπου μ η συνάρτηση Möbius. Για την απόδειξη του τύπου παραπέμπουμε στο [Apo, ϑ. 2.9].

[4] Για τον ορισμό και βασικές ιδιότητες της συνάρτησης Möbius δες [Apo, §2.2].

απόδειξη που θα δώσουμε στο κείμενο αυτό είναι κατά βάση εκείνη του Bombieri.

Στην παράγραφο αυτή διατηρούμε τους συμβολισμούς και τις συμβάσεις των προηγούμενων παραγράφων αυτού του κεφαλαίου. Το θεώρημα που θα αποδείξουμε είναι το παρακάτω.

ΘΕΩΡΗΜΑ 4.3.1 (Hasse-Weil). *Όλες οι ρίζες της συνάρτησης ζήτα βρίσκονται πάνω στην ευθεία* $\{s \in \mathbb{C} \mid \Re s = 1/2\}$.

Μια εναλλακτική διατύπωση σύμφωνα με ό,τι αποδείθχηκε στις προηγούμενες παραγράφους, θα ήταν ότι

$$|\rho_j| = q^{1/2} \quad \text{για κάθε} \quad j = 1, \ldots, 2g. \tag{4.20}$$

Ας ξεκινήσουμε τώρα την απόδειξη.

ΛΗΜΜΑ 4.3.2. *Έστω* $m \in \mathbb{Z}_{>0}$. *Το θεώρημα Hasse-Weil ισχύει για το* $F/\mathbb{F}$ *αν ισχύει για το* $F_m/\mathbb{F}_{q^m}$.

ΑΠΟΔΕΙΞΗ. Αν ω_m είναι μια μιγαδική m-στή ρίζα της μονάδας, τότε από το θεώρημα 4.2.3 και το λήμμα 4.2.2 έχουμε ότι

$$\begin{aligned} L_{F_m}(t^m) &= (1-t^m)(1-q^m t^m) Z_{F_m}(t^m) \\ &= (1-t^m)(1-q^m t^m) \prod_{j=0}^{m-1} Z_F(\omega_m^j t) \\ &= (1-t^m)(1-q^m t^m) \prod_{j=0}^{m-1} \frac{L_F(\omega_m^j t)}{(1-\omega_m^j t)(1-q\omega_m^j t)} \\ &= \prod_{j=0}^{m-1} L_F(\omega_m^j t) = \prod_{i=1}^{2g} \prod_{j=0}^{m-1} (1-\rho_i \omega_m^j t) = \prod_{i=1}^{2g} (1-\rho_i^m t^m). \end{aligned}$$

Άρα $L_{F_m}(u) = \prod_{i=1}^{2g}(1-\rho_i^m u)$, οπότε, το ζητούμενο έπεται άμεσα, αφού για κάθε $j = 1, \ldots, 2g$ έχουμε ότι

$$|\rho_j| = q^{1/2} \iff |\rho_j^m| = (q^m)^{1/2}. \qquad \heartsuit$$

Στο παραπάνω λήμμα δείξαμε ότι αρκεί να δείξουμε το θεώρημα Hasse-Weil για κάποια επέκταση σταθερού σώματος του $F/\mathbb{F}$. Ας δούμε τώρα ένα ακόμα χρήσιμο λήμμα.

ΛΗΜΜΑ 4.3.3. *Αν υπάρχει κάποιο* $c \in \mathbb{R}$ *τέτοιο ώστε για κάθε* $r \geq 1$ *να ισχύει ότι*

$$|a_{F_r,1} - (q^r + 1)| \leq c q^{r/2},$$

τότε ισχύει το θεώρημα Hasse-Weil για το $F/\mathbb{F}$.

ΑΠΟΔΕΙΞΗ. Έστω ότι ισχύει η αναφερόμενη συνθήκη. Από την απόδειξη του προηγούμενου λήμματος έχουμε ότι για κάθε $r \geq 1$ ισχύει ότι $L_{F_r}(u) = \prod_{i=1}^{2g}(1-\rho_i^r u)$, οπότε αν αναπτύξουμε το γινόμενο αυτό βλέπουμε ότι ο συντελεστής του u είναι $-\sum_{i=1}^{2g} \rho_i^r$, οπότε $L'_{F_r}(0) = -\sum_{i=1}^{2g} \rho_i^r$.

Έτσι από το λήμμα 4.1.18 έχουμε ότι $a_{F_r,1} - (q^r + 1) = -\sum_{i=1}^{2g} \rho_i^r$, άρα σύμφωνα με την υπόθεση θα έχουμε ότι

$$\left| \sum_{i=1}^{2g} \rho_i^r \right| \leq cq^{r/2}. \tag{4.21}$$

Ακόμα θεωρούμε τη συνάρτηση

$$H(t) := \sum_{i=1}^{2g} \frac{\rho_i t}{1 - \rho_i t}. \tag{4.22}$$

Θέτουμε $\mu := \min\{|\rho_i^{-1}| \mid 1 \leq i \leq 2g\}$. Από την (4.22) η ακτίνα σύγκλισης της δυναμοσειράς της $H(t)$ γύρω από το 0 είναι ακριβώς μ. Ακόμα, για $|t| < \mu$ έχουμε ότι

$$H(t) = \sum_{i=1}^{2g} \sum_{r=1}^{\infty} (\rho_i t)^r = \sum_{r=1}^{\infty} \left(\sum_{i=1}^{2g} \rho_i^r \right) t^r.$$

Όμως, από την (4.21), η τελευταία δυναμοσειρά συγκλίνει[5] για $|t| < q^{-1/2}$. Από αυτά παίρνουμε ότι $q^{-1/2} \leq \mu$, δηλαδή

$$q^{1/2} \geq |\rho_i| \quad \text{για κάθε} \quad i = 1, \ldots, 2g. \tag{4.23}$$

Όμως από τη συναρτησιακή εξίσωση της ζήτα έχουμε ότι το s είναι ρίζα της ζήτα ανν και το $1 - s$ είναι ρίζα της ζήτα. Αυτό σημαίνει ότι το u είναι ρίζα του L_F ανν το $1/qu$ είναι ρίζα του L_F. Έτσι οι ($2g$ το πλήθος) ρίζες έχουν ανά δύο γινόμενο q^{-1}, οπότε το γινόμενο των (g το πλήθος) ζευγών ριζών που ισούται με το γινόμενο των ριζών, είναι ίσο με q^{-g}. Από αυτό, αλλά και από το γεγονός ότι τα ρ_j είναι τα αντίστροφα των ριζών της ζήτα παίρνουμε ότι

$$\prod_{j=1}^{2g} \rho_j = q^g. \tag{4.24}$$

Από τις (4.23) και (4.24) παίρνουμε ότι $|\rho_j| = q^{1/2}$ για κάθε $j = 1, \ldots, 2g$. ♡

Το παραπάνω λήμμα ουσιαστικά μας καθοδηγεί στην αναζήτηση κάποιων σταθερών $c_1, c_2 \in \mathbb{R}_{>0}$ τέτοιων ώστε

$$a_{F_r,1} - (q^r + 1) \leq c_1 q^{r/2}$$

και

$$a_{F_r,1} - (q^r + 1) \geq -c_2 q^{r/2}$$

για κάθε $r \geq 1$. Η επόμενη πρόταση μας δίνει έμμεσα την πρώτη ανισότητα.

[5] Χωρίς όμως κατ' ανάγκη αυτό να είναι και η ακτίνα σύγκλισης.

ΠΡΟΤΑΣΗ 4.3.4. *Αν το q είναι τετράγωνο $> (g+1)^4$, τότε*

$$a_1 - (q+1) < (2g+1)q^{1/2}.$$

ΑΠΟΔΕΙΞΗ. Αν $a_1 = 0$, τότε η ισχύς της πρότασης είναι προφανής. Αν $a_1 > 0$, τότε υπάρχει κάποιο $Q \in \mathbb{P}_F$, με $\deg Q = 1$. Θέτουμε $q_0 := \sqrt{q}$, $m := q_0 - 1$ και $n := 2g + q_0$. Από τις υποθέσεις είναι προφανές ότι οι παραπάνω αριθμοί είναι θετικοί ακέραιοι. Ακόμα, εύκολα βλέπουμε ότι για τον $r := q - 1 + (2g+1)q^{1/2}$ έχουμε ότι

$$r = m + nq_0. \tag{4.25}$$

Στη συνέχεια θεωρούμε το χώρο

$$\mathcal{L} := \mathcal{L}(mQ)\mathcal{L}(nQ)^{q_0},$$

που αποτελείται από όλα τα πεπερασμένα αθροίσματα της μορφής $\sum x_\nu y_\nu^{q_0}$, με $x_\nu \in \mathcal{L}(mQ)$ και $y_\nu \in \mathcal{L}(nQ)$. Από τις ιδιότητες της συνάρτησης ord_Q ως διακριτής αποτίμησης, εύκολα παρατηρούμε ότι κάθε τέτοιο άθροισμα ανήκει και στο $\mathcal{L}(rQ)$, δηλαδή

$$\mathcal{L} \subseteq \mathcal{L}(rQ). \tag{4.26}$$

Έστω τώρα ότι υπάρχει κάποιο $x \in \mathcal{L} \setminus \{0\}$, τέτοιο ώστε όλοι οι πρώτοι του $F/\mathbb{F}$ βαθμού 1, εκτός του Q, να είναι ρίζες του. Από την ιδιότητα του x να έχει ως ρίζες του όλους τους πρώτους βαθμού 1, εκτός από τον Q εύκολα συμπεραίνουμε ότι

$$(x)_0 \geq \sum_{\substack{P \in \mathbb{P}_F \\ \deg P = 1,\, P \neq Q}} P \quad \Rightarrow \quad \deg(x)_0 \geq a_1 - 1.$$

Ακόμα, από το ότι $x \in \mathcal{L}$, από την (4.26) και τον ορισμό των $\mathcal{L}$-χώρων παίρνουμε ότι

$$(x)_\infty \leq rQ \quad \Rightarrow \quad \deg(x)_\infty \leq r.$$

Όμως εξ ορισμού $r = q - 1 + (2g+1)q^{1/2}$ και $\deg(x)_0 = \deg(x)_\infty$ από το θεώρημα 1.3.13, έτσι οι δύο τελευταίες σχέσεις μας δίνουν

$$a_1 - 1 \leq q - 1 + (2g+1)q^{1/2} \quad \Rightarrow \quad a_1 - (q+1) < (2g+1)q^{1/2}.$$

Έτσι, βλέπουμε ότι αρκεί να αποδείξουμε την ύπαρξη κάποιου $x \in \mathcal{L} \setminus \{0\}$ τέτοιου ώστε όλοι οι πρώτοι του $F/\mathbb{F}$ βαθμού 1, εκτός του Q, να είναι ρίζες του. Αυτό θα το κάνουμε σε τέσσερα βήματα.

Βήμα 1ο Αν

$$T := \{i \in \mathbb{Z} \mid 0 \leq i \leq m \text{ και } \exists\, x \in F \text{ τέτοιο ώστε } (x)_\infty = iQ\}$$

και για κάθε $i \in T$ επιλέξουμε κάποιο $u_i \in F \setminus \{0\}$, τέτοιο ώστε $(u_i)_\infty = iQ$, τότε το σύνολο $\{u_i \mid i \in T\}$ είναι μια $\mathbb{F}$-βάση του $\mathcal{L}(mQ)$.

Κατ᾽ αρχάς παρατηρούμε ότι $m = \sqrt{q} - 1$, οπότε αφού από την υπόθεση $q > (g+1)^4$ θα έχουμε ότι $m > g^2 + 2g \geq 2g - 1$, επομένως από το θεώρημα Riemann θα έχουμε

$$l(mQ) = m + 1 - g.$$

Ακόμα, εκμεταλλευόμενοι πάλι το γεγονός ότι $m > 2g$, από το θεώρημα κενών του Weierstraß (βλέπε [Sti, θ. I.6.7]), θα πάρουμε ότι

$$|T| = m + 1 - g.$$

Έτσι από τις δύο τελευταίες σχέσεις έχουμε ότι

$$\dim_{\mathbb{F}} \mathcal{L}(mQ) = |\{u_i \mid i \in T\}|$$

και αφού $\{u_i \mid i \in T\} \subseteq \mathcal{L}(mQ)$, αρκεί να δείξουμε ότι τα στοιχεία του $\{u_i \mid i \in T\}$ είναι $\mathbb{F}$-γραμμικά ανεξάρτητα. Έστω λοιπόν ότι $k_i \in \mathbb{F}$, με $i \in T$, τέτοια ώστε

$$\sum_{i \in T} k_i u_i = 0.$$

Αυτό σημαίνει ότι

$$\mathrm{ord}_Q \left(\sum_{i \in T} k_i u_i \right) = \infty.$$

Ακόμα από την ισχυρή τριγωνική ανισότητα θα πάρουμε ότι αν για κάποια $i \in T$ ισχύει ότι $k_i \neq 0$, τότε

$$\mathrm{ord}_Q \left(\sum_{i \in T} k_i u_i \right) = -\max\{i \in T \setminus \{0\} \mid k_i \neq 0\} \neq \infty.$$

Απο τις δύο τελευταίες σχέσεις παίρνουμε ότι $k_i = 0$ για κάθε $i \in T$.

Βήμα 2ο Κάθε $y \in \mathcal{L}$ γράφεται κατά μοναδικό τρόπο στη μορφή

$$y = \sum_{i \in T} u_i z_i^{q_0} \quad \text{με} \quad z_i \in \mathcal{L}(nQ).$$

Η ύπαρξη αυτής της γραφής είναι άμεσο αποτέλεσμα του πρώτου βήματος και του ορισμού του $\mathcal{L}$. Για να αποδείξουμε τη μοναδικότητα, αρκεί να δείξουμε ότι αν

$$\sum_{i \in T} u_i x_i^{q_0} = 0, \tag{4.27}$$

τότε $x_i = 0$ για κάθε $i \in T$. Έστω λοιπόν ότι υπάρχουν κάποια $i \in T$, με $x_i \neq 0$. Τότε για τα i αυτά θα έχουμε ότι

$$\mathrm{ord}_Q(u_i x_i^{q_0}) \equiv \mathrm{ord}_Q(u_i) \equiv -i \pmod{q_0}.$$

Ακόμα $m = q_0 - 1$, επομένως οι αριθμοί $i \in T$ είναι ανά δύο διάφοροι modulo q_0, άρα από την ισχυρή τριγωνική ανισότητα θα πάρουμε ότι

$$\mathrm{ord}_Q \left(\sum_{i \in T} u_i x_i^{q_0} \right) = \min\{\mathrm{ord}_Q(u_i x_i^{q_0}) \mid i \in T\} \neq \infty,$$

που είναι άτοπο.

Βήμα 3ο Η απεικόνιση

$$\lambda : \begin{array}{ccc} \mathcal{L} & \to & \mathcal{L}((q_0 m + n)Q) \\ \sum_{i \in T} u_i z_i^{q_0} & \mapsto & \sum_{i \in T} u_i^{q_0} z_i \end{array},$$

με $z_i \in \mathcal{L}(nQ)$ είναι ομομορφισμός των κατάλληλων προσθετικών ομάδων και $\ker \lambda \neq \{0\}$.

Το δεύτερο βήμα μας εξασφαλίζει το ότι η απεικόνιση είναι καλά ορισμένη και το γεγονός ότι πρόκειται για ομομορφισμό των προσθετικών ομάδων είναι προφανές. Επομένως, μας απομένει να δείξουμε ότι $\ker \lambda \neq \{0\}$. Από τα παραπάνω μας αρκεί να δείξουμε ότι

$$\dim_{\mathbb{F}} \mathcal{L} > \dim_{\mathbb{F}} \mathcal{L}((q_0 m + n)Q).$$

Από τα δύο πρώτα βήματα και την ανισότητα Riemann θα έχουμε ότι

$$\dim_{\mathbb{F}} \mathcal{L} = l(mQ) \cdot l(nQ) \geq (m + 1 - g)(n + 1 - g).$$

Επιπροσθέτως, εφόσον ισχύει ότι

$$\deg((q_0 m + n)Q) = q_0 m + n = q_0(q_0 - 1) + (2g + q_0) = 2g + q,$$

από το θεώρημα 2.3.3 και το θεώρημα Riemann, θα έχουμε ότι

$$\begin{aligned} \dim_{\mathbb{F}} \mathcal{L}((q_0 m + n)Q) &=: l((q_0 m + n)Q) \\ &= (2g + q) + 1 - g \\ &= g + q + 1. \end{aligned}$$

Έτσι από τα παραπάνω μας αρκεί να δείξουμε ότι

$$(m + 1 - g)(n + 1 - g) > g + q + 1.$$

Πράγματι, έχουμε διαδοχικά

$$\begin{aligned} & (m + 1 - g)(n + 1 - g) > g + q - 1 \\ \iff & (q_0 - g)(2g + q_0 + 1 - g) > g + q - 1 \\ \iff & q - g^2 + q_0 - g > g + q + 1 \\ \iff & q_0 > g^2 + 2g + 1 \\ \iff & q_0 > (g + 1)^2 \\ \iff & q > (g + 1)^4 \end{aligned}$$

και το τελευταίο ισχύει από την υπόθεση.

Βήμα 4ο Αν $x \in \ker \lambda \setminus \{0\}$, τότε όλοι οι πρώτοι του $F/\mathbb{F}$ βαθμού 1, εκτός του Q, είναι ρίζες του x.

Έστω $P \in \mathbb{P}_{\mathbb{F}}$, με $P \neq Q$ και $\deg P = 1$. Αν $y \in \mathcal{L} \setminus \{0\}$, τότε από τον ορισμό του $\mathcal{L}$, το y θα έχει ως μοναδικό του πόλο τον Q, δηλαδή $\mathrm{ord}_P(y) \geq 0$ και από το θεώρημα 1.2.10(α′) θα έχουμε ότι $y \in \mathcal{O}_P$. Έτσι $\mathcal{L} \subseteq \mathcal{O}_P$. Ακόμα, μιας και $\deg P = 1$ από τον ορισμό του βαθμού ενός πρώτου, θα έχουμε ότι ${}^{\mathcal{O}_P}/_{P} = \mathbb{F}$. Έτσι, συνδυάζοντας τα παραπάνω με γνωστό αποτέλεσμα της θεωρίας πεπερασμένων σωμάτων, θα πάρουμε ότι

$$\bar{y}^p = \bar{y} \quad \text{για κάθε} \quad y \in \mathcal{L}. \tag{4.28}$$

Τονίζουμε ότι με πανομοιότυπο τρόπο μπορούμε να δείξουμε ότι όλα τα παραπάνω ισχύουν και για τα $\mathcal{L}(nQ)$ και $\mathcal{L}(mQ)$. Έστω τώρα κάποιο $x \in \ker \lambda \setminus \{0\}$. Η ύπαρξη τέτοιου x εξασφαλίζεται από το τρίτο βήμα.

Από το δεύτερο βήμα θα υπάρχει κάποια μοναδική γραφή $x = \sum_{i\in T} u_i z_i^{q_0}$, με $z_i \in \mathcal{L}(nQ)$. Έτσι από την (4.28), μιας που το q_0 είναι πολλαπλάσιο του p, θα πάρουμε ότι

$$\begin{aligned}\bar{x}^{q_0} &= \left(\sum_{i\in T} \bar{u}_i \bar{z}_i^{q_0}\right)^{q_0} = \sum_{i\in T} \bar{u}_i{}^{q_0} \bar{z}_i{}^{q} = \sum_{i\in T} \bar{u}_i{}^{q_0} \bar{z}_i \\ &= \overline{\sum_{i\in T} u_i^{q_0} z_i} = \overline{\lambda(x)} = \bar{0},\end{aligned}$$

δηλαδή $\bar{x} = \bar{0}$, οπότε το P είναι ρίζα του x. ♡

Η παραπάνω πρόταση μας δείχνει ότι, αν θεωρήσουμε κάποια επέκταση σταθερού σώματος του $F/\mathbb{F}$, δεδομένου ότι το γένος δεν αλλάζει, λόγω της πρότασης 3.2.8, μπορούμε να πάρουμε ένα άνω φράγμα, όπως αυτό απαιτήθηκε στα σχόλια μετά το λήμμα 4.3.3. Ας δούμε τώρα το ζητούμενο κάτω φράγμα.

Πρόταση 4.3.5. *Υπάρχουν σταθερές σταθερά $c_1, c_2 \in \mathbb{R}_{>0}$, που εξαρτώνται αποκλειστικά από το $F/\mathbb{F}$, τέτοιες ώστε αν q τετράγωνο και $q > c_1$, τότε για κάθε $r \geq 1$ ισχύει ότι*

$$a_{F_r,1} - (q^r + 1) > -c_2 q^{r/2}.$$

Απόδειξη. Για την απόδειξη δες [Sti, σελ. 174–178], [Ros, σελ. 335–336] ή [Bom]. ♡

Η απόδειξη της παραπάνω πρότασης κάνει χρήση επεκτάσεων Galois, που δεν μελετήσαμε στο κείμενο αυτό. Ακόμα, η πρόταση αυτή, μαζί με την πρόταση 4.3.4 και τα λήμματα 4.3.2 και 4.3.3 είναι τα κομμάτια ενός «παζλ», η «συναρμολόγηση» του οποίου, όπως θα δούμε, αποτελεί την απόδειξη του θεωρήματος Hasse-Weil.

Ολοκλήρωση της απόδειξης. Θέτουμε $C := \max\{(g+1)^4, c_1\}$ (όπου c_1 η αντίστοιχη σταθερά της πρότασης 4.3.5) και παρατηρούμε ότι είναι προφανές ότι μπορεί να βρεθεί κάποιο $s \geq 1$ τέτοιο ώστε το q^s να είναι τετράγωνο και $q^s > C$.

Θέτουμε $Y := \max\{2g+1, c_2\}$ και από την πρόταση 3.2.8 έχουμε ότι για κάθε $r \geq 1$ το γένος του $F_r/\mathbb{F}_{q^r}$ είναι g, επομένως για κάθε r θετικό ακέραιο πολλαπλάσιο του s ικανοποιούνται οι υποθέσεις της πρότασης 4.3.4 και άρα για κάθε r θετικό ακέραιο πολλαπλάσιο του s έχουμε ότι

$$a_{F_r,1} - (q^r + 1) < (2g+1) q^{r/2} \leq Y q^{r/2}. \tag{4.29}$$

Ακόμα, από την πρόταση 4.3.5 έχουμε ότι για κάθε r θετικό ακέραιο πολλαπλάσιο του s ισχύει ότι

$$a_{F_r,1} - (q^r + 1) > -c_2 q^{r/2} \geq Y q^{r/2}. \tag{4.30}$$

Συνδυάζοντας τις (4.29) και (4.30) καταλήγουμε ότι για κάθε r θετικό ακέραιο πολλαπλάσιο του s ισχύει ότι

$$|a_{F_r,1} - (q^r + 1)| < Y q^{r/2},$$

δηλαδή το $F_s/\mathbb{F}_{q^s}$ ικανοποιεί τις προϋποθέσεις του λήμματος 4.3.3. Έτσι από το λήμμα 4.3.3 ισχύει το θεώρημα Hasse-Weil για το $F_s/\mathbb{F}_{q^s}$.

Τέλος, εφόσον ισχύει το θεώρημα Hasse-Weil για το $F_s/\mathbb{F}_{q^s}$ θα ισχύει και για το $F/\mathbb{F}$, από το λήμμα 4.3.2. Αυτό ολοκληρώνει την απόδειξή μας!

4.4. Μερικές συνέπειες του θεωρήματος Hasse-Weil

Κλείνουμε την εργασία αυτή με κάποιες ενδιαφέρουσες συνέπειες του θεωρήματος Hasse-Weil. Ξεκινάμε με την ισχυρή μορφή του θεωρήματος των πρώτων αριθμών.

ΘΕΩΡΗΜΑ 4.4.1 (Πρώτων Αριθμών – Ισχυρή Μορφή). *Ισχύει ότι*

$$a_N = \frac{q^N}{N} + O\left(\frac{q^{N/2}}{N}\right).$$

ΑΠΟΔΕΙΞΗ. Από τον ορισμό της συνάρτησης Möbius και το θεώρημα Hasse-Weil έχουμε ότι

$$\left|\sum_{d|N} \mu(d)\left(\sum_{j=1}^{2g} \rho_j^{N/d}\right)\right| \leq 2gq^{N/2} + 2gNq^{N/4}.$$

Η ανισότητα αυτή, σε συνδυασμό με τις σχέσεις (4.17) και (4.18), συνεπάγεται ότι

$$Na_N = q^N + O(q^{N/2}),$$

απ᾽ όπου το ζητούμενο έπεται άμεσα. ♡

Μία ακόμα συνέπεια του θεωρήματος Hasse-Weil είναι το φράγμα Hasse-Weil.

ΘΕΩΡΗΜΑ 4.4.2 (Φράγμα Hasse-Weil). *Ισχύει ότι*

$$|a_1 - (q+1)| \leq 2gq^{1/2}.$$

ΑΠΟΔΕΙΞΗ. Από το λήμμα 4.1.18 έχουμε ότι $L'_F(0) = a_1 - (1+q)$. Ακόμα, από τη σχέση (4.15) έχουμε ότι $L'_F(0) = -\sum_{j=1}^{2g} \rho_j$. Έτσι, τα παραπάνω μας δίνουν ότι

$$|a_1 - (1+q)| = \left|\sum_{j=1}^{2g} \rho_j\right| \leq \sum_{j=1}^{2g} |\rho_j|$$

και το τελευταίο σε συνδυασμό με το θεώρημα Hasse-Weil, μας δίνει ότι

$$|a_1 - (q+1)| \leq 2gq^{1/2}.$$ ♡

Βιβλιογραφία

[Apo] Apostol Tom, *Εισαγωγή στην Αναλυτική Θεωρία των Αριθμών* (μετάφραση Ανδρέας & Ελένη Ζαχαρίου), Gutenberg, Αθήνα, 1986.

[Ash] Ash Robert, *Abstract Algebra: The Basic Graduate Year*, 2000.
`http://www.math.uiuc.edu/~r-ash/Algebra.html`

[Bom] Bombieri Enrico, "Counting Points on Curves Over Finite Fields", *Séminaire Bourbaki, n^o 430*, p. 234-241, 1973.

[Jam] Jameson Graham, *The Prime Number Theorem*, Cambridge University Press, Cambridge, 2003.

[Mor] Morandi Patrick, *Field and Galois Theory*, Springer, New York, 1996.

[Mur] Murty Ram, *Problems in Analytic Number Theory*, Springer, New York, 2001.

[Neu] Neukirch Jürgen, *Algebraic Number Theory* (translated by Nobert Schappacher), Springer-Verlag, Berlin Heidelberg New York, 1999.

[Rei] Reid Miles, *Udergraduate Commutative Algebra*, Cambridge University Press, Cambridge, 1995.

[Ros] Rosen Michael, *Number Theory in Function Fields*, Springer, New York, 2002.

[Sch] Schmidt Friedrich Karl, "Analytische Zahlentheorie in Körpern der Charakteristik p", *Mathematische Zeitschrift, vol. 33, n^o 1*, p. 1–32, 1931.

[Ser] Serre Jean-Pierre, *Local Fields* (translated by Marvin Greenberg), Springer-Verlag, New York, 1979.

[Sha] Sharp Rodney, *Steps in Commutative Algebra*, Cambridge University Press, Cambridge, 2000.

[Sti] Stichtenoth Henning, *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin Heidelberg, 1993.

[Wei] Weil André, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Hermann, Paris, 1948.

[Ανδ] Ανδρεαδάκης Στυλιανός, *Γραμμική Άλγεβρα*, Συμμετρία, Αθήνα, 1991.

[Για] Γιανναkούλιας Ευστάθιος, Γιωτόπουλος Σταύρος και Νεγρεπόντης Στυλιανός, *Απειροστικός Λογισμός*, Συμμετρία, Αθήνα, 1993.

Ευρετήριο