Κουμουτση Σοφια

Αλγεβρικα Σωματα Συναρτησεων

και γεωμετρικοι κωδικες Goppa

Μεταπτυχιακη Εργασια

Πανεπιστήμιο Αιγαίου, Τμήμα Μαθηματικών

Σάμος Νοέμβριος 2005.

Εισηγητης: Κοντογεώργης Αριστείδης

Επιτροπη

Ανούσης Μιχάλης, καθηγητής,
Κοντογεώργης Αριστείδης, λέκτορας,
Τσολομύτης Αντώνης, λέκτορας

Η εργασία αυτή αφιερώνεται
στον σύζυγο μου Βαγγέλη
και στις κόρες μου
Ιάσμη και Ιωάννα.

Περιεχόμενα

Εισαγωγή

Το κύριο θέμα της πτυχιακής αυτής εργασίας είναι οι γεωμετρικοί κώδικες Goppa, τους οποίους για να ορίσουμε και να δώσουμε τις κυριότερες ιδιότητες τους, κρίναμε σκόπιμο να παρουσιάσουμε πρώτα τις μαθηματικές έννοιες στις οποίες στηρίχτηκαμε.

Έτσι στο πρώτο κεφάλαιο θα δούμε τι είναι αλγεβρικό σώμα συναρτήσεων και πως ορίζονται σ' αυτό οι δακτύλιοι εκτίμησης και οι θέσεις. Στη συνέχεια γίνεται εφαρμογή αυτών των εννοιών στο ρητό σώμα συναρτήσεων. Το πρώτο κεφάλαιο τελειώνει με τους διαιρέτες του F/K και τις ιδιότητες αυτών.

Στο δεύτερο κεφάλαιο παρουσιάζουμε στο πρώτο μέρος τις έννοιες της παραγώγου και του διαφορικού ενός αλγεβρικού σώματος συναρτήσεων, ορίζουμε το γένος g του F/K και αποδεικνύουμε το Θεώρημα Riemann. Ενώ στο δεύτερο μέρος αναλύεται η έννοια της P-adic πλήρωσης ενός σώματος F.

Στο τρίτο κεφάλαιο εισάγουμε τις έννοιες index of speciality ενός διαιρέτη και της adele. Στόχος του κεφαλαίου είναι η διατύπωση και η απόδειξη του Θεωρήματος Riemann-Roch.

Στο τέταρτο και τελευταίο καφάλαιο δίνουμε τον ορισμό ενός κώδικα καθώς και τα χαρακτηριστικά στοιχεία του. Στην συνέχεια παρουσιάζουμε τους γνωστούς και ευρείας χρήσης κώδικες Reed Solomon και ως γενίκευση αυτών τους γεωμετρικούς κώδικες Goppa.

Για την εκπόνηση αυτής της πτυχιακής θα ήθελα να ευχαριστήσω τον εισηγητή καθηγητή μου κ. Αριστείδη Κοντογεώργη για την καθοδήγηση που μου παρείχε και την κατανόηση που έδειξε. Επίσης ευχαριστώ θερμά τους κυρίους Μ. Ανούση και Α. Τσολομύτη για την παρουσία τους στην παρουσίαση αυτής της εργασίς. Ευχαριστώ την οικογένεια μου για την κατανόηση που έδειξε και όλους αυτούς που με τον τρόπο τους με βοήθησαν να ολοκληρώσω τις σπουδές μου.

Σ. Κουμούτση, Σάμος 2005.

Κεφάλαιο 1

Αλγεβρικά σώματα συναρτήσεων

1.1 Θέσεις

Ορισμός 1.1. Έστω F ένα σώμα και K υποσώμα του F.

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

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

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

Αν F/K και M/F είναι πεπερασμένες επεκτάσεις, τότε και το M/K είναι πεπερασμένη επέκταση και ισχύει $[M : K] = [M : F] \cdot [F : K]$.

(iii) Ένα στοιχείο $\alpha \in F$ είναι *αλγεβρικό πάνω από το* K αν υπάρχει μη μηδενικό πολυώνυμο $f(x) \in K[x]$ ($K[x]$ ο δακτύλιος πολυωνύμων πάνω από το K) έτσι ώστε $f(\alpha) = 0$. Αν το α δεν είναι αλγεβρικό πάνω από το K, τότε το α λέγεται *υπερβατικό πάνω από το* K.

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

Σχόλια 1.1.

(i) Έστω $\gamma_1, \ldots, \gamma_r \in F$. Το μικρότερο υποσώμα του F το οποίο περιέχει το K και όλα τα στοιχεία $\gamma_1, \ldots, \gamma_r$ το συμβολίζουμε με $K(\gamma_1, \ldots, \gamma_r)$. Η επέκταση $K(\gamma_1, \ldots, \gamma_r)/K$ είναι πεπερασμένη ανν όλα τα γ_i είναι αλγεβρικά πάνω από το K.

(ii) Ειδικότερα το $\alpha \in F$ είναι αλγεβρικό πάνω από το K ανν $[K(\alpha) : K] < \infty$.

Παραδείγματα 1.1.

(i) Το $\mathbb{C}$ είναι μία επέκταση του $\mathbb{Q}$. Το $\sqrt{2}$ είναι αλγεβρικό στοιχείο πάνω από το $\mathbb{Q}$ εφ' όσον είναι ρίζα του x^2-2. Ομοίως το i είναι αλγεβρικό στοιχείο πάνω από το $\mathbb{Q}$, αφού είναι ρίζα του x^2+1.

(ii) Οι αριθμοί π και e είναι υπερβατικά στοιχεία πάνω από το $\mathbb{Q}$. Όμως ο π είναι αλγεβρικός πάνω από το $\mathbb{R}$ ως ρίζα του $(x-\pi) \in \mathbb{R}[x]$.

Ορισμός 1.2. Ένα *αλγεβρικό σώμα συναρτήσεων* F/K μίας μεταβλητής πάνω από το K είναι μία επέκταση σώματος $F(\supseteq K)$ έτσι, ώστε F είναι μία πεπερασμένη αλγεβρική επέκταση του $K(x)$ για κάποια $x \in F$ τα οποία είναι υπερβατικά πάνω από το K. Για συντομία το F/K το λέμε σώμα συναρτήσεων.

Σχόλια 1.2. Για τα στοιχεία του F τα οποία είναι υπερβατικά πάνω από το K ισχύει η ακόλουθη πρόταση: «Το $z \in F$ είναι υπερβατικό πάνω από το K ανν $[F : K(z)] < \infty$».

Απόδειξη:

Ευθύ: Αν $z \in F$ είναι υπερβατικό πάνω από το K τότε:

$$\begin{array}{c} F \\ | \quad \text{αλγεβρική} \\ K(z) \\ | \quad \text{άπειρη} \\ K \end{array}$$

άρα $[F : K(z)] < \infty$.

Αντίστροφο: Αν $[F : K(z)] < \infty$ και z αλγεβρικό τότε $[K(z) : K] < \infty$. Άρα $[F : K] = [F : K(z)] \cdot [K(z) : K] < \infty$ άρα z υπερβατικό πάνω από το K. ■

Ορισμός 1.3. Το σύνολο

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

λέγεται *σώμα των σταθερών του* F/K.

Παρατηρήσεις 1.1. (i) Το $\widetilde{K}$ είναι υπόσωμα του F. Πράγματι, αν α, β αλγεβρικά στοιχεία του F, τότε πρέπει να δείξουμε ότι $\alpha+\beta, \alpha\cdot\beta, -\alpha$ και α^{-1} (αν $\alpha \neq 0$) είναι επίσης αλγεβρικά. Εφ' όσον α είναι αλγεβρικό $[K(\alpha) : K] < \infty$. Επιπλέον το β είναι αλγεβρικό πάνω από το K, άρα είναι αλγεβρικό πάνω από το μεγαλύτερο σώμα $K(\alpha)$. Επομένως το σώμα $K(\alpha, \beta)$ είναι μία πεπερασμένη επέκταση του $K(\alpha)$, δηλαδή $[K(\alpha, \beta) : K(\alpha)] < \infty$. Επειδή $K \subset K(\alpha)$, το $[K(\alpha, \beta) : K]$ είναι επίσης πεπερασμένο. Επομένως κάθε στοιχείο του $K(\alpha, \beta)$ είναι αλγεβρικό πάνω από το K. Τα στοιχεία $\alpha+\beta, \alpha\cdot\beta, -\alpha$ και α^{-1} βρίσκονται όλα στο $K(\alpha, \beta)$. Άρα είναι αλγεβρικά.

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

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

Παραδείγματα 1.2. Το απλούστερο παράδειγμα ενός αλγεβρικού σώματος συναρτήσεων είναι το σώμα των ρητών συναρτήσεων.

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

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

$$z = a \cdot \prod_i p_i(x)^{n_i} \tag{1.1}$$

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

Σχόλια 1.3.

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

(ii) Αν F/K δεν είναι ρητό σώμα συναρτήσεων, δεν είναι ξεκάθαρο αν κάθε στοιχείο $z(\neq 0) \in F$ επιδέχεται ανάλυση ανάλογη της (1.1). Πράγματι δεν είναι ξεκάθαρο τι εννοούμε όταν λέμε ανάγωγο στοιχείο του F. Ένα άλλο πρόβλημα σχετικά με την (1.1) είναι το ακόλουθο: «Δίνονται τα στοιχεία $\alpha_1, \ldots, \alpha_n \in K$. Να βρείτε όλες τις ρητές συναρτήσεις $f(x) \in K(x)$ με προκαθορισμένη τάξη ριζών (ή πόλων) στα $\alpha_1, \ldots, \alpha_n$». Για να δώσουμε απάντηση σε τέτοια προβλήματα εισάγουμε τις έννοιες των δακτυλίων εκτίμησης και των θέσεων.

Ορισμός 1.4. Ένας *δακτύλιος εκτίμησης* ενός σώματος συναρτήσεων F/K είναι ένας δακτύλιος[1] $\mathcal{O} \subseteq F$ με τις ακόλουθες ιδιότητες:

(i) $K \subset \mathcal{O} \subset F$ και

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

Παρατηρήσεις 1.2. Στην περίπτωση του σώματος των ρητών συναρτήσεων $K(x)$ δοθέντος ενός ανάγωγου πολυωνύμου $p(x) \in K[x]$ θεωρούμε το σύνολο

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

Παρατηρούμε λοιπόν ότι

[1] Μία τριάδα $(R, +, \cdot)$ που αποτελείται από ένα (μη κενό) σύνολο R και δύο πράξεις $+, \cdot$ καλείται δακτύλιος αν ισχύουν τα ακόλουθα.

(i) Το ζεύγος $(R, +)$ είναι αβελιανή ομάδα.

(ii) Το ζεύγος $(R, \cdot)$ είναι ημιομάδα

(iii) $(a + b) \cdot c = a \cdot c + b \cdot c$ και $c \cdot (a + b) = c \cdot a + c \cdot b$ για όλα τα $a, b, c \in R$.

Αν επιπλέον ο πολλαπλασιασμός είναι μεταθετικός, τότε ο δακτύλιος ονομάζεται μεταθετικός. Ένας μεταθετικός δακτύλιος με μοναδιαίο στοιχείο και χωρίς διαιρέτες του μηδενός καλείται ακέραια περιοχή (π.χ. ο δακτύλιος $\mathbb{Z}$ των ακεραίων είναι ακέραια περιοχή).

(i) το $\mathcal{O}_{p(x)}$ είναι ένας δακτύλιος εκτιμήσεων του $K(x)/K$ [2] και

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

Ορισμός 1.5. Αν R είναι ένας μεταθετικός δακτύλιος, ένα υποσύνολο $I \subset R$ λέγεται *ιδεώδες* (ideal) αν

(i) $0 \in I$,

(ii) για κάθε $\alpha \in I$ και για κάθε $\beta \in R$ συνεπάγεται ότι $\alpha \cdot \beta \in I$ και

(iii) για κάθε $\alpha, \beta \in I$ το $\alpha + \beta \in I$.

Ορισμός 1.6.

(i) Ένα ιδεώδες I που παράγεται από ένα στοιχείο λέγεται *κύριο ιδεώδες*(principal ideal).

(ii) Μία ακέραια περιοχή λέγεται *περιοχή κυρίων ιδεωδών* (principal ideal domain) αν κάθε ιδεώδες της είναι κύριο. (Π.χ. κάθε στοιχείο του $K[x]$ είναι κύριο. Γι' αυτό το $K[x]$ είναι μία περιοχή κύριων ιδεωδών.)

Ορισμός 1.7. Αν το ιδεώδες I ενός δακτυλίου R είναι $I \neq R$ και $I \neq 0$, τότε το I λέγεται *γνήσιο ιδεώδες* του R.

Ορισμός 1.8. Ένα γνήσιο ιδεώδες I του δακτύλιου R λέγεται

(i) *πρώτο* (prime) αν από τη σχέση $ab \in I$ συμπεραίνουμε ότι είτε $a \in I$ είτε $b \in I$ και

(ii) *μέγιστο* αν από τη σχέση $I \subset M \lhd R$ [3] συμπεραίνουμε ότι $M = R$, δηλαδή δεν υπάρχει γνήσιο ιδεώδες του R που να περιέχει γνήσια το I.

Πρόταση 1.1. Έστω $\mathcal{O}$ ένας δακτύλιος εκτίμησης του σώματος συναρτήσεων F/K. Τότε

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

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

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

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

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

Απόδειξη:

(i) Θα δείξουμε ότι το $P := \mathcal{O} \backslash \mathcal{O}^*$ είναι ένα ιδεώδες του $\mathcal{O}$.

(α') Το $0 \in P$.

[2] Πράγματι $\mathcal{O}_{p(x)} \subset K(x)$ και για κάθε $z \in K(x)$ το $z \in \mathcal{O}_{p(x)}$ ή $z^{-1} \in \mathcal{O}_{p(x)}$. Κάθε $z \in K(x)$ είναι της μορφής $f(x)/g(x)$ όπου $f(x), g(x) \in K[x]$ και $p(x)$ ανάγωγο πολυώνυμο του $K[x]$ τότε $p(x) \nmid g(x)$ ή $p(x) \nmid f(x)$.

[3] Με άλλα λόγια το M είναι ιδεώδες του R.

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

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

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

(ii) Έχουμε ότι $x \in F$ άρα

$$x \in \mathcal{O} \text{ ή } x^{-1} \in \mathcal{O} \tag{1.2}$$

και $x \in P$ άρα

$$x \in \mathcal{O} \text{ και } x \notin \mathcal{O}^*. \tag{1.3}$$

Από τις (1.2) και (1.3) συνεπάγεται και αντιστρόφως ότι $x^{-1} \notin \mathcal{O}$.

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

$$a_r(z^{-1})^r + \cdots + a_1 z^{-1} + 1 = 0$$

ή

$$z^{-1}\big(a_r(z^{-1})^{r-1} + \cdots + a_1\big) = -1.$$

Επομένως

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

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

Θεώρημα 1.1. Έστω $\mathcal{O}$ ένας δακτύλιος εκτίμησης του σώματος συναρτήσεων F/K και P είναι το μοναδικό του μέγιστο ιδεώδες. Τότε:

(i) Το P είναι κύριο ιδεώδες.

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

$$z = t^n u$$

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

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

Ένας δακτύλιος με τις παραπάνω ιδιότητες ονομάζεται *διακριτός δακτύλιος εκτίμησης*.

Λήμμα 1.1. Έστω $\mathcal{O}$ ένας δακτύλιος εκτίμησης ενός αλγεβρικού σώματος συναρτήσεων F/K, P το μέγιστο ιδεώδες του και $x(\neq 0) \in P$. Έστω $x_1, x_2, \ldots, x_n \in P$ έτσι, ώστε $x_1 = x$ και $x_i \in x_{i+1}P$ για $i = 1, \ldots, n-1$. Τότε έχουμε $n \leq [F : K(x)] < \infty$.

Απόδειξη:

Το ότι $[F : K(x)] < \infty$ προκύπτει από το σχόλιο 1.2 και την πρόταση 1.1. Έτσι μένει να δείξουμε ότι τα $x_1, \ldots, x_n$ είναι γραμμικώς ανεξάρτητα πάνω από το $K(x)$. Για το λόγο αυτό υποθέτουμε ότι υπάρχει ένας μη-τετριμμένος γραμμικός συνδιασμός

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

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

$$-\varphi_j x_j = \sum_{i \neq j} \varphi_i x_i \tag{1.4}$$

με $\varphi_i \in \mathcal{O}$ για $i = 1, \ldots, n$ (εφ' όσον $x = x_1 \in P$), $x_i \in x_j P$ για $i < j$ και $\varphi_i = x g_i$ για $i > j$, όπου g_i τα πολυώνυμα του x. Διαιρώντας την (1.4) με x_j προκύπτει

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

τα αθροίσματα του δεύτερου μέλους ανήκουν στο P, επομένως $\varphi_j \in P$. Από την άλλη $\varphi_j = a_j + x g_j$ με $g_j \in K[x] \subseteq \mathcal{O}$ και $x \in P$, έτσι, ώστε $a_j = \varphi_j - x g_j \in P \cap K$. Εφ' όσον όμως $a_j \neq 0$ καταλήγουμε σε άτοπο. Άρα τα $x_1, \ldots, x_n$ είναι γραμμικώς ανεξάρτητα πάνω από το $K(x)$. ■

Απόδειξη του θεωρήματος 1.1:

(i) Υποθέτω ότι το P δεν είναι κύριο ιδεώδες. Έστω επίσης ένα στοιχείο $x_1 (\neq 0) \in P$. Αφού $P \neq x_1 \mathcal{O}$, υπάρχει $x_2 \in P \backslash x_1 \mathcal{O}$. Τότε $x_2 \cdot x_1^{-1} \notin \mathcal{O}$, οπότε $x_2^{-1} x_1 \in P$ από την πρόταση 1.1.2. Έτσι $x_1 \in x_2 P$. Με επαγωγή παίρνουμε μία άπειρη ακολουθία $x_1, x_2, x_3, \ldots$ στο P τέτοια, ώστε $x_i \in x_{i+1} P$ για κάθε $i \geq 1$, το οποίο είναι άτοπο σύμφωνα με το λήμμα 1.1. Άρα το P είναι κύριο ιδεώδες του $\mathcal{O}$.

(ii) Έστω ότι $z \in F$. Τότε $z \in \mathcal{O}$ ή $z^{-1} \in \mathcal{O}$, οπότε μπορώ να υποθέσω ότι $z \in \mathcal{O}$. Αν $z \in \mathcal{O}^*$ τότε $z = t^0 z$. Άρα ισχύει. Αν $z \in P$ υπάρχει ένα μέγιστο $m \geq 1$ με $z \in t^m \mathcal{O}$, εφ' όσον το μήκος της ακολουθίας

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

φράσσεται λόγω του λήμματος 1.1. Γράφουμε $z = t^m u$ με $u \in \mathcal{O}$. Τότε το u πρέπει να είναι μονάδα του $\mathcal{O}$ (αλλιώς $u \in P = t\mathcal{O}$ και έτσι $u = tw$ με $w \in \mathcal{O}$ και $z = t^{m+1} w \in t^{m+1} \mathcal{O}$, άτοπο γιατί το m είναι μέγιστο μ' αυτή την ιδιότητα). Άρα $z = t^m u$ με $m \in \mathbb{Z}$ και $u \in \mathcal{O}^*$.

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

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

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

δεν είναι κενό (αν $x(\neq 0) \in I$ τότε $x = t^r u$ με $u \in \mathcal{O}^*$ και $t^r = xu^{-1} \in I$). Θέτω $n := min(A)$. Απαιτούμε $I = t^n\mathcal{O}$. $t^n\mathcal{O} \subseteq I$ ισχύει, εφ' όσον $t^n \in I$. Έστω $y \in I$ με $y \neq 0$. Έχουμε $y = t^s w$ με $w \in \mathcal{O}^*$ και $s \geq 0$. Έτσι $t^s \in I$ και $s \geq n$. Επομένως $y = t^n t^{s-n} w \in t^n\mathcal{O}$. Άρα $I \subseteq t^n\mathcal{O}$. Άρα $I = t^n\mathcal{O}$. ■

Ορισμός 1.9. (i) Μία *θέση* P του σώματος συναρτήσεων F/K είναι το μέγιστο ιδεώδες κάποιου δακτυλίου εκτίμησης $\mathcal{O}$ του F/K. Κάθε στοιχείο $t \in P$ έτσι, ώστε $P = t\mathcal{O}$ ονομάζεται *πρώτο στοιχείο για το* P.

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

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

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

(Πρόταση 1.1). Επομένως το $\mathcal{O}_P(:= \mathcal{O})$ ονομάζεται *δακτύλιος εκτίμησης της θέσης* P.

Ορισμός 1.10. Μία *διακριτή εκτίμηση του* F/K είναι μία συνάρτηση $v : F \to \mathbb{Z} \cup \{\infty\}$ με τις ακόλουθες ιδιότητες:

(i) $v(x) = \infty \Leftrightarrow x = 0$

(ii) $v(xy) = v(x) + v(y),\ \forall x, y \in F$

(iii) $v(x + y) \geq min\{v(x), v(y)\},\ \forall x, y \in F$

(iv) Υπάρχει ένα στοιχείο $z \in F$ με $v(z) = 1$ και

(v) $v(a) = 0,\ \forall a(\neq 0) \in K$.

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

Από τις ιδιότητες 2 και 4 του ορισμού 1.10 προκύπτει αμέσως ότι η $v : F \to \mathbb{Z} \cup \{\infty\}$ είναι 1-1 και επί.

Η ιδιότητα 3 του ορισμού 1.10 ονομάζεται τριγωνική ανισότητα. Μία πιό αυστηρή μορφή της δίνεται από το ακόλουθο λήμμα.

Λήμμα 1.2. (*Αυστηρή Τριγωνική Ανισότητα*) Έστω v μία διακριτή εκτίμηση του F/K και $x, y \in F$ με $v(x) \neq v(y)$. Τότε

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

Απόδειξη:

Παρατηρούμε ότι

$$v(ay) = v(a) + v(y) = 0 + v(y) = v(y)$$

για $a(\neq 0) \in K$ (Ιδιότητες 2 και 5 του ορισμού 1.10). Ειδικότερα

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

Εφόσον $v(x) \neq v(y)$ μπορούμε να υποθέσουμε $v(x) < v(y)$. Υποθέτουμε ότι $v(x + y) \neq min\{v(x), v(y)\}$ και έτσι $v(x + y) > v(y)$ από την ιδιότητα 3 του ορισμού 1.10. Οπότε έχουμε $v(x) = v\big((x+y)-y\big) \geq min\{v(x+y), v(y)\} > v(x)$. Άτοπο! Άρα $v(x+y) = min\{v(x), v(y)\}$. ■

Ορισμός 1.11. Σε κάθε θέση $P \in \mathbb{P}_F$ αντιστοιχίζουμε μία συνάρτηση $v_P : F \to \mathbb{Z} \cup \{\infty\}$ (η οποία μπορεί να αποδειχθεί ότι είναι μία διακριτή εκτίμηση του F/K). Διαλέγουμε ένα πρώτο στοιχείο t για το P. Τότε κάθε $z(\neq 0) \in F$ έχει μοναδική αναπαράσταση $z = t^n u$ με $u \in \mathcal{O}_P^*$ και $n \in \mathbb{Z}$. Ορίζουμε $v_P(z) := n$ και $v_P(0) := \infty$.

Παρατηρήσεις 1.3. Ο προηγούμενος ορισμός εξαρτάται μόνο από το P και όχι από την επιλογή του t. Αν τυχόν t' είναι ένα άλλο πρώτο στοιχείο για το P τότε $P = t\mathcal{O} = t'\mathcal{O}$. Έτσι $t = t'w$ για κάποια $w \in \mathcal{O}_P^*$. Επομένως $t^n u = (t'^n w^n)u = t'^n(w^n u)$ με $w^n u \in \mathcal{O}_P^*$.

Θεώρημα 1.2. Έστω F/K ένα σώμα συναρτήσεων. Τότε

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

$$\mathcal{O}_P = \{z \in F : v_P(z) \geq 0\} \tag{1.5}$$

$$\mathcal{O}_P^* = \{z \in F : v_P(z) = 0\} \tag{1.6}$$

$$P = \{z \in F : v_P(z) > 0\} \tag{1.7}$$

Τέλος ένα στοιχείο $x \in F$ είναι ένα πρώτο στοιχείο για το P ανν $v_P(x) = 1$.

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

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

είναι μία θέση του F/K και το

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

είναι ο αντίστοιχος δακτύλιος εκτίμησης.

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

Απόδειξη:

(i) Η v_P έχει τις ιδιότητες 1, 2, 4 και 5 του ορισμού 1.10. Θα αποδείξουμε ότι ισχύει και η 3. Έστω ότι $x, y \in F$ με $v_P(x) = n$ και $v_P(y) = m$. Μπορούμε να υποθέσουμε ότι $n \leq m < \infty$. Έτσι $x = t^n u_1$ και $y = t^m u_2$ με $u_1, u_2 \in \mathcal{O}_P^*$. Τότε

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

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

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

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

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

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

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

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

Έστω P μία θέση του F/K και $\mathcal{O}_P$ ο δακτύλιος εκτίμησής της. Εφόσον P είναι ένα μέγιστο ιδεώδες, ο δακτύλιος κλάσης υπολοίπων $\mathcal{O}_P/P$ είναι σώμα. Για $x \in \mathcal{O}_P$ ορίζουμε $x(P) \in \mathcal{O}_P/P$ να είναι η κλάση των υπολοίπων του x modulo P, για $x \in F \backslash \mathcal{O}_P$ θέτουμε $x(P) := \infty$ (Το σύμβολο ∞ δεν έχει την ίδια έννοια με τον ορισμό 1.10).

Από την πρόταση 1.1 ξέρουμε ότι $K \subseteq \mathcal{O}_P$ και $K \cap P = \{0\}$. Έτσι η απεικόνιση $\mathcal{O}_P \to \mathcal{O}_P/P$ δημιουργεί μία κανονική εμφύτευση του K στο $\mathcal{O}_P/P$. Στο εξής θα θεωρούμε το K πάντα ως υπόσωμα του $\mathcal{O}_P/P$ μέσω αυτής της εμφύτευσης. Αυτό εφαρμόζεται και για το $\widetilde{K}$ αντί για το K. Έτσι μπορούμε να θεωρούμε το $\widetilde{K}$ ως υπόσωμα του $\mathcal{O}_P/P$.

Ορισμός 1.12. Έστω $P \in \mathbb{P}_F$.

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

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

Παρατηρήσεις 1.4. Ο βαθμός μιας θέσης είναι πάντα πεπερασμένος.

Πρόταση 1.2. Αν P είναι μία θέση του F/K και $0 \neq x \in P$ τότε $\deg P \leq [F : K(x)] < \infty$.

Απόδειξη:

$[F : K(x)] < \infty$ ισχύει από το σχόλιο 1.2. Οπότε μένει να δείξουμε ότι για οποιαδήποτε στοιχεία $z_1, \ldots, z_n \in \mathcal{O}_P$ των οποίων οι κλάσεις υπολοίπων $z_1(P), \ldots, z_n(P) \in F_P$ είναι γραμμικά ανεξάρτητες πάνω από το K, είναι γραμμικά ανεξάρτητες πάνω από το $K(x)$.
Υποθέτουμε ότι υπάρχει ένας μη- τετριμμένος γραμμικός συνδυασμός

$$\sum_{i=1}^{n} \varphi_i z_i = 0 \tag{1.8}$$

με $\varphi_i \in K(x)$. Χωρίς βλάβη της γενικότητας θεωρούμε ότι τα φ_i είναι πολυώνυμα του x και δεν είναι όλα διαιρετά από το x δηλαδή $\varphi_i = \alpha_i + xg_i$ με $\alpha_i \in K$, $g_i \in K[x]$ όχι όλα τα $\alpha_i = 0$.

Εφόσον $x \in P$ και $g_i \in \mathcal{O}_P$, $\varphi_i(P) = \alpha_i(P) = \alpha_i$. Εφαρμόζοντας την απεικόνιση κλάσης υπολοίπων στην (1.8) έχουμε:

$$0 = 0(P) = \sum_{i=1}^{n} \varphi_i(P) z_i(P) = \sum_{i=1}^{n} \alpha_i z_i(P) \tag{1.9}$$

άτοπο γιατί τα $z_i(P), \ldots, z_n(P)$ είναι γραμμικά ανεξάρτητα πάνω από το K ■

Πόρισμα 1.1. Το σώμα $\widetilde{K}$ των σταθερών του F/K είναι μία πεπερασμένη επέκταση του K.

Απόδειξη:

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

$$[\widetilde{K} : K] \leq [F_P : K] < \infty. \quad \blacksquare \tag{1.10}$$

Σχόλια 1.4. Για την περίπτωση που $\deg P = 1$ έχουμε $F_P = K$ και η απεικόνιση κλάσης υπολοίπων απεικονίζει το F στο $K \cup \{\infty\}$. Ειδικότερα αν K είναι ένα αλγεβρικά κλειστό σώμα, κάθε θέση έχει βαθμό 1, οπότε μπορούμε να διαβάσουμε ένα στοιχείο $z \in F$ ως μία συνάρτηση

$$z : \begin{cases} \mathbb{P}_F \to K \cup \{\infty\} \\ \\ P \mapsto z(P) \end{cases} . \tag{1.11}$$

Για αυτό το λόγο το F/K λέγεται σώμα συναρτήσεων. Τα στοιχεία του K που ερμηνεύονται ως συναρτήσεις με την έννοια της (1.11) είναι σταθερές συναρτήσεις γι' αυτό το λόγο το K ονομάζεται σώμα σταθερών του F.

Ορισμός 1.13. Έστω $z \in F$ και $P \in \mathbb{P}_F$. Λέμε ότι:

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

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

Θεώρημα 1.3. Έστω F/K ένα σώμα συναρτήσεων και R ένας υποδακτύλιος του F με $K \subseteq R \subseteq F$. Έστω ότι $\{0\} \neq I \subsetneq R$ ένα γνήσιο ιδεώδες του R. Τότε υπάρχει μία θέση $P \in \mathbb{P}_F$ τέτοια ώστε $I \subseteq P$ και $R \subseteq \mathcal{O}_P$.

Απόδειξη:

Θεωρούμε το σύνολο

$$\mathcal{F} := \{S : S \text{ είναι υποδακτύλιος του } F \text{ με } R \subseteq S \text{ και } IS \neq S\} \tag{1.12}$$

(εξ' ορισμού, IS είναι το σύνολο όλων των πεπερασμένων αθροισμάτων $\sum \alpha_\nu s_\nu$ με $\alpha_\nu \in I$, $s_\nu \in S$. IS είναι ένα ιδεώδες του S). $R \in \mathcal{F}$ άρα $\mathcal{F} \neq \emptyset$ και $\mathcal{F}$ είναι επαγωγικώς διατεταγμένο. Πράγματι, αν $\mathcal{H} \subseteq \mathcal{F}$ είναι ολικώς διατεταγμένο υποσύνολο του $\mathcal{F}$ τότε $T := \cup\{S : S \in \mathcal{H}\}$ είναι υποδακτύλιος του F με $R \subseteq T$. Έχουμε να αποδείξουμε ότι $IT \neq T$. Υποθέτουμε ότι αυτό δεν ισχύει, τότε

$1 = \sum_{\nu=1}^{n} \alpha_\nu s_\nu$ με $\alpha_\nu \in I$, $s_\nu \in T$. Εφόσον $\mathcal{H}$ είναι ολικά διατεταγμένο υπάρχει ένα $S_0 \in \mathcal{H}$ τέτοιο ώστε $s_1, \ldots, s_n \in S_0$, έτσι

$$1 = \sum_{\nu=1}^{n} \alpha_\nu s_\nu \in IS_0. \tag{1.13}$$

Άτοπο, άρα $IT \neq T$.

Από το Λήμμα του Zorn [4] το $\mathcal{F}$ περιέχει ένα μέγιστο στοιχείο, δηλαδή ένας δακτύλιος $\mathcal{O} \subseteq F$ τέτοιος ώστε $R \subseteq \mathcal{O} \subseteq F$, $I\mathcal{O} \neq \mathcal{O}$ και $\mathcal{O}$ μέγιστο με αυτές τις ιδιότητες.

Θα δείξουμε τώρα ότι το $\mathcal{O}$ είναι δακτύλιος εκτίμησης του F/K. Εφόσον $I \neq \{0\}$ και $I\mathcal{O} \neq \mathcal{O}$ έχουμε $\mathcal{O} \subsetneqq F$ και $I \subseteq \mathcal{O}\backslash\mathcal{O}^*$. Υποθέτουμε ότι υπάρχει ένα στοιχείο $z \in F$ με $z \notin \mathcal{O}$ και $z^{-1} \notin \mathcal{O}$. Τότε $I\mathcal{O}[z] = \mathcal{O}[z]$ και $I\mathcal{O}[z^{-1}] = \mathcal{O}[z^{-1}]$ και μπορούμε να βρούμε $\alpha_0, \ldots, \alpha_n, b_0, \ldots, b_n \in I\mathcal{O}$ με

$$1 = \alpha_0 + \alpha_1 z + \cdots + \alpha_n z^n \quad \text{και} \tag{1.14}$$

$$1 = b_0 + b_1 z^{-1} + \cdots + b_m z^{-m} \tag{1.15}$$

με $n \geq 1$ και $m \geq 1$. Μπορούμε να υποθέσουμε ότι m, n έχουν επιλεχθεί να είναι τα μικρότερα δυνατά και $m \leq n$. Πολλαπλασιάζοντας την (1.14) με $1 - b_0$ και την (1.15) με $\alpha_n z^n$ παίρνουμε

$$1 - b_0 = (1 - b_0)\alpha_0 + (1 - b_0)\alpha_1 z + \cdots + (1 - b_0)\alpha_n z^n \quad \text{και} \tag{1.16}$$

$$0 = (b_0 - 1)\alpha_n z^n + b_1 \alpha_n z^{n-1} + \cdots + b_m \alpha_n z^{n-m}. \tag{1.17}$$

Τις προσθέτω κατά μέλη όποτε

$$1 = c_0 + c_1 z + \cdots + c_{n-1} z^{n-1} \tag{1.18}$$

με συντελεστές $c_i \in I\mathcal{O}$. Άτοπο λόγω του ελάχιστου του n στην (1.14). Άρα $z \in \mathcal{O}$ ή $z^{-1} \in \mathcal{O}$ οπότε $\mathcal{O}$ είναι δακτύλιος εκτίμησης του F/K. ■

Πόρισμα 1.2. Έστω F/K σώμα συναρτήσεων, $z \in F$ υπερβατικό πάνω από το K. Τότε z έχει μία τουλάχιστον ρίζα και έναν τουλάχιστον πόλο. Ειδικότερα $\mathbb{P}_F \neq \emptyset$.

Απόδειξη:

Θεωρούμε τον δακτύλιο $R = K[z]$ και το ιδεώδες $I = zK[z]$. Από το θεώρημα 1.3 υπάρχει μία θέση $P \in \mathbb{P}_F$ με $z \in P$, οπότε P είναι μία ρίζα του z.
Ομοίως z^{-1} έχει μία ρίζα $Q \in \mathbb{P}_F$, τότε Q είναι ένας πόλος του z. ■

[4] Λήμμα Zorn: Αν S είναι ένα μερικά διατεταγμένο σύνολο τέτοιο ώστε κάθε αλυσίδα στο S να έχει ένα άνω φράγμα στο S, τότε το S έχει τουλάχιστον ένα μεγιστικό στοιχείο.

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

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

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

1.2 Το Σώμα των ρητών συναρτήσεων

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

$$\mathcal{O}_{p(x)} := \left\{ \frac{f(x)}{g(x)} : \ f(x), g(x) \in K[x], \ p(x) \nmid g(x) \right\} \tag{1.19}$$

του $K(x)/K$ με μέγιστο ιδεώδες

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)} : \ f(x), g(x) \in K[x], p(x) \mid f(x), \, p(x) \nmid g(x) \right\}. \tag{1.20}$$

Στην ειδική περίπτωση που το $p(x)$ είναι γραμμικό δηλαδή $p(x) = x - \alpha$ με $\alpha \in K$ συντομεύουμε και γράφουμε

$$P_\alpha := P_{x-\alpha} \in \mathbb{P}_{K(x)}. \tag{1.21}$$

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

$$\mathcal{O}_\infty := \left\{ \frac{f(x)}{g(x)} : \ f(x), g(x) \in K[x], \ \deg f(x) \leq \deg g(x) \right\}. \tag{1.22}$$

με μέγιστο ιδεώδες

$$P_\infty := \left\{ \frac{f(x)}{g(x)} : \ f(x), g(x) \in K[x], \ \deg f(x) < \deg g(x) \right\}. \tag{1.23}$$

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

Παρατηρούμε ότι αυτοί οι χαρακτηρισμοί εξαρτώνται από την ειδική επιλογή του παραγόμενου στοιχείου x του $K(x)/K$ (π.χ. $K(x) = K(1/x)$ και η άπειρη θέση με εκτίμηση στο $1/x$ είναι η θέση P_0 με εκτίμηση στο x).

Πρόταση 1.3. Έστω $F = K(x)$ το σώμα των ρητών συναρτήσεων.

(i) Έστω $P = P_{p(x)} \in \mathbb{P}_{K(x)}$ η θέση που ορίστηκε στην (1.20) όπου $p(x) \in K[x]$ είναι ένα ανάγωγο πολυώνυμο. Τότε $p(x)$ είναι ένα πρώτο στοιχείο του για το P, και η αντίστοιχη διακριτή εκτίμηση v_P μπορεί να περιγραφεί ως εξής: «Αν $z \in K(x)\backslash\{0\}$ γράφεται στη μορφή $z = p(x)^n(f(x)/g(x))$ με $n \in \mathbb{Z}$, $f(x)$, $g(x) \in K[x]$, $p(x) \nmid f(x)$ και $p(x) \nmid g(x)$ τότε $v_P(z) = n$». Το σώμα κλάσης υπολοίπων $K(x)_P = \mathcal{O}_P/P$ είναι ισομορφικό με το $K[x]/(p(x))$. Ο ισομορφισμός είναι

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

Συνεπώς, $\deg P = \deg p(x)$.

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

$$z(P) = z(\alpha) \quad \text{για} \quad z \in K(x), \tag{1.24}$$

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

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

(iii) Τέλος, έστω $P = P_\infty$ είναι η άπειρη θέση του $K(x)/K$ που ορίστηκε στην (1.23). Τότε $\deg P_\infty = 1$. Ένα πρώτο στοιχείο για την P_∞ είναι το $t = 1/x$. Η αντίστοιχη διακριτή εκτίμηση δίνεται από

$$v_\infty(f(x)/g(x)) = \deg g(x) - \deg f(x) \tag{1.25}$$

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

$$\text{Αν} \quad z = \frac{\alpha_n x^n + \ldots + \alpha_0}{b_m x^m + \ldots + b_0} \quad \text{με} \quad \alpha_n, b_m \neq 0, \tag{1.26}$$

τότε

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

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

Απόδειξη:

(i) Έστω $P = P_{p(x)}$, $p(x) \in K[x]$ ανάγωγο πολυώνυμο. Το ιδεώδες $P_{p(x)} \subseteq \mathcal{O}_{p(x)}$ παράγεται από το $p(x)$ οπότε το $p(x)$ είναι ένα πρώτο στοιχείο για το P. Για να αποδείξουμε ότι $K(x)_P$ είναι ισομορφικό με το $K[x]/(p(x))$ θεωρούμε τον ομοιομορφισμό [5]

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

Ο πυρήνας [6] της φ είναι το ιδεώδες που παράγεται από το $p(x)$. Επιπλέον η φ είναι $1-1$ και επί. Αν $z \in \mathcal{O}_{p(x)}$, μπορούμε να γράψουμε

$$z = u(x)/v(x) \quad \text{με} \quad u(x), v(x) \in K[x] \tag{1.27}$$

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

$$\alpha(x)p(x) + b(x)v(x) = 1, \tag{1.28}$$

[5] Έστω R, R' δύο δακτύλιοι. Μία απεικόνιση $\varphi : R \to R'$ λέγεται ομοιομορφισμός αν οι παρακάτω δύο ιδιότητες ικανοποιούνται $\forall \alpha, b \in R$:

(α') $\varphi(\alpha + b) = \varphi(\alpha) + \varphi(b)$

(β') $\varphi(\alpha b) = \varphi(\alpha)\varphi(b)$

[6] Αν $\varphi : R \to R'$ ομοιομορφισμός δακτυλίων τότε ο υποδακτύλιος $\varphi^{-1}(\{0'\})$ λέγεται πυρήνας της φ και συμβολίζεται με $Ker(\varphi)$.

επομένως

$$z = 1z = \big(\alpha(x)p(x) + b(x)v(x)\big)\frac{u(x)}{v(x)} =$$

$$\frac{\alpha(x)u(x)}{v(x)}p(x) + b(x)u(x) \tag{1.29}$$

και $z(P) = (b(x)u(x))(P)$ είναι στην εικόνα της φ. Άρα η φ δημιουργεί έναν ισομορφισμό ϕ από το $K[x]/(p(x))$ στο $K(x)_P$.

(ii) Τώρα $P = P_\alpha$ με $\alpha \in K$. Αν $f(x) \in K[x]$ τότε $(x-\alpha) \mid (f(x) - f(\alpha))$, από όπου

$$f(x)(P) = (f(x) - f(\alpha))(P) + f(\alpha)(P) = f(\alpha). \tag{1.30}$$

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

$$z(P) = \frac{f(x)(P)}{g(x)(P)} = \frac{f(\alpha)}{g(\alpha)} = z(\alpha). \tag{1.31}$$

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

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

Θεώρημα 1.4. Δεν υπάρχουν άλλες θέσεις για το σώμα των ρητών συναρτήσεων $K(x)/K$ εκτός από τις θέσεις $P_{p(x)}$ και P_∞ που ορίστηκαν από τις (1.20) και (1.23).

Απόδειξη:

Είναι αρκετό να δείξουμε το ακόλουθο: Δίνεται μια θέση $P \in \mathbb{P}_{K(x)}$, $P \neq P_\infty$ τότε υπάρχει ένα ανάγωγο πολυώνυμο $p(x) \in K[x]$ έτσι ώστε $\mathcal{O}_{p(x)} = \mathcal{O}_P$.

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

$$K[x]/I \hookrightarrow K(x)_P \tag{1.32}$$

συνεπώς $I \neq \{0\}$ από πρόταση (1.2) έπεται ότι υπάρχει ένα ανάγωγο πολυώνυμο με μεγιστοβάθμιο συντελεστή 1 (μοναδικά ορισμένο) $p(x) \in K[x]$ έτσι ώστε $I = K[x] \cap P = p(x)K[x]$. Κάθε $g(x) \in K[x]$ με $p(x) \nmid g(x)$ δεν είναι στο I, έτσι $g(x) \notin P$ και $1/g(x) \in \mathcal{O}_P$ από πρόταση 1.1. Συμπεραίνουμε ότι

$$\mathcal{O}_{p(x)} := \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x],\ p(x) \nmid g(x) \right\} \subseteq \mathcal{O}_P. \tag{1.33}$$

Ως δακτύλιοι εκτίμησης είναι μέγιστοι γνήσιοι υποδακτύλιοι του $K[x]$ (Θεώρημα 1.2) έχουμε $\mathcal{O}_P = \mathcal{O}_{p(x)}$.

- *Δεύτερη περίπτωση:* Τώρα $x \notin \mathcal{O}_P$. Συμπεραίνουμε ότι

$$K[x^{-1}] \subseteq \mathcal{O}_P, \quad x^{-1} \in P \cap K[x^{-1}] \tag{1.34}$$

και

$$P \cap K[x^{-1}] = x^{-1}K[x^{-1}]. \tag{1.35}$$

Όπως στην περίπτωση 1,

$$\mathcal{O}_{p(x)} \supseteq \left\{ \frac{f(x^{-1})}{g(x^{-1})} : f(x^{-1}), g(x^{-1}) \in K[x^{-1}],\, x^{-1} \nmid g(x^{-1}) \right\} =$$

$$\left\{ \frac{\alpha_0 + \alpha_1 x^{-1} + \cdots + \alpha_n x^{-n}}{b_0 + b_1 x^{-1} + \cdots + b_m x^{-m}} :\ b_0 \neq 0 \right\} =$$

$$\left\{ \frac{\alpha_0 x^{m+n} + \alpha_1 x^{m+n-1} + \cdots + \alpha_n x^m}{b_0 x^{m+n} + b_1 x^{m+n-1} + \cdots + b_m x^n} :\ b_0 \neq 0 \right\} =$$

$$\left\{ \frac{u(x)}{v(x)} \ :\ u(x), v(x) \in K[x],\ \deg u(x) \leq \deg v(x) \right\} = \mathcal{O}_\infty.$$

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

Πόρισμα 1.3. Οι θέσεις του $K(x)/K$ βαθμού 1 είναι σε «$1-1$» αντιστοιχία με το $K \cup \{\infty\}$.

Ορισμός 1.14. Έστω ότι το K είναι ένα αλγεβρικά κλειστό σώμα. *Ο n- διάστατος αφινικός χώρος* (affine space) $\mathbb{A}^n = \mathbb{A}^n(K)$ είναι το σύνολο όλων εκείνων των n-άδων με στοιχεία από το K.

Ορισμός 1.15. Ένα στοιχείο $P = (a_1, a_2, \ldots, a_n) \in \mathbb{A}^n$ είναι ένα *σημείο* του $\mathbb{A}^n$, και τα $a_1, a_2, \ldots, a_n$ είναι οι συντεταγμένες του P.

Ορισμός 1.16. Έστω $K[x_1, x_2, \ldots, x_n]$ ο δακτύλιος των πολυωνύμων με n μεταβλητές πάνω από το K. Ένα υποσύνολο $V \subseteq \mathbb{A}^n$ είναι ένα *αλγεβρικό σύνολο* αν υπάρχει ένα σύνολο $M \subseteq K[x_1, x_2, \ldots, x_n]$ τέτοιο, ώστε

$$V = \big\{ P \in \mathbb{A}^n \ :\ F(P) = 0 \text{ για όλα τα } F \in M \big\}.$$

Ορισμός 1.17. Το σύνολο των πολυωνύμων

$$I(V) = \big\{ F \in K[x_1, x_2, \ldots, x_n] \ :\ F(P) = 0 \text{ για όλα τα } P \in V \big\}$$

ονομάζεται *ιδεώδες του* V.

Παρατηρήσεις 1.5. Το $I(V)$ είναι ένα ιδεώδες του $K[x_1, x_2, \ldots, x_n]$ και μπορεί να παραχθεί από πεπερασμένου πλήθους πολυώνυμα $F_1, F_2, \ldots, F_r \in K[x_1, x_2, \ldots, x_n]$[7] (οπότε $V = \big\{ P \in \mathbb{A}^n \ :\ F_1(P) = F_2(P) = \cdots = F_r(P) = 0 \big\}$). Πράγματι το $0 \in I(V)$ εξ' ορισμού (γιατί μηδενίζεται από όλα τα σημεία). Αν $F, G \in I(V)$ και $H \in K[x_1, x_2, \ldots, x_n]$ τότε το $F(P) + G(P) = 0$ και το $H(P) \cdot F(P) = 0$ για κάθε $P \in V$. Άρα το $I(V)$ είναι πράγματι ένα ιδεώδες και καλείται ιδεώδες του V.

[7] Θεώρημα πεπερασμένης βάσης του Hilbert.

Ορισμός 1.18. Ένα αλγεβρικό σύνολο $V \subseteq \mathbb{A}^n$ ονομάζεται ανάγωγο αν δεν μπορεί να γραφεί ως $V = V_1 \cup V_2$ όπου τα V_1 και V_2 είναι γνήσια αλγεβρικά υποσύνολα του V.

Σχόλια 1.5.

(i) Το V είναι ανάγωγο αν και μόνο αν το $I(V)$ είναι πρώτο ιδεώδες.

(ii) Μία affine variety είναι ένα ανάγωγο αλγεβρικό σύνολο $V \subseteq \mathbb{A}^n$.

Ορισμός 1.19. Ο δακτύλιος συντεταγμένων μίας affine variety V είναι ο δακτύλιος κλάσης υπολοίπων

$$\Gamma(V) = K[x_1, x_2, \ldots, x_n]/I(V).$$

Πρόταση 1.4. Αν το $I(V)$ είναι ένα πρώτο ιδεώδες τότε το $\Gamma(V)$ είναι μία ακέραια περιοχή.

Ορισμός 1.20. Έστω V ανάγωγο αλγεβρικό σύνολο. Κάθε $f = F + I(V) \in \Gamma(V)$ δημιουργεί (παράγει) μία συνάρτηση $f : V \to K$ με $f(P) = F(P)$ για κάθε $P \in V$. Το σώμα πηλίκο $K(V) = Quot(\Gamma(V))$ ονομάζεται *σώμα των ρητών συναρτήσεων της* V και

(i) Περιέχει το K ως υποσώμα.

(ii) Η διάσταση της V είναι ο υπερβατικός βαθμός του $K(V)/K$.

(iii) Για ένα σημείο $P \in V$, έστω

$$\mathcal{O}_P(V) = \big\{ f \in K(V) \ : \ f = g/h \text{ με } g, h \in \Gamma(V) \text{ και } h(P) \neq 0 \big\}.$$

Το $\mathcal{O}_P(V)$ είναι τοπικός δακτύλιος με σώμα πηλίκο το $K(V)$. Το μοναδικό μέγιστο ιδεώδες του είναι το

$$M_P(V) = \big\{ f \in K(V) : f = g/h \text{ με } g, h \in \Gamma(V),$$

$$h(P) \neq 0 \text{ και } g(P) = 0 \big\}.$$

Ο $\mathcal{O}_P(V)$ λέγεται τοπικός δακτύλιος της V στο P. Για $f = g/h \in \mathcal{O}_P(V)$ με $h(P) \neq 0$, η τιμή της f στο P ορίζεται να είναι η $f(P) = g(P)/h(P)$.

Ορισμός 1.21. (i) Στο σύνολο $\mathbb{A}^{n+1} \setminus \{0, 0, \ldots, 0\}$ μπορούμε να ορίσουμε μία σχέση ισοδυναμίας «$\sim$» ως εξής

$$(x'_0, x'_1, \ldots, x'_n) \sim (x_0, x_1, \ldots, x_n) \Longleftrightarrow \exists \lambda (\neq 0) \in K \text{ έτσι},$$

$$\text{ώστε } x_i = \lambda x'_i \text{ για } 0 \leq i \leq n.$$

Η κλάση ισοδυναμίας του $(x_0, x_1, \ldots, x_n)$ συμβολίζεται $(x_0 : x_1 : \cdots : x_n)$.

(ii) Ο n-διάστατος προβολικός χώρος $\mathbb{P}^n = \mathbb{P}^n(K)$ είναι το σύνολο όλων των κλάσεων ισοδυναμίας, δηλαδή

$$\mathbb{P}^n = \big\{ (x_0 : x_1 : \cdots : x_n) \mid x_i \in K, \text{ όχι όλα τα } x_i = 0 \big\}.$$

Ένα στοιχείο $P = (x_0 : x_1 : \cdots : x_n) \in \mathbb{P}^n$ είναι ένα σημείο και τα $x_0, x_1, \ldots, x_n$ ονομάζονται ομογενείς συντεταγμένες του P.

Αν σκεφτούμε πιό γεωμετρικά τότε

$$\mathbb{P}^n(K) \cong \big\{ \text{Γραμμές που περνούν από την αρχή στο } K^{n+1} \big\}. \qquad (1.36)$$

Πρόταση 1.5. Έστω το

$$U_0 = \big\{(x_0, x_1, \ldots, x_n) \in \mathbb{P}^n \ : \ x_0 \neq 0\big\}.$$

Τότε η απεικόνιση ϕ που παίρνει το $(a_1, a_2, \ldots, a_n)$ του K^n και το απεικονίζει στο σημείο με ομογενείς συντεταγμένες $(1, a_1, a_2, \ldots, a_n)$ του $\mathbb{P}^n(K)$ είναι μία ένα προς ένα αντιστοιχία ανάμεσα στο K^n και στο $U_0 \subset \mathbb{P}^n(K)$.

Σχόλια 1.6.

(i) Από τον ορισμό του U_0 έχουμε $\mathbb{P}^n(K) = U_0 \cup H$ όπου

$$H = \big\{P \in \mathbb{P}^n(K) \ : \ P = (0, x_1, \ldots, x_n)\big\}. \tag{1.37}$$

Αν ταυτίσουμε το U_0 με τον αφινικό χώρο K^n, τότε μπορούμε να δούμε το H ως ένα υπερεπίπεδο στο άπειρο. Από την (1.36) έπεται ότι τα σημεία στο H είναι σε μία ένα προς ένα αντιστοιχία με τις n-άδες $(x_1, \ldots, x_n)$, όπου δύο n-άδες αντιπροσωπεύουν το ίδιο σημείο του H μόνο αν το ένα είναι μη μηδενικό βαθμωτό πολλαπλάσιο του άλλου. Με άλλα λόγια το H είναι ένα «αντίγραφο» του $\mathbb{P}^{n-1}(K)$, δηλαδή ο προβολικός χώρος με διάσταση μικρότερη κατά ένα.

Ταυτίζοντας το U_0 με το K^n και το H με το $\mathbb{P}^{n-1}(K)$ μπορούμε να γράψουμε

$$\mathbb{P}^n(K) = K^n \cup \mathbb{P}^{n-1}(K). \tag{1.38}$$

Για να εξηγήσουμε τι σημαίνει γεωμετρικά $H = \mathbb{P}^{n-1}(K)$ από την (1.36), ένα σημείο $P \in \mathbb{P}^{n-1}(K)$ δίνει μία γραμμή $L \subset K^n$ που περνάει από την αρχή. Συνεπώς στην ανάλυση (1.38) μπορεί κανείς να σκεφτει το P αναπαριστώντας την ασυμπτωτική κατεύθυνση όλων των γραμμών στο K^n παράλληλα στο L.

(ii) Μία ειδική περίπτωση είναι η προβολική γραμμή $\mathbb{P}^1(K)$. Εφ' όσον $\mathbb{P}^0(K)$ αποτελείται από απλά σημεία θέτοντας $n = 1$ στην (1.38) παίρνουμε

$$\mathbb{P}^1(K) = K^1 \cup \mathbb{P}^0(K) = K \cup \{\infty\},$$

όπου το ∞ αναπαριστά τα απλά σημεία του $\mathbb{P}^0(K)$.

Παρατηρήσεις 1.6. Από το πόρισμα (1.3) και την προηγούμενη ανάλυση για το $\mathbb{P}^1(K)$ μπορούμε να συμπεράνουμε ότι οι θέσεις του $K(x)/K$ με βαθμό 1 βρίσκονται σε ένα προς ένα αντιστοιχία με τα σημεία του $\mathbb{P}^1(K)$.

1.3 Ανεξαρτησία εκτιμήσεων

Θεώρημα 1.5. (*Ασθενούς Προσέγγισης*) Έστω ότι το F/K είναι ένα σώμα συναρτήσεων, $P_1, P_2, \ldots, P_n \in \mathbb{P}_F$ ανά δύο διαφορετικές θέσεις του F/K, $x_1, x_2, \ldots, x_n \in F$ και $r_1, r_2, \ldots, r_n \in \mathbb{Z}$. Τότε υπάρχουν κάποια $x \in F$ τέτοια, ώστε

$$v_{P_i}(x - x_i) = r_i, \text{ για } i = 1, 2, \ldots, n.$$

Απόδειξη:

(Η απόδειξη αυτού του θεωρήματος είναι τεχνική, επόμένως χωρίζεται σε βήματα. Για ευκολία το v_{P_i} συμβολίζεται κατά την διάρκεια αυτής της απόδειξης και μόνο με v_i.)

Βήμα 1: Υπάρχουν κάποια $u \in F$ με $v_1(u) > 0$ και $v_i(u) < 0$ για $i = 2, 3, \ldots, n$.

Απόδειξη του βήματος 1:

Η απόδειξη αυτού του βήματος θα γίνει με επαγωγή.

- Για $n = 2$ παρατηρούμε ότι $\mathcal{O}_{P_1} \not\subseteq \mathcal{O}_{P_2}$ και $\mathcal{O}_{P_2} \not\subseteq \mathcal{O}_{P_1}$, εφ' όσον οι δακτύλιοι εκτίμησης είναι γνήσιοι μέγιστοι υποδακτύλιοι του F (από το θεώρημα 1.2). Επομένως μπορούμε να βρούμε $y_1 \in \mathcal{O}_{P_1} \setminus \mathcal{O}_{P_2}$ και $y_2 \in \mathcal{O}_{P_2} \setminus \mathcal{O}_{P_1}$. Τότε

  $$v_1(y_1) \geq 0, v_2(y_1) < 0, v_2(y_2) < 0 \text{ και } v_2(y_2) \geq 0.$$

  Το στοιχείο $u := y_1/y_2$ έχει την ιδιότητα $v_1(u) > 0, v_2(u) < 0$ που είναι ακριβώς αυτή που θέλαμε.

- Για $n > 2$ έχουμε με επαγωγή από την υπόθεση ένα στοιχείο y με

  $$v_1(y) > 0, v_2(y) < 0, \ldots, v_{n-1}(y) < 0.$$

  Αν $v_n(y) < 0$ η απόδειξη τελειώνει. Στην περίπτωση που $v_n(y) \geq 0$ διαλέγουμε z με $v_1(z) > 0, v_n(z) < 0$ και θέτουμε $u := y + z^r$. Εδώ $r \geq 1$ επιλέγεται με τέτοιο τρόπο, ώστε $r \cdot v_i(z) \neq v_i(y)$ για $i = 1, 2, \ldots, n-1$ (αυτό είναι προφανώς πιθανό). Έπεται ότι

  $$v_1(u) \geq \min\{v_1(y), r \cdot v_1(z)\} > 0$$

  και

  $$v_i(u) = \min\{v_i(y), r \cdot v_i(z)\} < 0 \text{ για } i = 2, 3, \ldots, n.$$

  (Παρατηρούμε ότι ισχύει η αυστηρή τριγωνική ανισότητα.)

Βήμα 2:

Υπάρχουν $w \in F$ έτσι, ώστε $v_1(w-1) > r_1$ και $v_i(w) > r_i$ για $i = 2, 3, \ldots, n$.

Απόδειξη του βήματος 2:

Επιλέγουμε το u με τον ίδιο ακριβώς τρόπο που αυτό έγινε στο βήμα 1 και θέτουμε $w := (1 + u^s)^{-1}$. Για επαρκώς μεγάλο $s \in \mathbb{N}$ έχουμε

$$v_1(w-1) = v_1\left[-u^s(1+u^s)^{-1}\right] = s \cdot v_1(u) > r_1$$

και

$$v_i(w) = -v_i(1+u^s) = -s \cdot v_i(u) > r_i \text{ για } i = 2, 3, \ldots, n.$$

Βήμα 3

Δοθέντων $y_1, y_2, \ldots, y_n \in F$ υπάρχει ένα στοιχείο $z \in F$ με $v_i(z - y_i) > r_i$ για $i = 1, 2, \ldots, n$.

Απόδειξη του βήματος 3:

Διαλέγουμε $s \in \mathbb{Z}$ έτσι, ώστε $v_i(y_j) \geq s$ για όλα τα $i, j \in \{1, 2, \ldots, n\}$. Από το βήμα 2 υπάρχουν $w_1, w_2, \ldots, w_n$ με $v_i(w_i - 1) > r_i - s$ και $v_i(w_j) > r_i - s$ για $j \neq i$. Τότε το

$$z := \sum_{j=1}^{n} y_j w_j$$

έχει τις επιθυμητές ιδιότητες.

Από το βήμα 3 μπορούμε να βρούμε $z \in F$ με $v_i(z - x_i) > r_i, i = 1, 2, \ldots, n$. Έπειτα διαλέγουμε z_i με $v_i(z_i) = r_i$. Και πάλι από το βήμα 3 υπάρχει z' με $v_i(z' - z_i) > r_i$ για $i = 1, 2, \ldots, n$. Έπεται ότι

$$v_i(z') = v_i\big[(z' - z_i) + z_i\big] = \min\{v_i(z' - z_i), v_i(z_i)\} = r_i.$$

Έστω τώρα ότι $x := z + z'$. Θα είναι

$$v_i(x - x_i) = v_i\big[(z - x_i) + z'\big] = \min\{v_i(z - x_i), v_i(z')\} = r_i. \qquad \blacksquare$$

Πόρισμα 1.4. Κάθε σώμα συναρτήσεων έχει άπειρου πλήθους θέσεις.

Απόδειξη:

Η απόδειξη του πορίσματος αυτού μπορεί να γίνει με δύο τρόπους.

- (*Α΄ τρόπος*) Υποθέτουμε ότι υπάρχουν πεπερασμένου πλήθους θέσεις, έστω $P_1, P_2, \ldots, P_n$. Από το θεώρημα (1.5) βρίσκουμε ένα μη μηδενικό στοιχείο $x \in F$ με $v_{P_i}(x) > 0$, για $i = 1, 2, \ldots, n$. Τότε το x είναι υπερβατικό πάνω από το K εφ' όσον έχει ρίζες, αλλά δεν έχει πόλους. Αυτό όμως είναι άτοπο σύμφωνα με το πόρισμα 1.2.
- (*Β΄ τρόπος*) Αν το σώμα των σταθερών K είναι άπειρο, τότε το $K(x)$ έχει άπειρου πλήθους θέσεις βαθμού 1. Αν το σώμα των σταθερών είναι πεπερασμένο τότε υπάρχουν απείρου πλήθους ανάγωγα πολυώνυμα πάνω από το K[8]. $\blacksquare$

Πρόταση 1.6. Έστω F/K ένα σώμα συναρτήσεων και $P_1, P_2, \ldots, P_r$ ρίζες του στοιχείου $x \in F$. Τότε

$$\sum_{i=1}^{r} v_{P_i}(x) \cdot \deg P_i \leq [F : K(x)].$$

Απόδειξη:

Θέτουμε $v_i := v_{P_i}, f_i := \deg P_i$ και $e_i := v_i(x)$. Για κάθε i υπάρχει ένα στοιχείο t_i με

$$v_i(t_i) = 1 \text{ και } v_k(t_i) = 0 \text{ για } k \neq i.$$

Μετά διαλέγουμε $s_{i_1}, s_{i_2}, \ldots, s_{i_{f_i}} \in \mathcal{O}_{P_i}$ έτσι, ώστε τα $s_{i_1}(P), s_{i_2}(P), \ldots, s_{i_{f_i}}(P)$ να σχηματίζουν μία βάση του σώματος κλάσης υπολοίπων F_{P_i} πάνω από το K. Με εφαρμογή του θεωρήματος 1.5 μπορούμε να βρούμε $z_{ij} \in F$ έτσι, ώστε για όλα τα i, j να ισχύει το εξής

$$v_i(s_{ij} - z_{ij}) > 0 \text{ και } v_k(z_{ij}) \geq e_k \text{ για } k \neq i. \tag{1.39}$$

Για τα στοιχεία

$$t_i^a \cdot z_{ij} \text{ με } 1 \leq i \leq r,\ 1 \leq j \leq f_i,\ 0 \leq a \leq e_i,$$

[8] Αν υπάρχουν πεπερασμένου πλήθους ανάγωγα πολυώνυμα πάνω από το K, έστω $f_1, f_2, \ldots, f_n$, τότε το $f_1 f_2 \cdots f_n + 1$ είναι ένα πολυώνυμο με θετικό βαθμό που δεν διαιρείται από τα f_i και έτσι μπορούμε να το συμπεριλάβουμε ως παράγοντα. Άτοπο!

απαιτούμε να είναι γραμμικώς ανεξάρτητα πάνω από το $K(x)$. Το πλήθος τους είναι

$$\sum_{i=1}^{r} f_i e_i = \sum_{i=1}^{r} v_{P_i}(x) \cdot \deg P_i.$$

Υποθέτουμε ότι υπάρχει ένας μη τετριμμένος γραμμικός συνδιασμός

$$\sum_{i=1}^{r} \sum_{j=1}^{f_i} \sum_{a=0}^{e_i-1} \varphi_{ija} t_i^a z_{ij} = 0 \tag{1.40}$$

πάνω από το $K(x)$. Χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι $\varphi_{ija} \in K[x]$ και τα φ_{ija} δεν είναι όλα διαιρετά από το x. Τότε υπάρχουν δείκτες $k \in \{1, 2, \ldots, r\}$ και $c \in \{0, 1, \ldots, e_k - 1\}$ τέτοιοι, ώστε

$$x | \varphi_{kja} \text{ για κάθε } a < c \text{ και κάθε } j \in \{1, 2, \ldots, f_k\}$$

$$\text{και } x \nmid \varphi_{kjc} \text{ για κάποια } j \in \{1, 2, \ldots, f_k\}. \tag{1.41}$$

Πολλαπλασιάζουμε την (1.40) με t_k^{-c} και παίρνουμε

$$\sum_{i=1}^{r} \sum_{j=1}^{f_i} \sum_{a=0}^{e_i-1} \varphi_{ija} t_i^a t_k^{-c} z_{ij} = 0 \tag{1.42}$$

- Για $i \neq k$, όλα τα αθροίσματα της (1.42) είναι στο P_k

  $v_k(\varphi_{ija} t_i^a t_k^{-c} z_{ij}) = v_k(\varphi_{ija}) + a v_k(t_i) - c v_k(t_k) + v_k(z_{ij}) \geq 0 + 0 - c + e_k > 0.$

- Για $i = k$ και $a < c$, έχουμε

  $$v_k(\varphi_{kja} t_k^{a-c} z_{kj}) \geq e_k + a - c \geq e_k - c > 0.$$

  (Το $x | \varphi_{kja}$ και επομένως $v_k(\varphi_{kja}) \geq e_k$)

- Για $i = k$ και $a > c$, έχουμε

  $$v_k(\varphi_{kja} t_k^{a-c} z_{kj}) \geq a - c > 0.$$

Συνδυάζοντας τα προηγούμενα με την (1.42) έχουμε

$$\sum_{j=1}^{f_k} \varphi_{kjc} z_{kj} \in P_k. \tag{1.43}$$

Παράτηρούμε ότι $\varphi_{kjc}(P_k) \in K$ και όχι όλα τα $\varphi_{kjc}(P_k) = 0$ (από την (1.41)). Έτσι η (1.43) δίνει ένα μη τετριμμένο γραμμικό συνδιασμό

$$\sum_{j=1}^{f_k} \varphi_{kjc}(P_k) z_{kj}(P_k) = 0 \tag{1.44}$$

πάνω από το K. Αυτό όμως είναι άτοπο διότι τα $z_{k_1}(P_k), z_{k_2}(P_k), \ldots, z_{kf_k}(P_k)$, σχηματίζουν μία βάση του F_{P_k}/K. ■

Πόρισμα 1.5. Σε ένα σώμα συναρτήσεων F/K κάθε στοιχείο $x(\neq 0) \in F$ έχει πεπερασμένου πλήθους ρίζες και πόλους.

Απόδειξη:

Αν το x είναι σταθερό τότε δεν έχει ούτε ρίζες ούτε πόλους. Αν το x είναι υπερβατικό πάνω από το K, το πλήθος των ριζών είναι μικρότερο ή ίσο του $[F : K(x)]$ λόγω της πρότασης 1.6. Ομοίως το x^{-1} έχει πεπερασμένου πλήθους ρίζες άρα το x έχει πεπερασμένου πλήθους πόλους. ■

1.4 Διαιρέτες

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

Ορισμός 1.22. Η ελεύθερη αβελιανή ομάδα η οποία παράγεται από τις θέσεις του F/K συμβολίζεται με D_F και λέγεται *ομάδα των διαιρετών του* F/K. Τα στοιχεία του D_F λέγονται *διαιρέτες* του F/K.

Με άλλα λόγια ένας διαιρέτης είναι ένα τυπικό άθροισμα της μορφής

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

Ορισμός 1.23. Ο φορέας του D ορίζεται ως εξής

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

Πολλές φορές είναι βολικό να γράφουμε

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

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

Ορισμός 1.24.

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

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

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

(iii) Το *μηδενικό στοιχείο* της ομάδας των διαιρετών D_F είναι ο διαιρέτης

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

(iv) Για $Q \in \mathbb{P}_F$ και $D = \sum n_P P \in D_F$ ορίζουμε

$$v_Q(D) := n_Q.$$

Επομένως

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

και

$$D = \sum_{P \in \text{supp}D} v_P(D) \cdot P.$$

(v) Μία μερική διάταξη στο D_F ορίζεται ως εξής

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

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

(vii) Ο βαθμός ενός διαιρέτη ορίζεται μέσω της σχέσης

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

η οποία παράγει τον ακόλουθο ομοιομορφισμό

$$\deg : D_F \longrightarrow \mathbb{Z}.$$

Ορισμός 1.25. Έστω $x(\neq 0) \in F$. Ας συμβολίσουμε επίσης με Z (αντίστοιχα N) το σύνολο των ριζών (αντίστοιχα πόλων) του x στο $\mathbb{P}_F$. Τότε ορίζουμε

(i) τον *μηδενικό διαιρέτη του* x μέσω της

$$(x)_0 := \sum_{P \in Z} v_P(x)P, \tag{1.45}$$

(ii) τον *πόλο διαιρέτη του* x μέσω της

$$(x)_\infty := \sum_{P \in N} \big[-v_P(x)\big]P, \tag{1.46}$$

(iii) τον *κύριο διαιρέτη του* x μέσω της

$$(x) := (x)_0 - (x)_\infty. \tag{1.47}$$

Προφανώς

$$(x)_0 \geq 0,\ (x)_\infty \geq 0,\ (x) = \sum_{P \in \mathbb{P}_\mathbb{F}} v_P(x)P. \tag{1.48}$$

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

$$x \in K \Leftrightarrow (x) = 0.$$

Ορισμός 1.26. Το σύνολο

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

ονομάζεται *ομάδα κύριων διαιρετών του* F/K. Αυτή είναι μία υποομάδα του D_F εφ' όσον για $x, y(\neq 0) \in F$,

$$(xy) = \sum_{P \in \mathbb{P}_\mathbb{F}} v_P(xy)P = \sum_{P \in \mathbb{P}_\mathbb{F}} \big[v_P(x) + v_P(y)\big]P =$$

$$\sum_{P \in \mathbb{P}_\mathbb{F}} v_P(x)P + \sum_{P \in \mathbb{P}_\mathbb{F}} v_P(y)P = (x) + (y).$$

Ορισμός 1.27. Η ομάδα πηλίκο $\mathcal{C}_F := D_F/P_F$ ονομάζεται ομάδα κλάσης διαιρετών. Για ένα διαιρέτη $D \in D_F$, το αντίστοιχο στοιχείο στην ομάδα πηλίκο $\mathcal{C}_F$ συμβολίζεται με $[D]$, ο διαιρέτης κλάσης του D.

Ορισμός 1.28. Δύο διαιρέτες $D, D' \in D_F$ είναι ισοδύναμοι (συμβ. $D \sim D'$) αν $[D] = [D']$. [9] , δηλαδή $D = D' + (x)$ για κάποια $x \in F \setminus \{0\}$.

[9] Η σχέση αυτή είναι σχέση ισοδυναμίας αφού,

Ορισμός 1.29. Για έναν διαιρέτη $A \in D_F$ θέτουμε

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

Αυτός ο ορισμός μας λέει ότι αν

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

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

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

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

Σχόλια 1.7. Έστω ότι $A \in D_F$. Τότε

(i) Το $x \in \mathcal{L}(A)$ αν και μόνο αν $v_P(x) \geq -v_P(A)$ για όλα τα $P \in \mathbb{P}_\mathbb{F}$.

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

Απόδειξη:

(i) Εφ' όσον $x \in \mathcal{L}(A) \Leftrightarrow x \in F$ όπου $(x) \geq -A \Leftrightarrow \sum v_P(x)P \geq -\sum v_P(A)P \Leftrightarrow v_P(x) \geq -v_P(A)$.

(ii) ($\Rightarrow$) Αν $\mathcal{L}(A) \neq \{0\}$ τότε υπάρχει $x \in \mathcal{L}(A)$ με $(x) \geq -A$. Άρα $A' = (x) + A \geq 0$.
($\Leftarrow$) Αν $A \sim A'$ τότε υπάρχει διαιρέτης $x \in F \setminus \{0\}$ έτσι, ώστε $A' = (x) + A \geq 0$. Άρα $x \in \mathcal{L}(A)$ αφού $(x) \geq -A$. ■

Λήμμα 1.3. Έστω ότι $A \in D_F$. Τότε έχουμε ότι

(i) Το $\mathcal{L}(A)$ είναι διανυσματικός χώρος πάνω από το K[10].

(i) $[D] = [D']$, άρα $D \sim D'$.

(ii) Αν $D \sim D'$ τότε $[D] = [D']$. Άρα $[D'] = [D]$. Οπότε $D' \sim D$.

(iii) Αν $D \sim D'$ και $D' \sim D''$ τότε $[D] = [D']$ και $[D'] = [D'']$. Οπότε $[D] = [D'']$, δηλαδή $D \sim D''$.

[10] Έστω ότι το K είναι ένα σώμα. Ένας διανυσματικός χώρος πάνω από το K (ή ένας K διανυσματικός χώρος) αποτελείται από μία αβελιανή, ως προς την πρόσθεση, ομάδα V, η οποία είναι εφοδιασμένη με μία πράξη βαθμωτού πολλαπλασιασμού των στοιχείων του V με τα στοιχεία του K από αριστερά τέτοια, ώστε για κάθε $a, b \in K$ και $\alpha, \beta \in V$ να ικανοποιούνται τα εξής

(α') $a \cdot \alpha \in V$

(β') $a(b\alpha) = (ab)\alpha$

(γ') $(a + b)\alpha = (a\alpha) + (b\alpha)$

(δ') $a(\alpha + \beta) = (a\alpha) + (a\beta)$

(ε') $1 \cdot \alpha = \alpha$.

Τα στοιχεία του V λέγονται διανύσματα και τα στοιχεία του K βαθμωτά. Κάποια απλά παραδείγματα διανυσματικών χώρων είναι τα ακόλουθα

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

Απόδειξη:

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

$$v_P(x+y) \geq \min\{v_P(x), v_P(y)\} \geq -v_P(A)$$

(μέσω του σχόλιου 1.7) και

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

(επίσης μέσω του σχόλιου 1.7). Άρα $x+y$ και ax ανήκουν στο $\mathcal{L}(A)$. Επομένως ο $\mathcal{L}(A)$ είναι ένας διανυσματικός χώρος.

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

$$\varphi : \begin{cases} \mathcal{L}(A) \to F \\ \\ x \longmapsto xz \end{cases}$$

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

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

και

$$\varphi(ax) = (ax)z = a(xz) = a\big(\varphi(x)\big).$$

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

$$\varphi' : \begin{cases} \mathcal{L}(A') \to F \\ \\ x \longmapsto xz^{-1} \end{cases}$$

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

Λήμμα 1.4. Ισχύουν τα ακόλουθα

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

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

(α′) Αν το F είναι μία επέκταση του σώματος K, τότε μπορούμε να δούμε το F ως ένα διανυσματικό χώρο πάνω από το K στο οποίο η πρόσθεση των διανυσμάτων ταυτίζεται με τη συνήθη πρόσθεση στο F και ο βαθμωτός πολλαπλασιασμός ταυτίζεται με τον συνήθη πολλαπλασιασμό του σώματος F. Οι ιδιότητες από α' ως ε' του διανυσματικού χώρου προκύπτουν άμεσα από από τις ιδιότητες που ικανοποιούνται από το σώμα F.

(β′) Για κάθε σώμα K μπορούμε να δούμε τον $K[x]$ ως διανυσματικό χώρο πάνω από το K, στον οποίο η πρόσθεση διανυσμάτων ταυτίζεται με την συνήθη πρόσθεση πολυωνύμων του $K[x]$ και το βαθμωτό γινόμενο ενός στοιχείου του $K[x]$ με ένα στοιχείο του K ταυτίζεται με το συνηθισμένο γινόμενο στον $K[x]$. Οι ιδιότητες από α' ως ε' του διανυσματικού χώρου προκύπτουν άμεσα από τις ιδιότητες που ικανοποιούνται από την ακέραια περιοχή $K[x]$.

Απόδειξη:

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

Αντιστρόφως αν $x(\neq 0) \in \mathcal{L}(0)$ τότε $(x) \geq 0$. Αυτό σημαίνει ότι το x δεν έχει πόλους άρα από το πόρισμα 1.2, $x \in K$ επομένως $\mathcal{L}(0) \subseteq K$. Άρα $\mathcal{L}(0) = K$.

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

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

Λήμμα 1.5. Έστω A, B διαιρέτες του F/K με $A \leq B$. Τότε θα έχουμε ότι $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ και $\dim\big[\mathcal{L}(B)/\mathcal{L}(A)\big] \leq \deg B - \deg A$.

Απόδειξη:

Αν $x \in \mathcal{L}(A)$ τότε $(x) \geq -A \geq -B$. Άρα $x \in \mathcal{L}(B)$ και έτσι $\mathcal{L}(A) \subseteq \mathcal{L}(B)$.
Για να αποδείξουμε την δεύτερη σχέση θα υποθέσουμε αρχικά ότι $B = A + P$ για κάποια $P \in \mathbb{P}_F$. Διαλέγουμε ένα στοιχείο $t \in F$ με $v_P(t) = v_P(B) = v_P(A) + 1$. Για $x \in \mathcal{L}(B)$ έχουμε

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

από όπου

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

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

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

Το x ανήκει στον πυρήνα της ψ αν και μόνο αν

$$v_P(xt) > 0 \Leftrightarrow v_P(x) + v_P(t) > 0 \Leftrightarrow v_P(x) > -v_P(t) = -v_P(B) = -v_P(A) - 1,$$

δηλαδή $v_P(x) \geq -v_P(A)$. Άρα $\ker(\psi) = \mathcal{L}(A)$ και η ψ δίνει μία K-γραμμική «$1-1$» απεικόνιση από το $\mathcal{L}(B)/\mathcal{L}(A)$ στο F_P. Οπότε

$$\dim\big[\mathcal{L}(B)/\mathcal{L}(A)\big] \leq \dim F_P = \deg B - \deg A. \qquad \blacksquare$$

Πρόταση 1.7. Για κάθε διαιρέτη $A \in D_F$, ο χώρος $\mathcal{L}(A)$ είναι ένας πεπερασμένης διάστασης διανυσματικός χώρος πάνω από το K. Ακριβώς αν $A = A_+ - A_-$ με A_+, A_- θετικούς διαιρέτες, τότε $\dim \mathcal{L}(A) \leq \deg A_+ + 1$.

Απόδειξη:

Αφού ισχύει ότι $A \leq A_+$ θα είναι $\mathcal{L}(A) \subseteq \mathcal{L}(A_+)$. Αρκεί λοιπόν να δείξουμε ότι $\dim \mathcal{L}(A_+) \leq \deg A_+ + 1$.

Τώρα $0 \leq A_+$ οπότε από το λήμμα 1.5

$$\dim\big[\mathcal{L}(A_+)/\mathcal{L}(0)\big] \leq \deg A_+ - \deg 0 = \deg A_+.$$

Όμως από το λήμμα 1.4 $\mathcal{L}(0) = K$, άρα

$$\dim \mathcal{L}(A_+) = \dim\big[\mathcal{L}(A_+)/\mathcal{L}(0)\big] + 1$$

και έτσι

$$\dim\big[\mathcal{L}(A_+)/\mathcal{L}(0)\big] = \dim \mathcal{L}(A_+) - 1.$$

Επομένως $\dim \mathcal{L}(A_+) - 1 \leq \deg A_+$ ή $\dim \mathcal{L}(A_+) \leq \deg A_+ + 1$. ■

Ορισμός 1.30. Για $A \in D_F$, ο ακέραιος $\dim A := \dim \mathcal{L}(A)$ ονομάζεται *διάσταση του διαιρέτη* A.

Ένα από τα πιό σημαντικά προβλήματα της θεωρίας των αλγεβρικών σωμάτων συναρτήσεων είναι ο υπολογισμός της διάστασης ενός διαιρέτη.

Θεώρημα 1.6. Κάθε κύριος διαιρέτης έχει βαθμό μηδέν.
Αν $x \in F/K$ και $(x)_0$ (αντίστοιχα $(x)_\infty$) ο μηδενικός διαιρέτης του x (αντίστοιχα ο πόλος διαιρέτης του x), τότε

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

Απόδειξη:

Θέτουμε $n := [F : K(x)]$ και $B := (x)_\infty = \sum_{i=1}^{r} -v_{P_i}(x)P$ όπου $P_1, P_2, \ldots, P_r$ είναι όλοι πόλοι του x. Τότε

$$\deg B = \sum_{i=1}^{r} v_{P_i}(x^{-1}) \cdot \deg P_i \leq [F : K(x)] = n$$

από την πρόταση 1.6. Οπότε μένει να δείξουμε ότι $n \leq \deg B$.

Διαλέγουμε μία βάση $u_1, u_2, \ldots, u_n$ του $F/K(x)$ και έναν διαιρέτη $C \geq 0$ έτσι, ώστε $u_i \geq -C$ για $i = 1, 2, \ldots, n$. Οπότε έχουμε

$$\dim(lB + C) \geq n(l + 1) \text{ για όλα τα } l \geq 0, \tag{1.49}$$

το οποίο προκύπτει διότι $x^i u_j \in \mathcal{L}(lB + C)$ για $0 \leq i \leq l,\ 1 \leq j \leq n$ (τα στοιχεία αυτά είναι γραμμικώς ανεξάρτητα πάνω από το K εφόσον τα $u_1, u_2, \ldots, u_n$ είναι γραμμικώς ανεξάρτητα πάνω από το $K(x)$). Θέτοντας $c := \deg C$ παίρνουμε

$$n(l + 1) \leq \dim(lB + C) \leq l \cdot \deg B + c + 1$$

μέσω της πρότασης 1.7. Έτσι

$$l(\deg B - n) \geq n - c - 1 \tag{1.50}$$

για όλα τα $l \in \mathbb{N}$. Το δεξί μέλος της (1.50) είναι ανεξάρτητο του l, επομένως η (1.50) ισχύει μόνο όταν $\deg B \geq n$. Άρα

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

Εφόσον όμως $(x)_0 = (x^{-1})_\infty$, έχουμε ότι

$$\deg(x)_0 = \deg(x^{-1})_\infty = [F : K(x^{-1})] = [F : K(x)]. \qquad ■$$

Πόρισμα 1.6.

(i) Έστω A, A' διαιρέτες με $A \sim A'$. Τότε έχουμε $\dim A = \dim A'$ και $\deg A = \deg A'$.

(ii) Αν $\deg A < 0$ τότε $\dim A = 0$

(iii) Για έναν διαιρέτη με βαθμό μηδέν τα επόμενα είναι ισοδύναμα:

(α') A είναι κύριος

(β') $\dim A \geq 1$

(γ') $\dim A = 1$.

Απόδειξη:

(i) Αν $A \sim A'$ τότε από Λήμμα 1.3 $\mathcal{L}(A) \simeq \mathcal{L}(A')$ άρα $\dim \mathcal{L}(A) = \dim \mathcal{L}(A')$ οπότε από τον ορισμό 1.30 $\dim A = \dim A'$ και

$$\deg A = \sum_{P \in \mathbb{P}_F} v_P(A) \deg P = \sum_{P \in \mathbb{P}_F} v_P(A') \deg P = \deg A'. \tag{1.51}$$

(ii) Υποθέτουμε ότι $\dim A > 0$ τότε από το σχόλιο 1.7 υπάρχει κάποιος διαιρέτης $A' \sim A$ με $A' \geq 0$ και επομένως $\deg A = \deg A' \geq 0$ άτοπο γιατί $\deg A < 0$ άρα αν $\deg A < 0$ τότε $\dim A = 0$.

(iii) (α') $\Rightarrow$ (β') Αν $A = (x)$ είναι κύριος τότε $x^{-1} \in \mathcal{L}(A)$ οπότε $\dim A \geq 1$. (β') $\Rightarrow$ (γ') Έστω $\dim A \geq 1$ και $\deg A = 0$ τότε $A \sim A'$ για κάποιο $A' \geq 0$ (από σχόλιο 1.7). Τότε $A \geq 0$ και $\deg A' = 0$ άρα $A' = 0$ οπότε $\dim A = \dim A' = \dim 0 = 1$ από λήμμα 1.4. (γ') $\Rightarrow$ (α') Υποθέτω ότι $\dim A = 1$ και $\deg A = 0$. Επιλέγω $0 \neq z \in \mathcal{L}(A)$, τότε $(z) + A \geq 0$. Εφόσον $\deg((z) + A) = 0$ έπεται ότι $(z) + A = 0$ επομένως $A = -(z) = z^{-1}$ είναι κύριος. ■

Παραδείγματα 1.3. Θεωρούμε το σώμα των ρητών συναρτήσεων $F = K(x)$. Για $0 \neq z \in K(x)$ έχουμε $z = af(x)/g(x)$ με $a \in K\backslash\{0\}$, $f(x)$, $g(x) \in K[x]$ με συντελεστή μεγιστοβάθμιου όρου ίσο με 1 και σχετικά πρώτα. Έστω $f(x) = \prod_{i=1}^{r} p_i(x)^{n_i}$, $g(x) = \prod_{j=1}^{s} q_j(x)^{m_j}$ όπου $p_i(x)$, $q_j(x) \in K[x]$ πολυώνυμα ανάγωγα, με συντελεστή μεγιστοβάθμιου όρου ίσο με 1. Τότε ο κύριος διαιρέτης του z στο $D_{K(x)}$ είναι της μορφής

$$(z) = \sum_{i=1}^{n} n_i P_i - \sum_{j=1}^{s} m_j Q_j + (\deg g - \deg f) P_\infty \tag{1.52}$$

όπου P_i (αντίστοιχα Q_j) είναι οι θέσεις που αντιστοιχούν στα $p_i(x)$ (αντίστοιχα $q_j(x)$). Επομένως σε αυθαίρετα σώματα συναρτήσεων, οι κύριοι διαιρέτες χρησιμοποιούνται στην ανάλυση σε ανάγωγα πολυώνυμα, αυτό ισχύει και στο ρητό σώμα συναρτήσεων. □

Σχόλια 1.8. Δείξαμε στην πρόταση 1.7 ότι $\dim A \leq 1 + \deg A$ για κάθε διαιρέτη $A \geq 0$. Αυτό στην πραγματικότητα ισχύει για διαιρέτες με βαθμό μεγαλύτερο ή ίσο του μηδενός.

Απόδειξη:

Έστω $\dim A > 0$, τότε $A \sim A'$ για κάποιο $A' \geq 0$ από σχόλιο 1.7 οπότε $\dim A = \dim A' \leq 1 + \deg A' = 1 + \deg A$ από πόρισμα 1.6 άρα $\deg A \geq 0$. ■

Πρόταση 1.8. Υπάρχει μία σταθερά $\gamma \in \mathbb{Z}$ τέτοια ώστε για όλους τους διαιρέτες $A \in D_F$ να ισχύει:

$$\deg A - \dim A \leq \gamma. \tag{1.53}$$

Το γ δεν εξαρτάται από τον διαιρέτη A, εξαρτάται μόνο από το σώμα των συναρτήσεων F/K.

Απόδειξη:

$$A_1 \leq A_2 \Rightarrow \deg A_1 - \dim A_1 \leq \deg A_2 - \dim A_2 \tag{1.54}$$

από το λήμμα 1.5. Έστω $x \in F \backslash K$ και $B := (x)_\infty$, τότε υπάρχει ένας διαιρέτης $C \geq 0$ (εξαρτάται από το x) έτσι ώστε $\dim(lB + C) \geq (l+1)\deg B$ για όλα τα $l \geq 0$ (σχέση (1.49)). Αλλά ισχύει και:

$$\dim(lB + C) \leq \dim(lB) + \deg C \tag{1.55}$$

(από λήμμα 1.5). Συνδυάζοντας αυτές τις ανισότητες έχουμε:

$$\dim(lB) \geq (l+1)\deg B - \deg C = \deg(lB) + \deg B - \deg C =$$

$$\deg(lB) + ([F : K(x)] - \deg C). \tag{1.56}$$

Επομένως

$$\deg(lB) - \dim(lB) \leq \gamma \quad \text{για κάθε} \quad l > 0. \tag{1.57}$$

Θέλουμε τώρα να δείξουμε ότι ισχύει η (1.57) αν αντικαταστήσουμε το lB με οποιοδήποτε διαιρέτη $A \in D_F$.

Απαίτηση: Όταν δίνεται διαιρέτης A τότε υπάρχουν διαιρέτες A_1, D και ένας ακέραιος $l \geq 0$ έτσι ώστε $A \leq A_1$, $A_1 \sim D$ και $D \leq lB$.

Χρησιμοποιώντας αυτή την απαίτηση έχουμε

$$\begin{aligned} \deg A - \dim A &\leq \deg A_1 - \dim A_1 \quad (\text{από την (1.54) }) \\ &= \deg D - \dim D \quad (\text{από πόρισμα 1.6}) \\ &\leq \deg(lB) - \dim(lB) \quad (\text{από την (1.54) }) \\ &\leq \gamma \quad (\text{από την (1.57) }). \end{aligned} \tag{1.58}$$

Απόδειξη της απαίτησης: Επιλέγουμε $A_1 \geq A$ έτσι ώστε $A_1 \geq 0$. Τότε

$$\begin{aligned} \dim(lB - A_1) &\geq \dim(lB) - \deg A_1 \quad (\text{από λήμμα 1.5}) \\ &\leq \deg(lB) - \gamma - \deg A_1 \quad (\text{από την (1.57) }) \\ &> 0 \end{aligned} \tag{1.59}$$

για αρκετά μεγάλο l.
Έτσι υπάρχει κάποιο στοιχείο $0 \neq z \in \mathcal{L}(lB - A_1)$. Θέτοντας $D := A_1 - (z)$ παίρνουμε $A_1 \sim D$ και $D \leq A_1 - (A_1 - lB) = lB$ όπως θέλαμε. ■

Ορισμός 1.31. Το *γένος* g του F/K ορίζεται ως εξής:

$$g := \max\{\deg A - \dim A + 1 \mid A \in D_F\}. \tag{1.60}$$

Το γένος είναι η πιο σημαντική σταθερά ενός σώματος συναρτήσεων.

Σχόλια 1.9. Το γένος του F/K είναι ένας μη αρνητικός ακέραιος.

Απόδειξη:

Στον ορισμό 1.31 θέτω $A = 0$ τότε

$$\deg(0) - \dim(0) + 1 = 0 - 1 + 1 = 0 \tag{1.61}$$

άρα $g \geq 0$. ■

Θεώρημα 1.7. (Riemann) Έστω F/K ένα σώμα συναρτήσεων με γένος g.

(i) Για κάθε διαιρέτη $A \in D_F$,

$$\dim A \geq \deg A + 1 - g \tag{1.62}$$

(ii) Υπάρχει ένας ακέραιος c, εξαρτώμενος από το F/K έτσι ώστε $\dim A = \deg A + 1 - g$ οποτεδήποτε $\deg A \geq c$.

Απόδειξη:

(i) Από τον ορισμό του γένους έχουμε:

$$g \geq \deg A - \dim A + 1 \tag{1.63}$$

άρα

$$\dim A \geq \deg A + 1 - g. \tag{1.64}$$

(ii) Επιλέγουμε έναν διαιρέτη A_0 με

$$g = \deg A_0 - \dim A_0 + 1 \tag{1.65}$$

και θέτουμε

$$c := \deg A_0 + g. \tag{1.66}$$

Αν $\deg A \geq c$ τότε

$$\dim(A - A_0) \geq \deg(A - A_0) + 1 - g = \deg A - \deg A_0 + 1 - g \geq$$
$$c - \deg A_0 + 1 - g \geq 1 \tag{1.67}$$

Έτσι υπάρχει ένα στοιχείο $0 \neq z \in \mathcal{L}(A - A_0)$. Θεωρούμε τον διαιρέτη $A' := A + (z)$ ο οποίος είναι μεγαλύτερος ή ίσος του A_0 και έχουμε

$$\begin{aligned} \deg A - \dim A &= \deg A' - \dim A' \quad (\text{από πόρισμα 1.6}) \\ &\geq \deg A_0 - \dim A_0 \quad (\text{από λήμμα 1.5}) \\ &= g - 1 \end{aligned} \tag{1.68}$$

οπότε $\dim A \leq \deg A + 1 - g$. ■

Παραδείγματα 1.4. Θα δείξουμε ότι το ρητό σώμα των συναρτήσεων $K(x)/K$ έχει γένος $g = 0$. Έστω P_∞ ο πόλος διαιρέτης του x. Θεωρούμε για $r \geq 0$ τον διανυσματικό χώρο $\mathcal{L}(rP_\infty)$. Τότε τα $1, x, \ldots, x^r$ ανήκουν στον $\mathcal{L}(rP_\infty)$ οπότε $r + 1 \leq \dim(rP_\infty) = \deg(rP_\infty) + 1 - g = r + 1 - g$ για αρκετά μεγάλο r. Άρα $g \leq 0$, εφόσον όμως $g \geq 0$ για κάθε σώμα συναρτήσεων έχουμε $g = 0$.

Κεφάλαιο 2

Διαφορικά ενός αλγεβρικού σώματος συναρτήσεων

Σε αυτό το κεφάλαιο, θεωρούμε ένα αλγεβρικό σώμα συναρτήσεων F/K μιας μεταβλητής. K είναι το πλήρες σώμα σταθερών του F και K είναι τέλειο[1].

2.1 Παράγωγοι και διαφορικά

Ορισμός 2.1. Έστω M ένα module πάνω από το F (δηλαδή ένας διανυσματικός χώρος πάνω από το F). Μία απεικόνιση $\delta : F \to M$ λέμε ότι είναι μία *παράγωγος του* F/K αν η δ είναι k-γραμμική και ο κανόνας γινομένου $\delta(u \cdot v) = u \cdot \delta(v) + v \cdot \delta(u)$ ισχύει για κάθε u, $v \in F$.

Ορισμός 2.2. Έστω K ένα σώμα και $1 \in K$ είναι το ουδέτερο στοιχείο του πολλαπλασιασμού. Για κάθε ακέραιο $m > 0$ έστω $\underline{m} = 1+1+1+\cdots+1 \in K$ (m προσθετέοι). Αν $\underline{m} \neq 0$ (το μηδενικό στοιχείο του K) για όλα τα $m > 0$, λέμε ότι το K έχει χαρακτηριστική μηδέν (συμβολίζω $charK = 0$). Αλλιώς υπάρχει μοναδικός πρώτος αριθμός $p \in \mathbb{N}$ τέτοιος ώστε $\underline{p} = 0$ και το K λέμε τότε ότι έχει χαρακτηριστική p. Ο συμβολισμός που χρησιμοποιούμε είναι $charK = p$. Αν $charK = 0$, τότε το K περιέχει το σώμα $\mathbb{Q}$ των ρητών αριθμών. Αν $charK = p > 0$, το K περιέχει το σώμα $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Σε ένα σώμα με χαρακτηριστική $p > 0$, έχουμε $(a+b)^q = a^q + b^q$ για όλα τα a, $b \in K$ και $q = p^j$, $j \geq 0$.

Λήμμα 2.1. (Ιδιότητες της δ) Έστω $\delta : F \to M$ μία παράγωγος του F/K στο M. Τότε έχουμε:

(i) $\delta(a) = 0$ για κάθε $a \in K$

(ii) $\delta(z^n) = nz^{n-1} \cdot \delta(z)$ για $z \in F$ και $n \geq 0$

(iii) Αν $charK = p > 0$, τότε $\delta(z^p) = 0$ για κάθε $z \in F$

(iv) $\delta(x/y) = \frac{(y \cdot \delta(x) - x \cdot \delta(y))}{y}$ για x, $y \in F$ και $y \neq 0$.

[1] Βλέπε ορισμό 2.5

Απόδειξη:

(i) $\delta(\alpha x) = a \cdot \delta(x) + x \cdot \delta(a),\ \ a \in K,\ \ x \in F$ όμως δ $K-$γραμμική άρα

$$a \cdot \delta(x) = a \cdot \delta(x) + x \cdot \delta(a)$$

οπότε $x \cdot \delta(a) = 0$ άρα για $x = 1,\ \delta(a) = 0$.

(ii) Αποδεικνύεται με επαγωγή. Πράγματι για $n = 0$,

$$\delta(z^0) = 0 \cdot z^{-1} \cdot \delta(z) \quad \text{ή} \quad \delta(1) = 0$$

ισχύει λόγω του (1). Έστω ότι ισχύει για $n = k$, δηλαδή

$$\delta(z^k) = k \cdot z^{k-1} \cdot \delta(z).$$

Θα δείξουμε ότι ισχύει και για την τιμή $n = k+1$, δηλαδή θα δείξουμε ότι $\delta(z^{k+1}) = (k+1) \cdot z^k \cdot \delta(z)$.

$$\begin{aligned} \delta(z^{k+1}) &= \delta(z^k \cdot z) \\ &= z^k \cdot \delta(z) + z \cdot \delta(z^k) \\ &= z^k \cdot \delta(z) + z \cdot k \cdot z^{k-1} \cdot \delta(z) \\ &= z^k \cdot \delta(z) + k \cdot z^k \cdot \delta(z) \\ &= (k+1) \cdot z^k \cdot \delta(z) \end{aligned}$$

Άρα $\delta(z^n) = n \cdot z^{n-1} \cdot \delta(z)$ για $z \in F$ και $n \geq 0$.

(iii) Αν $charK = p > 0$, τότε $\delta(z^p) = p \cdot z^{p-1} \cdot \delta(z) = 0,\ \forall z \in F$.

(iv) $0 = \delta(1) = \delta\Big(y \cdot \frac{1}{y}\Big) = y \cdot \delta\Big(\frac{1}{y}\Big) + \frac{1}{y} \cdot \delta(y)$ άρα $\delta\Big(\frac{1}{y}\Big) = -\frac{1}{y^2} \cdot \delta(y)$.

$$\begin{aligned} \delta\Big(\frac{x}{y}\Big) &= \delta\Big(x \cdot \frac{1}{y}\Big) \\ &= x \cdot \delta\Big(\frac{1}{y}\Big) + \frac{1}{y} \cdot \delta(x) \\ &= x \cdot \Big(-\frac{1}{y^2} \cdot \delta(y)\Big) + \frac{1}{y} \cdot \delta(x) \\ &= \frac{-x}{y^2} \cdot \delta(y) + \frac{\delta(x)}{y} \\ &= \frac{y \cdot \delta(x) - x \cdot \delta(y)}{y^2}. \end{aligned}$$

Ορισμός 2.3. Έστω $f(x) \in K[x]$ ένα πολυώνυμο με συντελεστή μεγιστοβάθμιου όρου ίσο με 1 και βαθμού $d \geq 1$. Σε μία κατάλληλη επέκταση σώματος $L \supseteq K$, το $f(x)$ γράφεται $f(x) = \prod_{i=1}^{d}(x - a_i)$. Το $f(x)$ λέγεται *διαχωρίσιμο* αν $a_i \neq a_j$ για όλα τα $i \neq j$, διαφορετικά το f είναι ένα μη διαχωρίσιμο πολυώνυμο.

Αν $charK = 0$, όλα τα ανάγωγα πολυώνυμα είναι διαχωρίσιμα. Αν $charK = p > 0$, ένα ανάγωγο πολυώνυμο $f(x) = \sum a_i x^i \in K[x]$ είναι διαχωρίσιμο αν και μόνο αν $a_i \neq 0$ για κάποια $i \not\equiv 0 mod p$.

Η παράγωγος του $f(x) = \sum a_i x^i \in K[x]$ ορίζεται με τον συνηθισμένο τρόπο δηλαδή $f'(x) = \sum i a_i x^{i-1}$. Ένα ανάγωγο πολυώνυμο $f(x) \in K[x]$ είναι διαχωρίσιμο αν και μόνο αν $f'(x) \neq 0$.

Ορισμός 2.4. Έστω L/K μία αλγεβρική επέκταση σώματος. Ένα στοιχείο $a \in L$ λέγεται διαχωρίσιμο πάνω από το K αν το ελάχιστο πολυώνυμο του $p(x) \in K[x]$ είναι διαχωρίσιμο πολυώνυμο.

L/K είναι μία διαχωρίσιμη επέκατση αν όλα τα $a \in L$ είναι διαχωρίσιμα πάνω από το K. Αν $charK = 0$, τότε όλες οι αλγεβρικές επεκτάσεις L/K είναι διαχωρίσιμες.

Ορισμός 2.5. Ένα σώμα K λέγεται *τέλειο* αν όλες οι αλγεβρικές επεκτάσεις L/K είναι διαχωρίσιμες. Σώματα με χαρακτηριστική 0 είναι πάντα τέλεια. Ένα σώμα K με χαρακτηριστική $p > 0$ είναι τέλειο αν και μόνο αν κάθε $a \in K$ μπορεί να γραφεί $a = \beta^p$ για κάποια $\beta \in K$. Όλα τα πεπερασμένα σώματα είναι τέλεια.

Ορισμός 2.6. Ένα στοιχείο $x \in F$ ονομάζεται *διαχωριστικό* στοιχείο του F/K αν $F/K(x)$ είναι μία διαχωρίσιμη αλγεβρική επέκταση.

Λήμμα 2.2. Έστω x ένα διαχωριστικό στοιχείο του F/K και δ_1, $\delta_2 : F \to M$ παράγωγοι του F/K με $\delta_1(x) = \delta_2(x)$. Τότε $\delta_1 = \delta_2$.

Απόδειξη:

Από το λήμμα 2.1 έπεται ότι για ένα πολυώνυμο
$f(x) = \sum a_i x^i \in K[x]$ ισχύει $\delta_j(f(x)) = (\sum i a_i x^{i-1}) \cdot \delta_j(x)$ για $j = 1, 2$ οπότε $\delta_1(f(x)) = \delta_2(f(x))$. Για ένα αυθαίρετο στοιχείο $z = f(x)/g(x) \in K(x)$ από το λήμμα 2.1 (4) έπεται ότι

$$\delta_1(z) = \frac{g(x) \cdot \delta_1(f(x)) - f(x) \cdot \delta_1(g(x))}{g(x)^2} =$$

$$\frac{g(x) \cdot \delta_2(f(x)) - f(x) \cdot \delta_2(g(x))}{g(x)^2} = \delta_2(z) \tag{2.1}$$

Επομένως οι περιορισμοί των δ_1, δ_2 στο $K(x)$ είναι ίσοι.

Τώρα θεωρούμε ένα στοιχείο $y \in F$. Έστω $h(T) = \sum u_i T^i \in K(x)[T]$ το ελάχιστο πολυώνυμο του $K(x)[T]$ πάνω από το $K(x)$. Εφαρμόζουμε την δ_j $(j = 1, 2)$ στην $h(y) = 0$ και έχουμε

$$0 = \delta_j(h(y)) = \delta_j(\sum u_i y^i) = \sum (u_i \delta_j(y^i) + y^i \delta_j(u_i)) =$$

$$(\sum i u_i y^{i-1}) \cdot \delta_j(y) + \sum y^i \cdot \delta_j(u_i) \tag{2.2}$$

Αφού το y είναι διαχωρίσιμο πάνω από το $K(x)$ η παράγωγος του $h'(y) = \sum i u_i y^{i-1}$ δεν μηδενίζεται άρα $\delta_j(y) = \frac{-1}{h'(y)} \sum y^i \delta_j(u_i)$ για $j = 1, 2$. Εφόσον $u_i \in K(x)$ ξέρουμε ότι $\delta_1(u_i) = \delta_2(u_i)$ επομένως $\delta_1(y) = \delta_2(y)$. ■

Πρόταση 2.1.

(i) Έστω E/F είναι μία πεπερασμένη διαχωρίσιμη επέκταση του F και $\delta_0 : F \to N$ είναι μία παράγωγος του F/K σε κάποιο σώμα $N \supseteq E$. Τότε η δ_0 μπορεί να επεκταθεί σε μία παράγωγο $\delta : E \to N$. Αυτή η επέκταση ορίζεται μοναδικά από την δ_0.

(ii) Αν $x \in F$ ένα διαχωριστικό στοιχείο του F/K και $N \supseteq F$ είναι κάποιο σώμα, τότε υπάρχει μοναδική παράγωγος $\delta : F \to N$ του F/K με την ιδιότητα $\delta(x) = 1$.

Απόδειξη:

(i) Για να αποδείξουμε την ύπαρξη της δ_0, θεωρούμε δύο απεικονίσεις από τον δακτύλιο πολυωνύμων $F[T]$ στον $N[T]$, δηλαδή

$$s(T) = \sum s_i T^i \mapsto s'(T) := \sum i s_i T^{i-1} \tag{2.3}$$

και

$$s(T) = \sum s_i T^i \mapsto s^0(T) := \sum \delta_0(s_i) T^i \tag{2.4}$$

Αυτές οι δύο απεικονίσεις είναι k-γραμμικές και επαληθεύουν τον κανόνα του γινομένου. Τώρα διαλέγουμε ένα στοιχείο $u \in E$ τέτοιο ώστε $E = F(u)$. Έστω $f(T) \in F(T)$ το ελάχιστο πολυώνυμο του u πάνω από το F και θέτω $n := [E : F] = \deg f(T)$. Κάθε $y \in E$ έχει μοναδική αναπαράσταση $y = h(u)$ με $h(T) \in F[T]$ και $\deg h(T) < n$. Ορίζουμε την $\delta : E \to N$ με

$$\delta(y) := h^0(u) - \frac{f^0(u)}{f'(u)} \cdot h'(u) \tag{2.5}$$

το $f'(u) \neq 0$ εφόσον το u είναι διαχωρίσιμο πάνω από το F. Θα δείξουμε ότι η δ είναι παράγωγος του E η οποία επεκτείνει την δ_0. Αν $y \in F$ τότε $h(T) = y$, $h'(T) = 0$ και $h'(T) = \delta_0(y)$ οπότε η (2.5) γίνεται:

$$\delta(y) = \delta_0(y). \tag{2.6}$$

Η δ είναι k-γραμμική και θα δείξουμε τώρα ότι επαληθεύει και τον κανόνα του γινομένου. Έστω $y,\ z \in E$, $y = h(u)$, $z = g(u)$ με $\deg h(T) < n$ και $\deg g(T) < n$. Γράφουμε $g(T) \cdot h(T) = c(T) \cdot f(T) + r(T)$ με $c(T)$, $r(T) \in F[T]$ και $\deg r(T) < n$, οπότε $y \cdot z = c(u) \cdot f(u) + r(u) = r(u)$. Επομένως

$$\delta(y \cdot z) = (r^0 - \frac{f^0}{f'} r')(u) = \frac{1}{f'(u)} \cdot (r^0 \cdot f' - f^0 \cdot r')(u) =$$

$$\frac{1}{f'(u)} \cdot ((gh - cf)^0 \cdot f' - f^0 (gh - cf)')(u) \tag{2.7}$$

Υπολογίζουμε τους όρους $(gh - cf)^0$ και $(gh - cf)'$ χρησιμοποιώντας τον κανόνα του γινομένου και παρατηρώντας ότι $f(u) = 0$

$$\begin{aligned} (gh - cf)^0 &= (gh)^0 - (cf)^0 = g^0 h + g h^0 - c^0 f - c f^0 \\ (gh - cf)' &= (gh)' - (cf)' = g' h + g h' - c' f - c f' \end{aligned} \tag{2.8}$$

Τότε η (2.7) γίνεται

$$\delta(y \cdot z) = \frac{1}{f'(u)} (g^0 h f' + g h^0 f' - c f^0 f' - f^0 g' h - f^0 g h' + f^0 c f')(u) \tag{2.9}$$

ή

$$\delta(y \cdot z) = \frac{1}{f'(u)} (g^0 h f' + g h^0 f' - f^0 g' h - f^0 g h')(u) \tag{2.10}$$

και από την (2.5) έχουμε

$$y \cdot \delta(z) + z \cdot \delta(y) = h(u) \cdot (g^0 - \frac{f^0}{f'} \cdot g')(u) + g(u) \cdot (h^0 - \frac{f^0}{f'}h')(u) =$$

$$\frac{1}{f'(u)} \cdot (hg^0f' - hf^0g' + gh^0f' - gf^0h')(u) \tag{2.11}$$

Από τις (2.10) και (2.11) έχουμε $\delta(y \cdot z) = y \cdot \delta(z) + z \cdot \delta(y)$. Άρα η δ επαληθεύει τον κανόνα του γινομένου. Η μοναδικότητα έπεται από το λήμμα 2.2.

(ii) Για να δείξουμε την ύπαρξη μιας παραγώγου $\delta : F \to N$ με $\delta(x) = 1$ είναι αρκετό να δείξουμε ότι υπάρχει μία παράγωγος $\delta_0 : K(x) \to N$ του $K(x)/K$ με $\delta_0(x) = 1$. Ορίζουμε την δ_0 ως εξής:

$$\delta_0\left(\frac{f(x)}{g(x)}\right) := \frac{g(x) \cdot f'(x) - f(x) \cdot g'(x)}{(g(x))^2} \tag{2.12}$$

όπου $f(x)$, $g(x) \in K[x]$ και η $f'(x)$ εκφράζει την τυπική παράγωγο του $f(x)$ στο $K[x]$. Η (2.12) είναι καλά ορισμένη, k-γραμμική και επαληθεύει τον κανόνα του γινομένου άρα είναι μία παράγωγος του $K(x)/K$.

$$\delta_0(x) = \delta_0(\frac{x}{1}) = \frac{1(x)' - x(1)'}{1^2} = \frac{1-0}{1} = 1 \tag{2.13}$$

Η μοναδικότητα έπεται από το λήμμα 2.2. ■

Ορισμός 2.7.

(i) Έστω x ένα διαχωριστικό στοιχείο του σώματος συναρτήσεων F/K. Η μοναδική παράγωγος $\delta_x : F \to F$ του F/K με την ιδιότητα $\delta_x(x) = 1$ ονομάζεται η *παράγωγος με εκτίμηση στο* x.

(ii) Έστω

$$Der_F := \{\eta : F \to F \mid \eta \quad \text{είναι μία παράγωγος του} \quad F/K\}.$$

Για η_1, $\eta_2 \in Der_F$ και $z, u \in F$ ορίζουμε

$$(\eta_1 + \eta_2)(z) := \eta_1(z) + \eta_2(z) \tag{2.14}$$

και

$$(u \cdot \eta_1)(z) := u \cdot \eta_1(z) \tag{2.15}$$

$\eta_1 + \eta_2$ και $u \cdot \eta_1$ είναι παράγωγοι του F/K και Der_F είναι ένα F-module και λέγεται το module των παραγώγων του F/K.

Λήμμα 2.3. Έστω x ένα διαχωριστικό στοιχείο του F/K. Τότε ισχύουν τα ακόλουθα:

(i) Για κάθε παράγωγο $\eta \in Der_F$, έχουμε $\eta = \eta(x) \cdot \delta_x$. Ειδικότερα, Der_F είναι ένα μονοδιάστατο F-module.

(ii) (Κανόνας αλυσίδας) Αν y είναι ένα άλλο διαχωριστικό στοιχείο του F/K, τότε

$$\delta_y = \delta_y(x) \cdot \delta_x \tag{2.16}$$

(iii) Για $t \in F$, έχουμε $\delta_x(t) \neq 0 \Leftrightarrow t$ είναι ένα διαχωριστικό στοιχείο.

Απόδειξη:

(i) Θεωρούμε δύο παραγώγους η και $\eta(x) \cdot \delta_x$ του F/K στο F. Εφόσον $(\eta(x) \cdot \delta_x)(x) = \eta(x) \cdot \delta_x(x) = \eta(x)$ και το x είναι διαχωριστικό στοιχείο από το λήμμα 2.2 έπεται ότι $\eta(x) \cdot \delta_x = \eta$.

(ii) Στο (1) θέτουμε $\eta = \delta_y$ άρα

$$\delta_y = \delta_y(x) \cdot \delta_x \tag{2.17}$$

(iii) Έστω t διαχωριστικό στοιχείο,

$$1 = \delta_t(t) = \delta_t(x) \cdot \delta_x(t) \tag{2.18}$$

(από τον ορισμό του δ_t και τον κανόνα της αλυσίδας). Οπότε $\delta_x(t) \neq 0$. Υποθέτουμε τώρα ότι το t δεν είναι διαχωριστικό. Αν $charK = 0$, τότε $t \in K$ και $\delta_x(t) = 0$ εφόσον όλες οι παράγωγοι του F/K μηδενίζονται στο K. Αν $charK = p > 0$, τότε $t = u^p$ για $u \in F$ και $\delta_x(t) = \delta_x(u^p) = 0$ από το λήμμα 2.1. Οπότε για $t \in F$ έχουμε $\delta_x(t) \neq 0 \Leftrightarrow t$ είναι διαχωριστικό στοιχείο. ■

Ορισμός 2.8.

(i) Στο σύνολο $Z := \{(u, x) \in F \times F \mid x \quad \text{είναι διαχωριστικό}\}$ ορίζουμε την σχέση $\sim$ ως εξής:

$$(u, x) \sim (v, y) :\Leftrightarrow v = u \cdot \delta_y(x). \tag{2.19}$$

Αυτή είναι μία σχέση ισοδυναμίας στο Z.

(ii) Ορίζουμε την κλάση ισοδυναμίας του $(u, x) \in Z$ με την σχέση $\sim$ να είναι το udx και το ονομάζουμε διαφορικό του F/K. Η κλάση ισοδυναμίας του $(1, x)$ ορίζεται να είναι το dx. Παρατηρούμε ότι από την (2.19)

$$udx = vdy \Leftrightarrow v = u \cdot \delta_y(x). \tag{2.20}$$

(iii) Έστω $\Delta_F := \{udx \mid u \in F, \quad \text{και} \quad x \in F \quad \text{είναι διαχωριστικό}\}$ είναι το σύνολο όλων των διαφορικών του F/K. Ορίζουμε το άθροισμα δύο διαφορικών udx και $vdy \in \Delta_F$ ως εξής: Διαλέγουμε ένα διαχωριστικό στοιχείο z τότε

$$udx = (u \cdot \delta_z(x))dz \tag{2.21}$$

και

$$vdy = (v \cdot \delta_z(y))dz, \tag{2.22}$$

και έχουμε

$$udx + vdy := (u \cdot \delta_z(x) + v \cdot \delta_z(y))dz \tag{2.23}$$

Ο ορισμός (2.23) είναι ανεξάρτητος από την επιλογή του z. Ομοίως ορίζουμε $w \cdot (udx) := (wu)dx \in \Delta_F$ για $w \in F$ και $udx \in \Delta_F$. Οπότε το Δ_F με αυτόν τον τρόπο γίνεται ένα F-module.

(iv) Για ένα μη διαχωριστικό στοιχείο $t \in F$, ορίζουμε $dt := 0$ (το μηδενικό στοιχείο του Δ_F) έτσι έχουμε την απεικόνιση

$$d : \begin{cases} F \to \Delta_F \\ t \mapsto dt \end{cases} . \tag{2.24}$$

Το ζεύγος (Δ_F, d) ονομάζεται *module διαφορικό του* F/K (για συντομία θα αναφέρουμε το Δ_F ως module διαφορικό του F/K).

Πρόταση 2.2. (Ιδιότητες του module διαφορικού)

(i) Έστω $z \in F$ διαχωριστικό. Τότε $dz \neq 0$ και κάθε διαφορικό $w \in \Delta_F$ μπορεί με μοναδικό τρόπο να γραφεί στην μορφή $w = udz$ με $u \in F$. Οπότε Δ_F είναι ένα μονοδιάστατο F-module.

(ii) Η απεικόνιση $d : F \to \Delta_F$ που ορίζεται από την (2.24) είναι μία παράγωγος του F/K δηλαδή $d(ax) = adx$, $d(x+y) = dx + dy$ και $d(xy) = xdy + ydx$ για όλα τα $x, y \in F$ και $a \in K$.

(iii) Για $t \in F$, έχουμε $dt \neq 0 \Leftrightarrow t$ είναι διαχωριστικό.

(iv) Υποθέτω ότι $\delta : F \to M$ είναι μία παράγωγος του F/K σε κάποια F-module M. Τότε υπάρχει μοναδική F-γραμμική απεικόνιση $\mu : \Delta_F \to M$ τέτοια ώστε $\delta = \mu \circ d$.

Απόδειξη:

(i) Το διαφορικό $0 = 0dz$ είναι το μηδενικό στοιχείο του Δ_F. Το $(0, z)$ δεν είναι ισοδύναμο με το $(1, z)$ σύμφωνα με την (2.19) οπότε $dz \neq 0$. Έστω τώρα ένα αυθαίρετο διαφορικό $w \in \Delta_F$, $w = vdy$, y διαχωριστικό στοιχείο. Θέτω $u := v \cdot \delta_z(y)$. Χρησιμοποιώντας την (2.20) έχουμε $udz = (v\delta_z(y))dz = vdy = w$. Εφόσον $dz \neq 0$ και Δ_F είναι ένας διανυσματικός χώρος πάνω από το F το u είναι μοναδικό.

(ii) Ορίζουμε ένα διαχωριστικό στοιχείο $z \in F$. Για όλα τα $t \in F$ έχουμε

$$dt = \delta_z(t)dz \tag{2.25}$$

Αν t είναι διαχωριστικό τότε η (2.25) προκύπτει από την (2.20). Αν t δεν είναι διαχωριστικό τότε $dt = 0$ εξ' ορισμού και $\delta_z(t)dz = 0$ από το λήμμα 2.3. Θα χρησιμοποιήσουμε την (2.25) για να δείξουμε ότι η $d : F \to \Delta_F$ είναι μία παράγωγος του F/K. Έστω $x, y \in F$ και $a \in K$, εφόσον δ_z είναι μία παράγωγος του F/K έχουμε

$$d(ax) = \delta_z(ax)dz = (a\delta_z(x))dz = a\delta_z(x)dz = adx \tag{2.26}$$

$$d(x+y) = \delta_z(x+y)dz = (\delta_z(x) + \delta_z(y))dz =$$
$$\delta_z(x)dz + \delta_z(y)dz = dx + dy \tag{2.27}$$

$$d(xy) = \delta_z(xy)dz = (y\delta_z(x) + x\delta_z(y))dz =$$
$$y(\delta_z(x)dz) + x(\delta_z(y)dz) = ydx + xdy \tag{2.28}$$

Άρα η $d : F \to \Delta_F$ είναι μία παράγωγος του F/K.

(iii) Προκύπτει από τον ορισμό της d.

(iv) Έστω $\delta : F \to M$ μια παράγωγος του F/K. Από το (1) κάθε $w \in \Delta_F$ γράφεται $w = udz$ και μπορούμε να ορίσουμε $\mu : \Delta_F \to M$ με $\mu(w) := u \cdot \delta(z)$. Η μ είναι F-γραμμική. Για να δείξουμε ότι $\delta = \mu \circ d$ αρκεί να δείξουμε ότι

$$\delta(z) = (\mu \circ d)(z) \tag{2.29}$$

το οποίο προκύπτει από τον ορισμό της μ.

Μοναδικότητα της μ: Έστω $\nu : \Delta_F \to M$ είναι F-γραμμική και $\delta = \nu \circ d$ τότε

$$\nu(udz) = u \cdot \nu(dz) = u \cdot ((\nu \circ d)(z)) = u \cdot \delta(z) = \mu(udz) \tag{2.30}$$

Άρα $\nu = \mu$. ■

Σχόλια 2.1.

(i) Ένα διαφορικό της ειδικής μορφής $w = dx$ (με $x \in F$) λέγεται *πλήρες* (exact). Τα πλήρη διαφορικά σχηματίζουν ένα K υπόχωρο του Δ_F.

(ii) Εφόσον Δ_F είναι ένα μονοδιάστατο F-module μπορούμε να ορίσουμε το πηλίκο $w_1/w_2 \in F$ για w_1, $w_2 \in \Delta_F$ και $w_2 \neq 0$ θέτοντας

$$u = \frac{w_1}{w_2} :\Leftrightarrow w_1 = uw_2. \tag{2.31}$$

Ειδικότερα, αν $z \in F$ είναι διαχωριστικό και $y \in F$, ορίζεται το πηλίκο dy/dz και έχουμε $\delta_z(y) = \frac{dy}{dz}$, από πρόταση 2.2. Χρησιμοποιώντας αυτό μπορούμε να γράψουμε κάποιους προηγούμενους τύπους με άλλο τρόπο. Π.χ.

$$udx = vdy \Leftrightarrow v = u \cdot \frac{dx}{dy} \Leftrightarrow u = v \cdot \frac{dy}{dx} \tag{2.32}$$

και

$$\frac{dy}{dx} = \frac{dy}{dz} \cdot \frac{dz}{dx} \tag{2.33}$$

αν x και z είναι διαχωριστικά. Το (2.32) είναι ο τύπος (2.20) και το (2.33) είναι ο κανόνας της αλυσίδας.

2.2 Η P-adic πλήρωση

Το $\mathbb{R}$ είναι η πλήρωση του $\mathbb{Q}$ με μετρική την γνωστή απόλυτη τιμή. Αυτό σημαίνει: (1) το σώμα $\mathbb{Q}$ είναι πυκνό στο $\mathbb{R}$, και (2) κάθε ακολουθία Cauchy στο $\mathbb{R}$ είναι συγκλίνουσα.

Σ' αυτό το κεφάλαιο θα εισάγουμε κάτι ανάλογο, δηλαδή την πλήρωση ενός σώματος συναρτήσεων F/K με εκτίμηση σε μια θέση $P \in \mathbb{P}_F$. Αυτό θα μας εφοδιάσει με ένα πολύ χρήσιμο εργαλείο για τον υπολογισμό της παραγώγου $\frac{dz}{dt}$ (όπου t είναι ένα $P-$πρώτο στοιχείο) και επίσης θα είμαστε ικανοί να ορίσουμε το ολοκληρωτικό υπόλοιπο ενός διαφορικού σε μια θέση P.

Ορισμός 2.9. Μια διακριτή εκτίμηση ενός σώματος T είναι μια "1-1"και επί απεικόνιση $v : T \to \mathbb{Z} \cup \{\infty\}$ η οποία ικανοποιεί τα εξής:

(i) $v(x) = \infty \Leftrightarrow x = 0$

(ii) $v(x, y) = v(x) + v(y)$ για όλα τα $x, y \in T$

(iii) $v(x + y) \geq \min\{v(x), v(y)\}$ για όλα τα $x, y \in T$ (τριγωνική ανισότητα)

Το σώμα T (ή καλύτερα το ζέυγος (T, v)) ονομάζεται valued σώμα.

Η αυστηρή τριγωνική ανισότητα είναι

$$v(x + y) = \min\{v(x), v(y)\} \text{ αν } x, y \in T \text{ και } v(x) \neq v(y).$$

Μια ακολουθία $(x_n)_{n\geq 0}$ στο T είναι συγκλίνουσα αν υπάρχει ένα στοιχείο $x \in T$ (ονομάζεται όριο της ακολουθίας) για το οποίο ισχύει:
για κάθε $c \in \mathbb{R}$ υπάρχει ένας δείκτης $n_0 \in \mathbb{N}$ έτσι ώστε $v(x-x_n) \geq c$ οποτεδήποτε $n \geq n_0$.

Μια ακολουθία $(x_n)_{n\geq 0}$ ονομάζεται Cauchy ακολουθία αν έχει την ακόλουθη ιδιότητα:
για κάθε $c \in \mathbb{R}$ υπάρχει ένας δείκτης $n_0 \in \mathbb{N}$ ετσι ώστε $v(x_n - x_m) \geq c$ οποτεδήποτε $n, m \geq n_0$.

Όπως και στην πραγματική ανάλυση ισχύουν τα εξής:

(*i*) Αν μια ακολουθία $(x_n)_{n\geq 0}$ είναι συγκλίνουσα τότε το όριο της $x \in T$ είναι μοναδικό. Επομένως μπορούμε να γράφουμε $x = \lim_{n\to\infty} x_n$.

(*ii*) Κάθε συγκλίνουσα ακολουθία είναι μια ακολουθία Cauchy. Ενώ μια ακολουθία Cauchy δεν είναι πάντα συγκλίνουσα.

Ορισμός 2.10.

(i) Ένα valued σώμα T λέγεται πλήρες, αν κάθε ακολουθία Cauchy στο T είναι συγκλίνουσα.

(ii) Έστω (T, v) ένα valued σώμα. Μια πλήρωση του T είναι ένα valued σώμα $(\widehat{T}, \widehat{v})$ με τις ακόλουθες ιδιότητες:

(α') $T \subseteq \widehat{T}$ και v είναι ο περιορισμός της $\widehat{v}$ στο T.

(β') $\widehat{T}$ είναι πλήρες με μετρική την εκτίμηση $\widehat{v}$.

(γ') T είναι πυκνό στο $\widehat{T}$, δηλαδή για κάθε $z \in \widehat{T}$ υπάρχει μια ακολουθία $(x_n)_{n\geq 0}$ στο T με $\lim_{n\to\infty} x_n = z$.

Πρόταση 2.3. Για κάθε valued σώμα (T, v) υπάρχει μια πλήρωση $(\widehat{T}, \widehat{v})$. Αυτή είναι μοναδική, δηλαδή αν $(\widetilde{T}, \widetilde{v})$ είναι μια άλλη πλήρωση του (T, v) τότε υπάρχει μοναδικός ισομορφισμός $f : \widehat{T} \to \widetilde{T}$ έτσι ώστε $\widehat{v} = \widetilde{v} \circ f$. Οπότε το $(\widehat{T}, \widehat{v})$ λέγεται πλήρωση του (T, v).

Απόδειξη:

Σκιαγραφούμε την απόδειξη.

Θεωρούμε το σύνολο

$$R := \{(x_n)_{n\geq 0} \,/\, (x_n)_{n\geq 0} \text{ είναι ακολουθία Cauchy στο } T\}.$$

Το R εφοδιασμένο με τις πράξεις πρόσθεσης και πολλαπλασιασμού ακολουθιών γίνεται μεταθετικός δακτύλιος. Στο R θεωρούμε το σύνολο M των ακολουθιών που συγκλίνουν στο 0. Αποεικνύεται ότι το M είναι μέγιστο ιδεώδες του R. Η ζητούμενη πλήρωση είναι το σώμα $\widehat{T} := R/M$ όπου το T εμφυτεύεται στο $\widehat{T}$ μέσω της απεικόνισης

$$T \ni a \mapsto (a_n = a).$$

Ο έλεγχος των λεπτομερειών αφήνεται στον αναγνώστη. ■

Λήμμα 2.4. Έστω $(z_n)_{n\geq 0}$ μια ακολουθία στο πλήρες valued σώμα (T, v). Τότε έχουμε: η άπειρη σειρά $\sum_{i=0}^{\infty} z_i$ είναι συγκλίνουσα αν και μόνο αν η ακολουθία $(z_n)_{n\geq 0}$ συγκλίνει στο μηδέν.

Απόδειξη:

Υποθέτουμε ότι η $(z_n)_{n\geq 0}$ συγκλίνει στο μηδέν.

Θεωρούμε το μερικό άθροισμα $s_m : \sum_{i=0}^{m} z_i$.

Για $n > m$ έχουμε:

$$v(s_n - s_m) = v(\sum_{i=m+1}^{n} z_i) \geq \min\{v(z_i) \ / \ m < i \leq n\} \geq \min\{v(z_i) \ / \ i > m\}.$$

Εφόσον $v(z_i) \to \infty$ για $i \to \infty$ έχουμε ότι η ακολουθία $(s_n)_{n\geq 0}$ είναι ακολουθία Cauchy στο T άρα συγκλίνουσα. ■

Παρατηρήσεις 2.1. Στο $\mathbb{R}$ με την συνήθη μετρική αυτό δεν είναι σωστό

$$\frac{1}{n} \to 0 \ \text{ και η σειρά } \ \sum_{n=1}^{\infty} \frac{1}{n} \ \text{ αποκλίνει.}$$

Τώρα για την περίπτωση ενός αλγεβρικού σώματος συναρτήσεων F/K έχουμε:

Ορισμός 2.11. Έστω P μια θέση του F/K. Η πλήρωση του F με εκτίμηση στο v_P ονομάζεται *P-adic πλήρωση* του F. Συμβολίζουμε την πλήρωση αυτή με $\widehat{F}_P$ και την εκτίμηση του $\widehat{F}_P$ με v_P.

Θεώρημα 2.1. Έστω $P \in \mathbb{P}_F$ μια θέση βαθμού 1 και $t \in F$ ένα $P-$πρώτο στοιχείο. Τότε κάθε στοιχείο $z \in \widehat{F}_P$ έχει μια μοναδική αναπαράσταση της μορφής

$$z = \sum_{i=1}^{\infty} a_i t^i \ \text{ με } \ n \in \mathbb{Z} \ \text{ και } \ a_i \in K. \tag{2.34}$$

Η μορφή (2.34) λέγεται P-adic δυναμοσειρά ανάπτυξης του z με εκτίμηση στο t.

Από την άλλη, αν $(c_i)_{i\geq n}$ είναι μια ακολουθία στο K, τότε οι σειρές $\sum_{i=n}^{\infty} c_i t^i$ συγκλίνουν στο $\widehat{F}_P$ και έχουμε:

$$v_P\Big(\sum_{i=n}^{\infty} c_i t^i\Big) = \min\{i \ / \ c_i \neq 0\}.$$

Απόδειξη:

Αν $z \in \widehat{F}_P$ διαλέγω $n \in \mathbb{Z}$ με $n \leq v_P(z)$. Υπάρχει ένα στοιχείο $y \in F$ με $v_P(z-y) > n$ εφόσον F είναι πυκνό στο $\widehat{F}_P$.

Από την τριγωνική ανισότητα έχουμε:

$$v_P(z-y) \geq \min\{v_P(z), v_P(-y)\}$$

άρα $v_P(y) \geq n$ οπότε $v_P(yt^{-n}) \geq 0$.

Αφού η P είναι μια θέση βαθμού 1, υπάρχει ένα στοιχείο $a_n \in K$ με $v_P(yt^{-n} - a_n) > 0$ και

$$v_P(z - a_n t^n) = v_P((z-y) + (y - a_n t^n)) > n.$$

Ομοίως βρίσκουμε $a_{n+1} \in K$ έτσι ώστε

$$v_P(z - a_n t^n - a_{n+1} t^{n+1}) > n+1.$$

Επαναλαμβάνοντας τη διαδικασία προκύπτει μια άπειρη ακολουθία $a_n, a_{n+1}, a_{n+2}, \ldots$ στο K έτσι ώστε

$$v_P(z - \sum_{i=n}^{m} a_i t^i) > m$$

για όλα τα $m \geq n$.

Αυτό δείχνει ότι:

$$z = \sum_{i=n}^{\infty} a_i t^i.$$

Μοναδικότητα. Έστω μια άλλη ακολουθία $(b_i)_{i \geq m}$ στο K για την οποία

$$z = \sum_{i=n}^{\infty} a_i t^i = \sum_{i=m}^{\infty} b_i t^i.$$

Μπορούμε να υποθέσουμε ότι $n = m$ (διαφορετικά, αν $n < m$, ορίζουμε $b_i := 0$ για $n \leq i \leq m$).

Υποθέτουμε ότι υπάρχει κάποιο j με $a_j \neq b_j$.

Διαλέγουμε j ελάχιστο με αυτή την ιδιότητα και έχουμε για όλα τα $k > j$:

$$v_P\Big(\sum_{i=n}^{k} a_i t^i - \sum_{i=n}^{k} b_i t^i\Big) = v_P\Big((a_j - b_j)t^j + \sum_{i=j+1}^{k} (a_i - b_i)t^i\Big) = j \qquad (2.35)$$

(εφόσον $v_P((a_j - b_j)t^i) = j$ εφαρμόζεται η αυστηρή τριγωνική ανισότητα).

Από την άλλη

$$\begin{aligned} v_P\Big(\sum_{i=n}^{k} a_i t^i - \sum_{i=n}^{k} b_i t^i\Big) &= v_P\Big(\sum_{i=n}^{k} a_i t^i - z + z\sum_{i=n}^{k} b_i t^i\Big) \\ &\geq \min\Big\{v_P\Big(z - \sum_{i=n}^{k} a_i t^i\Big), v_P\Big(z - \sum_{i=n}^{k} b_i t^i\Big)\Big\} \qquad (2.36) \end{aligned}$$

Για $k \to \infty$ η (2.36) τείνει στο άπειρο αυτό σύμφωνα με την (2.35) είναι άτοπο άρα αποδείξαμε ότι η μορφή (2.34) είναι μοναδική.

Τελικά θεωρούμε μια αυθαίρετη ακολουθία $(c_i)_{i\geq n}$ στο K. Αφού $v_P(c_i t^i) \geq i$ για όλα τα i, η ακολουθία $(c_i t^i)_{i\geq n}$ συγκλίνει στο μηδέν. Οπότε από το Λήμμα 2.4 η σειρά $\sum_{i=n}^{\infty} c_i t^i$ είναι συγκλίνουσα στο $\widehat{F}_P$,

$$\sum_{i=n}^{\infty} c_i t^i =: y \in \widehat{F}_P.$$

Θέτω $j_0 := \min\{i \ / \ c_i \neq 0\}$.

Αν $j_0 = \infty$ τότε όλα τα $c_i = 0$, οπότε $y = 0$ και $v_P(y) = \infty$.

Αν $j_0 < \infty$ έχουμε για όλα τα $k \geq j_0$, $v_P\Big(\sum_{i=n}^{k} c_i t^i\Big) = j_0$ από την αυστηρή τριγωνική ανισότητα.

Εφόσον $v_P\Big(y - \sum_{i=n}^{k} c_i t^i\Big) > j_0$ για όλα τα αρκετά μεγάλα k, έχουμε:

$$\begin{aligned} v_P(y) &= v_P\Big(y - \sum_{i=n}^{k} c_i t^i + \sum_{i=n}^{k} c_i t^i\Big) \\ &= \min\Big\{v_P\Big(y - \sum_{i=n}^{k} c_i t^i\Big), v_P\Big(\sum_{i=n}^{k} c_i t^i\Big)\Big\} = j_0. \ \blacksquare \end{aligned}$$

Πρόταση 2.4. Έστω P μια θέση του F/K βαθμού 1 και $t \in F$ ένα $P-$πρώτο στοιχείο. Αν το $z \in F$ έχει την P-adic ανάπτυξη $z = \sum_{i=n}^{\infty} a_i t^i$ με συντελεστές $a_i \in K$ τότε

$$\frac{dz}{dt} = \sum_{i=n}^{\infty} i a_i t^{i-1}.$$

Απόδειξη:

Ορίζουμε την απεικόνιση $\delta : \widehat{F}_P \to \widehat{F}_P$ με

$$\delta\Big(\sum_{i=m}^{\infty} c_i t^i\Big) := \sum_{i=m}^{\infty} i c_i t^{i-1}.$$

Η δ είναι $K-$γραμμική και

$$\delta(u \cdot v) = u\delta(v) + v\delta(u)$$

για όλα τα $v, u \in \widehat{F}_P$, (δηλαδή επαληθεύει τον κανόνα του γινομένου). Επιπλέον $\delta(t) = 1$. Επομένως

$$\delta(z) = \delta_t(z) = \frac{dz}{dt}$$

για κάθε $z \in F$. $\blacksquare$

Ορισμός 2.12. Έστω P μια θέση του F/K βαθμού 1 και $t \in F$ είναι ένα $P-$πρώτο στοιχείο. Αν $z \in F$ έχει την P-adic ανάπτυξη $z = \sum_{i=n}^{\infty} a_i t^i$ με $n \in \mathbb{Z}$

και $a_i \in K$ ορίζουμε το *ολοκληρωτικό υπόλοιπο του με εκτίμηση στο P και στο t* ως εξής:

$$res_{P,t}(z) := a_{-1}.$$

Η απεικόνιση $res_{P,t} : F \to K$ είναι $K-$γραμμική και

$$res_{P,t}(z) = 0 \ \text{ αν } \ v_P(z) \geq 0. \tag{2.37}$$

Πρόταση 2.5. Έστω $s, t \in F$ είναι $P-$πρώτα στοιχεία (όπου P είναι μια θέση βαθμού 1). Τότε:

$$res_{P,s}(z) = res_{P,t}\big(z \cdot \frac{ds}{dt}\big) \ \text{ για όλα τα } \ z \in F.$$

Απόδειξη:

Η ανάπτυξη του s σε δυναμοσειρά με εκτίμηση στο t έχει την ακόλουθη μορφή

$$s = \sum_{i=1}^{\infty} c_i t^i$$

με $c_1 \neq 0$ (από Θεώρημα 2.1).

Από την πρόταση 2.4 έχουμε:

$$\frac{ds}{dt} = c_1 + \sum_{i=2}^{\infty} i c_i t^{i-1} \tag{2.38}$$

Τώρα διακρίνουμε τις παρακάτω περιπτώσεις:

(i) $v_P(z) \geq 0$. Τότε $v_P\big(z \cdot \frac{ds}{dt}\big) \geq 0$ (από την 2.38). Από την (2.37) έπεται ότι

$$res_{P,s}(z) = res_{P,t}\big(z \cdot \frac{ds}{dt}\big) = 0.$$

(ii) $z = s^{-1}$. Τότε έχουμε $res_{P,s}(s^{-1}) = 1$. Ορίζουμε την ανάπτυξη του s^{-1} σε δυναμοσειρά με εκτίμηση στο t να είναι:

$$\begin{aligned} s^{-1} &= \frac{1}{c_1 t + c_2 t^2 + \dots} \\ &= \frac{1}{c_1 t} \cdot \Big(1 + \frac{c_2}{c_1} t + \frac{c_3}{c_1} t^2 + \dots\Big)^{-1} \\ &= \frac{1}{c_1 t} \cdot \Big(1 + \sum_{r=1}^{\infty} (-1)^r \Big(\frac{c_2}{c_1} t + \frac{c_3}{c_1} t^2 + \dots\Big)^r\Big) \\ &= \frac{1}{c_1 t} \cdot \Big(1 + \frac{f_2(c_2)}{c_1} t + \frac{f_3(c_2, c_3)}{c_1^2} t^2 + \dots\Big) \end{aligned} \tag{2.39}$$

για κάποια πολυώνυμα $f_j(\mathrm{X}_2, \dots, \mathrm{X}_j) \in \mathbb{Z}[\mathrm{X}_2, \dots, \mathrm{X}_j]$. Επομένως

$$s^{-1} \cdot \frac{ds}{dt} = \frac{1}{t} + y$$

με $v_P(y) \geq 0$ (από 2.38 και 2.39).

Έχουμε:

$$res_{P,t}\Big(s^{-1} \cdot \frac{ds}{dt}\Big) = 1 + res_{P,t}(y) = 1$$

από την 1η περίπτωση.

(iii) $z = s^{-n}$ με $n \geq 2$. Τότε $res_{P,s}(s^{-n}) = 0$.

Αν $charK = 0$ τότε

$$s^{-n} \cdot \frac{ds}{dt} = \frac{1}{-n+1} \cdot \frac{d(s^{-n+1})}{dt}.$$

Γράφουμε $s^{-n+1} = \sum_{i=k}^{\infty} d_i t^i$ με $k = -n+1$ και $d_i \in K$ και παίρνουμε:

$$\frac{d(s^{-n+1})}{dt} = \sum_{i=k}^{\infty} i d_i t^{i-1}.$$

Οπότε

$$res_{P,t}\Big(s^{-n} \cdot \frac{ds}{dt}\Big) = \frac{1}{-n+1} \cdot res_{P,t}\Big(\sum_{i=k}^{\infty} i d_i t^{i-1}\Big) = 0. \tag{2.40}$$

Αν $charK \neq 0$ από τις (2.38) και (2.39) έχουμε

$$\begin{aligned} s^{-n} \cdot \frac{ds}{dt} &= \frac{1}{c_1^n t^n}(c_1 + 2c_2 t + \ldots) \cdot \Big(1 + \frac{f_2(c_2)}{c_1} t + \frac{f_3(c_2, c_3)}{c_1^2} t^2 + \ldots\Big)^n \\ &= \frac{1}{c_1^n t^n} \cdot \Big(c_1 + \frac{g_2(c_1, c_2)}{c_1} t + \frac{g_3(c_1, c_2, c_3)}{c_1^2} t^2 + \ldots\Big) \end{aligned}$$

με $g_j(\mathrm{X}_1, \ldots, \mathrm{X}_j) \in \mathbb{Z}[\mathrm{X}_1, \ldots, \mathrm{X}_j]$.

Αυτά τα πολυώνυμα είναι ανεξάρτητα από το $charK$, έχουμε:

$$res_{P,t}\Big(s^{-n} \cdot \frac{ds}{dt}\Big) = \frac{1}{c_1^{2n-1}} \cdot g_n(c_1, \ldots, c_n).$$

Από την (2.40) έπεται $g_n(c_1, \ldots, c_n) = 0$ για οποιαδήποτε στοιχεία $c_1 \neq 0, c_2, \ldots, c_n$ σε σώμα με χαρακτηριστική μηδέν. Έτσι $g_n(\mathrm{X}_1, \ldots, \mathrm{X}_n)$ πρέπει να είναι το μηδενικό πολυώνυμο στον $\mathbb{Z}[\mathrm{X}_1, \ldots, \mathrm{X}_j]$.

Οπότε η ισότητα

$$res_{P,t}\Big(s^{-n} \cdot \frac{ds}{dt}\Big) = 0 = res_{P,s}(s^{-n})$$

ισχύει για ένα σώμα με οποιαδήποτε χαρακτηριστική (για $n \geq 2$).

(iv) Έστω z ένα τυχαίο στοιχείο του F με $v_P(z) < 0$, $z = \sum_{i=-n}^{\infty} a_i s^i$ με $n \geq 1$ και $a_i \in K$. Τότε $res_{P,s}(z) = a_{-1}$ και $z = a_{-n}s^{-n} + \ldots + a_{-1}s^{-1} + y$ με $v_P(y) \geq 0$.

Χρησιμοποιώντας τα αποτελέσματα των περιπτώσεων 1, 2 και 3 έχουμε:

$$\begin{aligned} res_{P,t}\Big(z \cdot \frac{ds}{dt}\Big) &= \sum_{i=-n}^{-1} a_i \cdot res_{P,t}\Big(s^i \cdot \frac{ds}{dt}\Big) + res_{P,t}\Big(y \cdot \frac{ds}{dt}\Big) \\ &= a_{-1} \cdot res_{P,t}\Big(s^{-1} \cdot \frac{ds}{dt}\Big) \\ &= a_{-1} = res_{P,s}(z). \end{aligned}$$

■

Ορισμός 2.13. Έστω $\omega \in \Delta_F$ ένα διαφορικό και $P \in \mathbb{P}_F$ μια θέση βαθμού 1. Διαλέγω ένα $P-$πρώτο στοιχείο $t \in F$ και γράφω $\omega = udt$ με $u \in F$. Τότε ορίζουμε το *ολοκληρωτικό υπόλοιπο του* ω *στο* P ως εξής:

$$res_P(\omega) := res_{P,t}(u).$$

Παρατηρήσεις 2.2. Ο προηγούμενος ορισμός είναι ανεξάρτητος από την επιλογή του πρώτου στοιχείου t.

Πράγματι, αν s είναι ένα άλλο $P-$πρώτο στοιχείο και $\omega = udt = zds$, τότε $u = z \cdot \frac{ds}{dt}$ και

$$res_{P,s}(z) = res_{P,t}\Big(z \cdot \frac{ds}{dt}\Big) = res_{P,t}(u).$$

Κεφάλαιο 3

Το θεώρημα Riemann - Roch

Σ' αυτό το κεφάλαιο, F/K θα είναι ένα αλγεβρικό σώμα συναρτήσεων με γένος g.

Ορισμός 3.1. Για $A \in D_F$, $i(A) := \dim A - \deg A + g - 1$ ονομάζεται *index of speciality* του A.

Από το Θεώρημα Riemann έχουμε ότι ο $i(A)$ είναι μη αρνητικός ακέραιος και $i(A) = 0$ αν $\deg A$ είναι αρκετά μεγάλο.

Ορισμός 3.2. Μια *adele* του F/K είναι μια απεικόνιση

$$\alpha : \begin{cases} \mathbb{P}_F \to F \\ \\ P \mapsto \alpha_P \end{cases}$$

έτσι ώστε $\alpha_P \in \mathcal{O}_P$ για σχεδόν όλα τα $P \in \mathbb{P}_F$.

Θεωρούμε μια adele ως ένα στοιχείο του ευθύ γινομένου $\prod_{P \in \mathbb{P}_F} F$ και επομένως χρησιμοποιούμε τον συμβολισμό $\alpha = (\alpha_P)_{P \in \mathbb{P}_F}$ ή για συντομία $\alpha = (\alpha_P)$.

Το σύνολο $\mathcal{A}_F := \{\alpha / \alpha \text{ είναι μια adele του } F/K\}$ ονομάζεται *χώρος adele* του F/K. Θεωρείται διανυσματικός χώρος πάνω από το K.

Ορισμός 3.3. Μια *κύρια adele* ενός στοιχείου $x \in F$ είναι μια adele της οποίας όλες οι συνιστώσες είναι ίσες με x. Αυτό δίνει μια εμφύτευση $F \hookrightarrow \mathcal{A}_F$.

Οι εκτιμήσεις v_P του F/K επεκτείνονται στο $\mathcal{A}_F$ θέτοντας $v_P(\alpha) := v_P(\alpha_P)$ (όπου α_P είναι η P συνιστώσα της adele α).

Από τον ορισμό, $v_P(\alpha) \geq 0$ για όλα σχεδόν τα $P \in \mathbb{P}_F$.

Ορισμός 3.4. Για $A \in D_F$ ορίζουμε

$$\mathcal{A}_F(A) := \{\alpha \in \mathcal{A}_F / v_P(\alpha) \geq -v_P(A) \text{ για όλα τα } P \in \mathbb{P}_F\}$$

Το $\mathcal{A}_F(A)$ είναι $K-$υπόχωρος του $\mathcal{A}_F$.

Θεώρημα 3.1. Για κάθε διαιρέτη A, ο index of speciality είναι

$$i(A) = \dim(\mathcal{A}_F/(\mathcal{A}_F(A) + F))$$

(dim σημαίνει διάσταση του $K-$διανυσματικού χώρου).

Απόδειξη:
Βήμα 1: Έστω $A_1, A_2 \in D_F$ και $A_1 \leq A_2$. Τότε $\mathcal{A}_F(A_1) \subseteq \mathcal{A}_F(A_2)$ και

$$\dim(\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1)) = \deg A_2 - \deg A_1 \tag{3.1}$$

Απόδειξη του βήματος 1:

$$\mathcal{A}_F(A_1) := \{\alpha \in \mathcal{A}_F / v_P(\alpha) \geq -v_P(A_1)\ \forall\ P \in \mathbb{P}_F\}$$

$$\mathcal{A}_F(A_2) := \{\alpha \in \mathcal{A}_F / v_P(\alpha) \geq -v_P(A_2)\ \forall\ P \in \mathbb{P}_F\}$$

όμως

$$\begin{aligned} A_1 \leq A_2 &\Leftrightarrow v_P(A_1) \leq v_P(A_2) \\ &\Leftrightarrow -v_P(A_1) \geq -v_P(A_2) \end{aligned}$$

άρα $\mathcal{A}_F(A_1) \subseteq \mathcal{A}_F(A_2)$.

Αν $A_2 = A_1 + P$ με $P \in \mathbb{P}_F$, διαλέγουμε $t \in F$ με $v_P(t) = v_P(A_1) + 1$ και θεωρούμε την $K-$γραμμική απεικόνιση

$$\phi : \begin{cases} \mathcal{A}_F(A_2) \to F_P \\ \\ \alpha \mapsto (t\alpha_P)(P) \end{cases}$$

- αν $\phi(\alpha) = \phi(\beta)$ τότε $(t\alpha_P)(P) = (t\beta_P)(P)$ άρα $\alpha = \beta$, δηλαδή η ϕ είναι "1-1".
- είναι επί
- ο πυρήνας της είναι $\mathcal{A}_F(A_1)$

Άρα $\deg A_2 - \deg A_1 = \deg P = [F_P : K] = \dim(\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1))$.

Βήμα 2: Έστω $A_1, A_2 \in D_F$ και $A_1 \leq A_2$. Τότε

$$\dim((\mathcal{A}_F(A_2) + F)/(\mathcal{A}_F(A_1) + F)) = (\deg A_2 - \dim A_2) - (\deg A_1 - \dim A_1) \tag{3.2}$$

Απόδειξη του βήματος 2:

Έχουμε μια ακολουθία γραμμικών απεικονίσεων η οποία είναι ακριβής

$$0 \longrightarrow \mathcal{L}(A_2)/\mathcal{L}(A_1) \xrightarrow{\sigma_1} \mathcal{A}_F(A_2)/\mathcal{A}_F(A_1) \xrightarrow{\sigma_2} (\mathcal{A}_F(A_2)+F)/(\mathcal{A}_F(A_1)+F) \longrightarrow 0 \tag{3.3}$$

θα δείξουμε ότι ο πυρήνας της σ_2 περιέχεται στην εικόνα της σ_1.

Έστω $\alpha \in \mathcal{A}_F(A_2)$ με $\sigma_2(\alpha + \mathcal{A}_F(A_1)) = 0$.

Τότε $\alpha \in \mathcal{A}_F(A_1) + F$, έτσι υπάρχει κάποιο $x \in F$ με $\alpha - x \in \mathcal{A}_F(A_1)$.

Εφόσον $\mathcal{A}_F(A_1) \subseteq \mathcal{A}_F(A_2)$ έχουμε $x \in \mathcal{A}_F(A_2) \cap F = \mathcal{L}(A_2)$.

Επομένως $\alpha + \mathcal{A}_F(A_1) = x + \mathcal{A}_F(A_1) = \sigma_1(x + \mathcal{L}(A_1))$ βρίσκεται στην εικόνα της σ_1.

Από την (3.3) έχουμε

$$\begin{aligned} \dim(\mathcal{A}_F(A_2) + F)/(\mathcal{A}_F(A_1) + F) &= \dim(\mathcal{A}_F(A_2)/(\mathcal{A}_F(A_1)) - \dim(\mathcal{L}(A_2)/\mathcal{L}(A_1)) \\ &= (\deg A_2 - \deg A_1) - (\dim A_2 - \dim A_1) \end{aligned}$$

Βήμα 3: Αν B είναι ένας διαιρέτης με $\dim B = \deg B + 1 - g$ τότε

$$\mathcal{A}_F = \mathcal{A}_F(B) + F \tag{3.4}$$

Απόδειξη του βήματος 3:

Για διαιρέτη $B_1 \geq B$ έχουμε

$$\dim B_1 \leq \deg B_1 + \dim B - \deg B = \deg B_1 + 1 - g$$

αλλά και από το θεώρημα Riemann

$$\dim B_1 \geq \deg B_1 + 1 - g.$$

Επομένως

$$\dim B_1 = \deg B_1 + 1 - g \tag{3.5}$$

για κάθε $B_1 \geq B$.

Έστω $\alpha \in \mathcal{A}_F$ τότε μπορεί κανείς να βρει έναν διαιρέτη $B_1 \geq B$ έτσι ώστε $\alpha \in \mathcal{A}_F(B_1)$.
Από (3.2) και (3.5)

$$\begin{aligned} \dim(\mathcal{A}_F(B_1) + F)/(\mathcal{A}_F(B) + F) &= (\deg B_1 - \dim B_1) - (\deg B - \dim B) \\ &= (g-1) - (g-1) \\ &= 0 \end{aligned}$$

οπότε $\mathcal{A}_F(B) + F = \mathcal{A}_F(B_1) + F$.

Εφόσον $\alpha \in \mathcal{A}_F(B_1)$ έπεται ότι $\alpha \in \mathcal{A}_F(B) + F$ άρα αποδείχτηκε η (3.4).

Βήμα 4:(*τέλος της απόδειξης*)

Θεωρούμε έναν αυθαίρετο διαιρέτη A. Από το θεώρημα Riemann υπάρχει κάποιος διαιρέτης $A_1 \geq A$ έτσι ώστε $\dim A_1 = \deg A_1 + 1 - g$.

Από την (3.4)

$$\mathcal{A}_F = \mathcal{A}_F(A_1) + F$$

και χρησιμοποιώντας και την (3.2)

$$\begin{aligned} \dim(\mathcal{A}_F/\mathcal{A}_F(A) + F) &= \dim(\mathcal{A}_F(A_1) + F)/(\mathcal{A}_F(A) + F) \\ &= (\deg A_1 - \dim A_1) - (\deg A - \dim A) \\ &= (g-1) + \dim A - \deg A \\ &= i(A) \end{aligned}$$

■

Παρατηρήσεις 3.1.

(i) Οι διανυσματικοί χώροι $\mathcal{A}_F, \mathcal{A}_F(A)$ και F είναι άπειρης διάστασης, το θεώρημα (3.1) λέει ότι ο χώρος πηλίκο $\mathcal{A}_F/(\mathcal{A}_F(A)+F)$ έχει πεπερασμένη διάσταση πάνω από το K.

(ii) Μια άλλη διατύπωση του Θεωρήματος (3.1) θα μπορούσε να είναι η εξής:

Για κάθε διαιρέτη $A \in D_F$ ισχύει

$$\dim A = \deg A + 1 - g + \dim(\mathcal{A}_F/(\mathcal{A}_F(A)+F)) \tag{3.6}$$

Πόρισμα 3.1. $g = \dim(\mathcal{A}_F/(\mathcal{A}_F(0)+F))$

Απόδειξη:

$$i(0) = \dim(0) - \deg(0) + g - 1 = 1 - 0 + g - 1 = g. \quad \blacksquare$$

Ορισμός 3.5. Ένα Weil διαφορικό του F/K είναι μια $K-$γραμμική απεικόνιση $\omega : \mathcal{A}_F \to K$ η οποία μηδενίζεται στον $\mathcal{A}_F(A)+F$ για κάποιον διαιρέτη $A \in D_F$.

Ονομάζουμε $\Omega_F := \{\omega/\omega$ είναι ένα Weil διαφορικό του $F/K\}$ το module των Weil διαφορικών του F/K.

Για $A \in D_F$ έχουμε:

$$\Omega_F(A) := \{\omega \in \Omega_F/\omega \text{ μηδενίζεται στον } \mathcal{A}_F(A)+F\}$$

- Ο Ω_F είναι ένας $K-$διανυσματικός χώρος.

  Πράγματι αν ω_1 μηδενίζεται στον $\mathcal{A}_F(A_1)+F$

  και ω_2 μηδενίζεται στον $\mathcal{A}_F(A_2)+F$

  τότε $\omega_1+\omega_2$ μηδενίζεται στον $\mathcal{A}_F(A_3)+F$ για κάθε διαιρέτη A_3 με $A_3 \le A_1$ και $A_3 \le A_2$,

  και $a\omega_1$ μηδενίζεται στον $\mathcal{A}_F(A_1)+F$ για $a \in K$.

- Προφανώς $\Omega_F(A)$ είναι ένας υπόχωρος του Ω_F

Λήμμα 3.1. Για $A \in D_F$ έχουμε $\dim \Omega_F(A) = i(A)$.

Απόδειξη:

Ο $\Omega_F(A)$ είναι ισομορφικός με τον χώρο των γραμμικών μορφών του $\mathcal{A}_F/(\mathcal{A}_F(A)+F)$. Ο $\mathcal{A}_F/(\mathcal{A}_F(A)+F)$ είναι πεπερασμένης διάστασης και από το Θεώρημα (3.1) έχουμε:

$$i(A) = \dim(\mathcal{A}_F/(\mathcal{A}_F(A)+F)) = \dim \Omega_F(A). \quad \blacksquare$$

Σχόλια 3.1. Μια απλή συνέπεια του Λήμματος 3.1 είναι ότι $\Omega_F \neq 0$.

Πράγματι αν A ένας διαιρέτης βαθμού ≤ -2 τότε

$$\dim \Omega_F(A) = i(A) = \dim A - \deg A + g - 1 \ge 1$$

άρα $\Omega_F(A) \neq 0$.

Ορισμός 3.6. Για $x \in F$ και $\omega \in \Omega_F$ ορίζουμε

$$x\omega : \mathcal{A}_F \to K \ \text{ με } \ (x\omega)(\alpha) := \omega(x\alpha).$$

Το $x\omega$ είναι ένα Weil διαφορικό του F/K. Πράγματι αν ω μηδενίζεται στον $\mathcal{A}_F(A) + F$ τότε $x\omega$ μηδενίζεται στον $\mathcal{A}_F(A + (x)) + F$.

Πρόταση 3.1. Ω_F είναι ένας μονοδιάστατος διανυσματικός χώρος πάνω από το F.

Απόδειξη:

Διαλέγουμε $0 \neq \omega_1 \in \Omega_F$ (υπάρχει τέτοιο ω_1 γιατί $\Omega_F \neq 0$). Θα δείξουμε ότι για κάθε $\omega_2 \in \Omega_F$ υπάρχει κάποιο $z \in F$ ώστε $\omega_2 = z\omega_1$.

Μπορούμε να υποθέσουμε ότι $\omega_2 \neq 0$.

Επιλέγουμε $A_1, A_2 \in D_F$ έτσι ώστε $\omega_1 \in \Omega_F(A_1)$ και $\omega_2 \in \Omega_F(A_2)$.

Για ένα διαιρέτη B θεωρούμε τις $K-$γραμμικές $1-1$ και επί απεικονίσεις:

$$\varphi_i : \begin{cases} \mathcal{L}(A_i + B) \to \Omega_F(-B) \\ \\ x \mapsto x\omega_i \end{cases} \qquad (i = 1, 2).$$

Απαίτηση
Με κατάλληλη επιλογή του διαιρέτη B ισχύει

$$\varphi_1(\mathcal{L}(A_1 + B)) \cap \varphi_2(\mathcal{L}(A_2 + B)) \neq \{0\}.$$

Απόδειξη της απαίτησης:

Από την γραμμική άλγεβρα γνωρίζουμε ότι αν U_1, U_2 είναι υπόχωροι του πεπερασμένης διάστασης διανυσματικού χώρου V τότε

$$\dim(U_1 \cap U_2) \geq \dim U_1 + \dim U_2 - \dim V. \tag{3.7}$$

Έστω $B > 0$ ένας διαιρέτης με αρκετά μεγάλο βαθμό, έτσι ώστε

$$\dim(A_i + B) = \deg(A_i + B) + 1 - g \ \text{ για } \ i = 1, 2$$

(αυτό είναι δυνατόν από το Θεώρημα Riemann).

Θέτουμε

$$U_i := \varphi_i(\mathcal{L}(A_i + B) \subseteq \Omega_F(-B).$$

Εφόσον

$$\Omega_F(-B) = i(-B) = \dim(-B) - \deg(-B) + g - 1 = \deg B - (1 - g)$$

έχουμε

$$\dim U_1 + \dim U_2 - \dim \Omega_F(-B) =$$

$$\deg(A_1 + B) + 1 - g + \deg(A_2 + B) + 1 - g - (\deg B + g - 1) =$$

$$\deg B + (\deg A_1 + \deg A_2 + 3(1 - g)).$$

Οι όροι που είναι μέσα στις παρενθέσεις στην τελευταία σχέση είναι ανεξάρτητοι του B, άρα

$$\dim U_1 + dim U_2 - \dim \Omega_F(-B) > 0$$

αν ο $\deg B$ είναι αρκετά μεγάλος.

Από την (3.7) έχουμε λοιπόν ότι $U_1 \cap U_2 \neq \{0\}$ άρα και

$$\varphi_1(\mathcal{L}(A_1 + B)) \cap \varphi_2(\mathcal{L}(A_2 + B)) \neq \{0\}$$

έτσι αποδείξαμε την απαίτηση.

Διαλέγουμε τώρα $x_1 \in \mathcal{L}(A_1+B)$ και $x_2 \in \mathcal{L}(A_2+B)$ έτσι ώστε $x_1\omega_1 = x_2\omega_2 \neq 0$ οπότε $\omega_2 = (x_1 x_2^{-1})\omega_1$ όπως θέλαμε. ■

Ορισμός 3.7. $M(\omega) := \{A \in D_F/\omega$ μηδενίζεται στον $\mathcal{A}_F(A) + F\}$

(Το σύνολο αυτό το ορίζουμε γιατί θέλουμε να συνδέσουμε ένα διαιρέτη με κάθε Weil διαφορικό $\omega \neq 0$.)

Λήμμα 3.2. Έστω $0 \neq \omega \in \Omega_F$. Τότε υπάρχει ένας μοναδικά ορισμένος διαιρέτης $W \in M(\omega)$ έτσι ώστε $A \leq W$ για κάθε $A \in M(\omega)$.

Απόδειξη:

Υπάρχει μια σταθερά c, η οποία εξαρτάται μόνο από το σώμα συναρτήσεων F/K με την ιδιότητα $i(A) = 0$ για όλους τους διαιρέτες $A \in D_F$ με βαθμό $\geq c$ (αυτό είναι δυνατόν από το Θεώρημα Riemann).

Εφόσον $\dim(\mathcal{A}_F/\mathcal{A}_F(A) + F)) = i(A)$ (Θεώρημα 3.1) έχουμε ότι $\deg A < c$ για όλα τα $A \in M(\omega)$. Οπότε μπορούμε να επιλέξουμε έναν διαιρέτη $W \in M(\omega)$ με μέγιστο βαθμό.

Αν ο W δεν είναι τέτοιος ώστε $A \leq W$ για κάθε $A \in M(\omega)$ τότε υπάρχει ένας διαιρέτης $A_0 \in M(\omega)$ με $A_0 \not\leq W$ δηλαδή $v_Q(A_0) > v_Q(W)$ για κάποιο $Q \in \mathbb{P}_F$.

Θεωρούμε μια adele $\alpha = (\alpha_P) \in \mathcal{A}_F(W + Q)$. Μπορούμε να γράψουμε $\alpha = \alpha' + \alpha''$ με

$$\alpha'_P := \begin{cases} \alpha_P \ \text{ για } \ P \neq Q \\ \\ 0 \ \text{ για } \ P = Q \end{cases} \quad \text{και} \quad \alpha''_P := \begin{cases} 0 \ \text{ για } \ P \neq Q \\ \\ \alpha_Q \ \text{ για } \ P = Q \end{cases}$$

Τότε $\alpha' \in \mathcal{A}_F(W)$ και $\alpha'' \in \mathcal{A}_F(A_0)$. Επομένως

$$\omega(\alpha) = \omega(\alpha') + \omega(\alpha'') = 0.$$

Άρα ω μηδενίζεται στον $\mathcal{A}_F(W + Q) + F$, οπότε $W + Q \in M(\omega)$ άτοπο λόγω του μεγίστου βαθμού του W.

Άρα υπάρχει μοναδικά ορσιμένος διαιρέτης $W \in M(\omega)$ έτσι ώστε $A \leq W$ για κάθε $A \in M(\omega)$. ■

Ορισμός 3.8.

(i) Ο διαιρέτης (ω) ενός Weil διαφορικού $\omega \neq 0$ είναι ο διαιρέτης του F/K που ορίζεται μοναδικά και επαληθεύει τα επόμενα:

(α′) ω μηδενίζεται στον $\mathcal{A}_F((\omega)) + F$.

(β′) Αν ω μηδενίζεται στον $\mathcal{A}_F(A) + F$ τότε $A \leq (\omega)$.

(ii) Για $0 \neq \omega \in \Omega_F$ και $P \in \mathbb{P}_F$ ορίζουμε $v_P(\omega) := v_P((\omega))$.

(iii) Μια θέση P λέγεται ρίζα (αντίστοιχα πόλος) του ω αν $v_P(\omega) > 0$ (αντίστοιχα $v_P(\omega) < 0$).

ω λέγεται κανονικό στο P αν $v_P(\omega) \geq 0$ και ω λέγεται κανονικό (ή ολομορφικό) αν είναι κανονικό σε κάθε $P \in \mathbb{P}_F$.

(iv) Ένας διαιρέτης W ονομάζεται *κανονικός διαιρέτης* του F/K αν $W = (\omega)$ για $\omega \in \Omega_F$.

Σχόλια 3.2.

- $\Omega_F(A) = \{\omega \in \Omega_F / \omega = 0 \text{ ή } (\omega) \geq A\}$.
- $\Omega_F(0) = \{\omega \in \Omega_F / \omega \text{ είναι κανονικό }\}$.
- $\dim \Omega_F(0) = g$ (συνέπεια του Λήμματος 3.1 και του ορισμού 3.1)

Πρόταση 3.2.

(α) Για $0 \neq x \in F$ και $0 \neq \omega \in \Omega_F$ έχουμε $(x\omega) = (x) + (\omega)$.

(β) Δύο οποιοιδήποτε κανονικοί διαιρέτες του F/K είναι ισοδύναμοι.

Απόδειξη:

(α) Αν ω μηδενίζεται στον $\mathcal{A}_F(A)+F$ τότε $x\omega$ μηδενίζεται στον $\mathcal{A}_F(A+(x))+F$ επομένως $(\omega) + (x) \leq (x\omega)$.

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

Άρα από τις δύο αυτές σχέσεις έχουμε:

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

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

(β) Έστω $W = (\omega)$ και $W' = (\omega')$ δύο κανονικοί διαιρέτες του F/K με $0 \neq \omega,\ \omega' \in \Omega_F$. Επειδή η διάσταση του Ω_F πάνω από το F είναι 1 έχουμε ότι:

$$(\omega') = (x\omega) \ \text{ για κάποιο } \ x \in F\backslash\{0\}$$

και από το (α) έπεται ότι:

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

που σημαίνει ότι $\omega \sim \omega'$. ■

Θεώρημα 3.2. Έστω A ένας αυθαίρετος διαιρέτης και $W = (\omega)$ ένας κανονικός διαιρέτης του F/K. Τότε η απεικόνιση

$$\mu : \begin{cases} \mathcal{L}(W-A) \to \Omega_F(A) \\ \\ x \mapsto x\omega \end{cases}$$

είναι ένας ισομορφισμός από $K-$διανυσματικούς χώρους και

$$i(A) = \dim(W - A).$$

Απόδειξη:

Για $x \in \mathcal{L}(W-A)$ έχουμε

$$(x\omega) = (x) + (\omega) \geq -(W-A) + W = A$$

άρα $x\omega \in \Omega_F(A)$ από τα Σχόλια 3.2. Επομένως η μ απεικονίζει τον $\mathcal{L}(W-A)$ στον $\Omega_F(A)$.

Η μ εξ' ορισμού είναι γραμμική.

Για $x_1, x_2 \in \mathcal{L}(W-A)$ αν $x_1\omega = x_2\omega$ για $\omega \neq 0$ έχουμε $x_1 = x_2$ άρα η μ είναι και 1-1.

Για να δείξουμε ότι η μ είναι επί θεωρούμε ένα Weil διαφορικό $\omega_1 \in \Omega_F(A)$. Από την Πρόταση 3.1 $\omega_1 = x\omega$ για κάποιο $x \in F$.

Εφόσον

$$(x) + W = (x) + (\omega) = (x\omega) = (\omega_1) \geq A$$

έχουμε ότι

$$(x) \geq -(W-A)$$

άρα

$$x \in \mathcal{L}(W-A) \quad \text{και} \quad \omega_1 = \mu(x).$$

Τώρα

$$\dim \Omega_F(A) = i(A) \quad (\text{Λήμμα } 3.1)$$

και

$$\dim \Omega_F(A) = \dim(W-A)$$

άρα $i(A) = \dim(W-A)$. ■

Θεώρημα 3.3. (*Θεώρημα Riemann-Roch*)
Έστω W ένας κανονικός διαιρέτης του F/K. Τότε για κάθε $A \in D_F$,

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

Απόδειξη:

$i(A) = \dim A - \deg A + g - 1$ (ορισμός 3.1)

$i(A) = \dim(W-A)$ (από Θεώρημα 3.2)

άρα

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

ή

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

Πόρισμα 3.2. Για έναν κανονικό διαιρέτη W, έχουμε

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

Απόδειξη:

Από το Θεώρημα Riemann-Roch και το Λήμμα (1.4) έχουμε:

- Για $A = 0$
$$1 = \dim 0 = \deg 0 + 1 - g + \dim(W - 0)$$
άρα
$$\dim W = g.$$
- Για $A = W$
$$g = \dim W = \deg W + 1 - g + \dim 0$$
άρα
$$g = \deg W + 1 - g + 1$$
δηλαδή
$$\deg W = 2g - 2. \quad \blacksquare$$

Σχόλια 3.3. Από το θεώρημα Riemann ξέρουμε ότι υπάρχει κάποια σταθερά c, εξαρτώμενη από το F/K για την οποία $\dim A = \deg A + 1 - g$, όταν $\deg A \geq c$, δηλαδή $i(A) = 0$, όταν $\deg A \geq c$. Στο επόμενο θεώρημα θα διαλέξουμε $c = 2g - 1$.

Θεώρημα 3.4. Αν A είναι ένας διαιρέτης του F/K με $\deg A \geq 2g - 1$ τότε

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

Απόδειξη:

Από το Θεώρημα Riemann-Roch έχουμε

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

όπου W είναι ένας κανονικός διαιρέτης.

Εφόσον $\deg A \geq 2g - 1$ και $\deg W = 2g - 2$ έχουμε ότι

$$\deg(W - A) < 0.$$

Όμως από το Πόρισμα (1.6) έπεται ότι

$$\dim(W - A) = 0$$

άρα

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

Παρατηρήσεις 3.2. Το φράγμα $2g - 1$ είναι το καλύτερο δυνατόν εφόσον για ένα κανονικό διαιρέτη W ισχύει

$$\dim W > \deg W + 1 - g.$$

Κεφάλαιο 4

Γεωμετρικοί κώδικες Goppa

4.1 Κώδικες

Σ' αυτό το κεφάλαιο θα περιγράψουμε μερικούς γραμμικούς error-correcting, τους γεωμετρικούς κώδικες Goppa. Οι κώδικες αυτοί αποτελούν γενίκευση των Reed-Solomon κωδίκων και για να οριστούν απαιτείται χρήση της θεωρίας αλγεβρικών σωμάτων συναρτήσεων.

Οι Error-Correcting κώδικες χρησιμοποιούνται για να διορθώνονται λάθη όταν μηνύματα μεταδίδονται μέσω δικτύου με παραμβολές. Οι παρεμβολές μπορεί να είναι ανθρώπινα λάθη, πρόβλημα υπερθέρμανσης, πρόβλημα εισαγωγής της πληροφορίας κ.τ.λ. Σ' αυτές τις περιπτώσεις είναι επιθυμητό να κωδικοποιήσουμε την πληροφορία με τέτοιο τρόπο ώστε τα λάθη να αναγνωρίζονται και να διορθώνονται όταν αυτά συμβαίνουν.

Παραδείγματα 4.1. Γενικά ένα ψηφιακό σύστημα επικοινωνίας είναι όπως το επόμενο:

Το ίδιο μοντέλο μπορεί να χρησιμοποιηθεί για να περιγράψουμε ένα σύστημα αποθήκευσης πληροφοριών αν το αποθηκευτικό μέσο θεωρηθεί ως ένα κανάλι. Ένα τυπικό παράδειγμα είναι το cd.

Ας δούμε τώρα ένα πολύ απλό πράδειγμα στο οποίο τα μοναδικά μηνύματα που θέλουμε να στείλουμε είναι 'YES'και 'NO'.

Έδω έχουν γίνει δύο λάθη και το λαμβανόμενο μήνυμα 01001 διορθώνεται και γίνεται 00000 (ή 'YES') ως η πλησιέστερη λέξη για το 01001.

Σ' αυτό το κεφάλαιο με $\mathbb{F}_q$ συμβολίζουμε το πεπερασμένο σώμα με q στοιχεία (όπου q είναι δύναμη πρώτου). Θεωρούμε τον $n-$διάστατο διανυσματικό χώρο

$\mathbb{F}_q^n$ του οποίου τα στοιχεία είναι διατεταγμένες της μορφής $a = (a_1, \ldots, a_n)$ με $a_i \in \mathbb{F}_q$.

Ορισμός 4.1. Για $a = (a_1, a_2, \ldots, a_n)$ και $b = (b_1, b_2, \ldots, b_n) \in \mathbb{F}_q^n$ ορίζουμε:

- την $d(a, b) := |\{i; a_i \neq b_i\}|$.

  Η d είναι συνάρτηση και ονομάζεται *Hamming* απόσταση στον $\mathbb{F}_q^n$, μετρά το πλήθος των διαφορετικών συντεταγμένων μεταξύ των διανυσμάτων a και b επομένως σε πόσα σημεία διαφέρει η πληροφορία.

- το $w(a) := d(a, 0) = |\{i; a_i \neq 0\}|$, λέγεται *βάρος* του στοιχείου $a \in \mathbb{F}_q^n$, μας δείχνει πόσο απέχει το a από το να είναι μηδέν.

Παρατηρήσεις 4.1. Η Hamming απόσταση είναι μια μετρική στον $\mathbb{F}_q^n$, εφόσον ικανοποιεί τα εξής:

(i) $d(a, b) = 0$ αν και μόνο αν $a = b$

(ii) $d(a, b) = d(b, a)$ για όλα τα $a, b \in \mathbb{F}_q^n$

(iii) $d(a, b) \leq d(a, c) + d(c, b)$ για όλα τα $a, b, c \in \mathbb{F}_q^n$.

Τα $(i), (ii)$ είναι προφανή. Το (iii) είναι η τριγωνική ανισότητα και αποδεικνύεται ως εξής:

$d(a, b)$ είναι ο ελάχιστος αριθμός διαφορετικών συντεταγμένων μεταξύ a και b που θα θέλαμε στην μεταβολή του a σε b. Αλλά μπορούμε επίσης να μεταβάλλουμε το a σε b κάνοντας πρώτα $d(a, c)$ αλλαγές (μεταβάλλοντας το a σε c) και μετά $d(c, b)$ αλλαγές (μεταβάλλοντας το c σε b). Έτσι

$$d(a, b) \leq d(a, c) + d(c, b).$$

Παραδείγματα 4.2. Στον $\mathbb{F}_2^5$ έχουμε $d(00111, 11001) = 4$, ενώ στον $\mathbb{F}_3^4$ έχουμε $d(0122, 1220) = 3$.

Ορισμός 4.2. Ένας *κώδικας* C (πάνω από το αλφάβητο $\mathbb{F}_q$) είναι ένας γραμμικός υπόχωρος του $\mathbb{F}_q^n$. Τα στοιχεία του C ονομάζονται κωδικές λέξεις. Ονομάζουμε μήκος του C τον αριθμό n και με $\dim C$ συμβολίζουμε την διάσταση του C. Ένας $[n, k]$ κώδικας είναι ένας κώδικας με μήκος n και διάσταση k.

Παρατηρήσεις 4.2. Πιο γενικά, μπορεί κανείς να ορίσει έναν κώδικα ως ένα μη κενό υποσύνολο $C \subseteq A^n$ όπου $A \neq \emptyset$ είναι ένα πεπερασμένο σύνολο. Αν $A = \mathbb{F}_q$ και $C = \mathbb{F}_q^n$ είναι ένας γραμμικός υπόχωρος, ο C λέγεται γραμμικός κώδικας. Οι κώδικες με τους οποίους θα ασχοληθούμε είναι γραμμικοί.

Ορισμός 4.3. Η *ελάχιστη απόσταση ενός κώδικα* $C \neq 0$ συμβολίζεται με $d(C)$ και ορίζεται ως εξής:

$$d(C) := \min\{d(a, b)/a, b \in C \text{ και } a \neq b\}.$$

Ένας $[n, k]$ κώδικας με ελάχιστη απόσταση d συμβολίζετια $[n, k, d]$ κώδικας.

Σχόλια 4.1.

$$d(C) = \min\{w(c)/0 \neq c \in C\} = W(C)$$

όπου $W(C)$ το ελάχιστο βάρος του κώδικα C.

Απόδειξη:

Αν $a, b \in C$ τότε

$$d(a, b) = d(a - b, 0) = w(a - b) \tag{4.1}$$

Τώρα υπάρχουν κωδικές λέξεις x και y του κώδικα C έτσι ώστε $d(C) = d(x, y)$ και από τη σχέση (4.1)

$$d(C) = w(x - y) \geq W(C)$$

εφόσον $x - y$ είναι μια κωδική λέξη του γραμμικού κώδικα C.

Από την άλλη για κάποια κωδική λέξη $x \in C$,

$$W(C) = w(x) = d(x, 0) \geq d(C),$$

εφόσον το 0 ανήκει στον γραμμικό κώδικα C.

Άρα

$$d(C) \geq W(C) \quad \text{και} \quad W(C) \geq d(C)$$

οπότε

$$d(C) = W(C). \qquad \blacksquare$$

Παραδείγματα 4.3. Στο παράδειγμα (4.1) έχουμε τον κώδικα $\{00000, 11111\}$. Αν τα μηνύματα YES και NO αναγνωρίζονται με τα σύμβολα 0 και 1 αντίστοιχα, τότε κάθε σύμβολο του μηνύματος επαναλαμβάνεται 5 φορές. Γι' αυτό λέμε ότι αυτός είναι ένας κώδικας μήκους 5.

Ορισμός 4.4.

- Η *κατανομή βάρους* ενός $[n, k]$ κώδικα είναι ένα $(n+1)-$διάστατο διάνυσμα $(A_0, \ldots, A_n) \in \mathbb{N}_0^{n+1}$ με

  $$A_i := |\{c \in C : w(c) = i\}|.$$

  Προφανώς $A_0 = 1$ (μόνο ένα στοιχείο έχει μηδενική νόρμα) και $A_i = 0$ για $1 \leq i \leq d(C) - 1$. Δηλαδή τα A_i δίνουν τον αριθμό των κωδικών λέξεων στον C με βάρος i.

- Το πολυώνυμο $W_C(X) := \sum_{i=0}^{n} A_i X^i \in \mathbb{Z}[X]$ ονομάζεται *μετρητής βάρους* του κώδικα C.

- Για ένα κώδικα C με ελάχιστη απόσταση $d = d(C)$ θέτουμε

  $$t := [(d - 1)/2]$$

  (όπου $[x]$ δηλώνει το ακέραιο μέρος ενός πραγματικού αριθμού x, δηλαδή $x = [x] + \varepsilon$ με $[x] \in \mathbb{Z}$ και $0 \leq \varepsilon < 1$). Τότε ο C λέγεται t-error correcting.

Σχόλια 4.2. Αν $u \in \mathbb{F}_q^n$ και $d(u,c) \leq t$ για κάποιο $u \in C$ τότε c είναι η μοναδική κωδική λέξη με $d(u,c) \leq t$.

Απόδειξη:

Αν c' είναι μια άλλη κωδική λέξη με $d(u,c') \leq t$ τότε

$$d(c',c) \leq d(c',u) + d(u,c) \leq t + t = 2t = 2 \cdot \left[\frac{d-1}{2}\right] < d$$

δηλαδή $d(c',c) < d$ άτοπο γιατί $d = d(C)$ η ελάχιστη απόσταση του κώδικα C. ■

Ένας άπλος τρόπος για να περιγράψουμε έναν κώδικα C είναι να γράψουμε μια βάση για τον C.

Ορισμός 4.5. Έστω C ένας $[n,k]$ κώδικας πάνω από το $\mathbb{F}_q$. Ένας *πίνακας γεννήτρια* του C είναι ένας $k \times n$ πίνακας του οποίου οι γραμμές είναι μια βάση του C.

Ορισμός 4.6. Το *κανονικό εσωτερικό γινόμενο* στον $\mathbb{F}_q^n$ ορίζεται ως εξής

$$\langle a,b \rangle := \sum_{i=1}^{n} a_i b_i$$

για $a = (a_1, a_2, \ldots, a_n)$ και $b = (b_1, b_2, \ldots, b_n) \in \mathbb{F}_q^n$.

Ορισμός 4.7. Αν $C \subseteq \mathbb{F}_q^n$ είναι ένας κώδικας τότε

$$C^{\perp} := \{u \in \mathbb{F}_q^n / \langle u,c \rangle = 0 \ \text{ για όλα τα } c \in C\}$$

ονομάζεται *δυϊκός* του C.

Ο C λέγεται *αυτο-δυϊκός* αν $C = C^{\perp}$.

Ο C λέγεται *αυτο-ορθογώνιος* αν $C \subseteq C^{\perp}$.

Σχόλια 4.3.

(*i*) Αν C είναι ένας $[n,k]$ κώδικας πάνω από το $\mathbb{F}_q$ τότε ο $C^{\perp}$ είναι ένας $[n, n-k]$ κώδικας.

Απόδειξη:

Έστω $G = [g_{ij}]$ ένας πίνακας γεννήτρια του κώδικα C. Τότε για τα στοιχεία του $C^{\perp}$ ισχύει ότι είναι διανύσματα $v = (v_1, v_2, \ldots, v_n)$ για τα οποία

$$\sum_{j=1}^{n} g_{ij} v_j = 0 \ \text{ για } \ i = 1, 2, \ldots, k \tag{4.2}$$

Η (4.2) είναι ένα σύστημα από k ανεξάρτητες ομογενείς εξισώσεις με n αγνώστους, τότε ο χώρος λύσεων $C^{\perp}$ έχει διάσταση $n-k$.

Πράγματι αν C_1 και C_2 είναι ισοδύναμοι[1] τότε το ίδιο ισχύει και για τους $C_1^\perp$ και $C_2^\perp$. Άρα θα δείξουμε ότι $\dim(C^\perp) = n - k$ στην περίπτωση που ο C έχει πίνακα γεννήτρια της μορφής

$$G = \begin{bmatrix} 1 & \dots & 0 & a_{11} & \dots & a_{1,n-k} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & 1 & a_{k1} & \dots & a_{k,n-k} \end{bmatrix}.$$

Τότε

$$C^\perp = \{(v_1, v_2, \dots, v_n) \in \mathbb{F}_q^n \ / \ v_i + \sum_{j=1}^{n-k} a_{ij} v_{k+j},\ i = 1, 2, \dots, k\}.$$

Για κάθε μια από τις q^{n-k} επιλογές του $(v_{k+1}, \dots, v_n)$ υπάρχει μοναδικό διάνυσμα $(v_1, v_2, \dots, v_n)$ στον $C^\perp$. Άρα $|C^\perp| = q^{n-k}$ οπότε

$$\dim(C^\perp) = n - k. \qquad \blacksquare$$

(*ii*) Για κάθε $[n, k]$ κώδικα C, $(C^\perp)^\perp = C$.

Απόδειξη:

Ισχύει $C \subseteq C^\perp$ εφόσον κάθε διάνυσμα στον C είναι ορθογώνιο σε κάθε διάνυσμα στο $C^\perp$. Αλλά $\dim\left((C^\perp)^\perp\right) = n-(n-k) = k = \dim C$ άρα $C = (C^\perp)^\perp$. $\blacksquare$

(*iii*) Ειδικότερα η διάσταση ενός αυτο-δυϊκού κώδικα με μήκος n είναι $\frac{n}{2}$.

Ορισμός 4.8. Ένας πίνακας γεννήτρια H του $C^\perp$ λέγεται *parity check πίνακας* για τον C[2]. Ο H είναι ένας $(n-k) \times n$ πίνακας με τάξη $n-k$ εφόσον ο C είναι ένας $[n, k]$ κώδικας και έχουμε ότι:

$$C = \{u \in \mathbb{F}_q^n \ / \ H \cdot u^t = 0\}$$

όπου u^t εκφράζει τον ανάστροφο του u.

[1] Δύο κώδικες (πάνω από το αλφάβητο $\mathbb{F}_q$) λέγονται ισοδύναμοι αν ο ένας μπορεί να προκύψει από τον άλλο με ένα συνδυασμό πράξεων της μορφής:

(α′) Μετάθεση των θέσεων του κώδικα.

(β′) Μετάθεση των συμβόλων που εμφανίζονται σε μια σταθερή θέση.

Π.χ. Ο κώδικας

$$C = \begin{Bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{Bmatrix}$$

είναι ισοδύναμος με τον κώδικα

$$C' = \begin{Bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{Bmatrix}$$

εφαρμόζοντας την μετάθεση

$$\begin{pmatrix} 0 & 1 \\ \downarrow & \downarrow \\ 1 & 0 \end{pmatrix}.$$

στα σύμβολα στην τρίτη θέση του C και μετά ανταλλάσσοντας τις θέσεις 2 και 4.

[2] Πρόκειται για μια βάση του $C^\perp$.

Δηλαδή ένας parity check πίνακας ελέγχει αν ένα διάνυσμα $u \in \mathbb{F}_q^n$ είναι κωδική λέξη.

Ένα από τα βασικά προβλήματα της κωδικοποίησης είναι να κατασκευάζει κώδικες πάνω από ένα αλφάβητο $\mathbb{F}_q$ των οποίων η διάσταση και η ελάχιστη απόσταση να είναι μεγάλα σε σχέση με το μήκος τους. Πάντως υπάρχουν κάποιοι περιορισμοί, αν η διάσταση ενός κώδικα είναι μεγάλη τότε η ελάχιστη απόστασή του είναι μικρή. Το πιο απλό φράγμα είναι το ακόλουθο.

Πρόταση 4.1. (Singleton Bound) Για έναν $[n, k, d]$ κώδικα C ισχύει:

$$k + d \leq n + 1.$$

Απόδειξη:

Θεωρούμε έναν γραμμικό υπόχωρο $W \subseteq \mathbb{F}_q^n$ ο οποίος είναι

$$W := \{(a_1, \ldots, a_n) \in \mathbb{F}_q^n \ / \ a_i = 0 \ \text{ για όλα τα } \ i \geq d\}.$$

Κάθε $a \in W$ έχει βάρος $\leq d - 1$ άρα $W \cap C = 0$.

Αφού $\dim W = d - 1$ έχουμε:

$$\begin{aligned} k + (d-1) &= \dim C + \dim W \\ &= \dim(C + W) + \dim(C \cap W) \\ &= \dim(C + W) \leq n. \end{aligned}$$

Άρα

$$k + d \leq n + 1. \qquad \blacksquare$$

Ορισμός 4.9. Κώδικες με $k + d = n + 1$ είναι τέλειοι, τέτοιοι κώδικες λέγονται *MDS κώδικες* (maximum distance separable codes).

Αν $n \leq q + 1$, υπάρχουν MDS κώδικες πάνω από το $\mathbb{F}_q$ για όλες τις διαστάσεις $k \leq n$.

Το φράγμα Singleton δεν αναφέρει το μέγεθος του αλφαβήτου. Υπάρχουν βέβαια και άλλα φράγματα για τις παραμέτρους k και d, τα οποία είναι ισχυρότερα από το φράγμα Singleton αν το n είναι μεγάλο σε σχέση με το q.

Όπως αναφέραμε στην αρχή του κεφαλαίου ένας κώδικας C πάνω από το αλφάβητο $\mathbb{F}_q$ είναι ένας γραμμικός υπόχωρος του $\mathbb{F}_q^n$ άρα ανακεφαλαιώνοντας μπορούμε να δούμε και σχηματικά τις βασικές έννοιες της παράγραφου:

όπου $d = d(C)$ η ελάχιστη απόσταση του κώδικα C.

Τώρα θέλοντας να διορθώσουμε την "πληροφορία"x μέσω του κώδικα C επιλέγεται η κωδική λέξη που είναι πιο κοντά στο x άρα η y. Για να μπορούμε τώρα να διορθώσουμε περισσότερα λάθη θέλουμε χαμηλότερα φράγματα για την ελάχιστη απόσταση σε ένα κώδικα. Τέτοιοι κώδικες είναι οι κλασικοί κώδικες Goppa, οι οποίοι παρουσιάζουν μεγάλο ενδιφέρον και ένας από τους λόγους είναι ότι μπορεί κανείς να έχει ένα καλό χαμηλό φράγμα για την ελάχιστη απόστασή τους.

4.2 Γεωμετρικοί κώδικες Goppa

Καταρχήν θα μελετήσουμε τους κώδικες Reed Solomon πάνω από το $\mathbb{F}_q$. Οι γεωμετρικοί Goppa κώδικες είναι γενίκευση των Reed Solomon κωδίκων.

Έστω $n = q-1$ και $\beta \in \mathbb{F}_q$ ένα πρωτεύον στοιχείο της πολλαπλασιαστικής ομάδας $\mathbb{F}_q^* = \mathbb{F}_q \backslash \{0\}$, δηλαδή $\mathbb{F}_q^* = \{\beta, \beta^2, \ldots, \beta^n = 1\}$. Για έναν ακέραιο k με $1 \leq k \leq n$ θεωρούμε τον $k-$διάστατο διανυσματικό χώρο

$$\mathcal{L}_k := \{f \in \mathbb{F}_q[x] \ / \ \deg f \leq k-1\} \tag{4.3}$$

και την απεικόνιση εκτίμησης

$$ev(f) := \big(f(\beta), f(\beta^2), \ldots, f(\beta^n)\big) \in \mathbb{F}_q^n. \tag{4.4}$$

Η απεικόνιση αυτή είναι $\mathbb{F}_q-$γραμμική και "1-1" διότι ένα μη μηδενικό πολυώνυμο $f \in \mathbb{F}_q[x]$ με βαθμό $< n$ έχει λιγότερες από n ρίζες.

Επομένως

$$C_k := \Big\{\big(f(\beta), f(\beta^2), \ldots, f(\beta^n)\big) \ / \ f \in \mathcal{L}_k\Big\} \tag{4.5}$$

είναι ένας $[n,k]$ κώδικας πάνω από το $\mathbb{F}_q$ και λέγεται RS κώδικας (Reed Solomon κώδικας).

Το βάρος μιας κωδικής λέξης $0 \neq c = ev(f) \in C_k$ δίνεται από την

$$\begin{aligned} \omega(c) &= n - \mid \{i \in \{1, \ldots, n\}; f(\beta^i) = 0\} \mid \\ &\geq n - \deg f \\ &\geq n - (k-1). \end{aligned}$$

Άρα η ελάχιστη απόσταση d του C_k ικανοποιεί την ανισότητα $d \geq n+1-k$. Από την άλλη από το φράγμα Singleton ισχύει $d \leq n+1-k$. Άρα $d = n+1-k$, δηλαδή οι Reed Solomon κώδικες είναι MDS (maximum distance separable) κώδικες πάνω από το $\mathbb{F}_q$.

Παρατηρούμε επίσης ότι οι Reed Solomon κώδικες είναι μικρότεροι σε σύγκριση με το μέγεθος του αλφάβητου $\mathbb{F}_q$ εφόσον $n = q-1$.

Παραδείγματα 4.4. Έστω ένας Reed Solomon κώδικας πάνω από το $\mathbb{F}_9$ με $k = 3$. Χρησιμοποιώντας την βάση $\{1, t, t^2\}$ για τον $\mathcal{L}_3$ έχουμε τον πίνακα γεννήτρια

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & a & a^2 & a^3 & a^4 & a^5 & a^6 & a^7 \\ 1 & a^2 & a^4 & a^6 & 1 & a^2 & a^4 & a^6 \end{pmatrix}.$$

όπου η πρώτη γραμμή δίνει τις τιμές του $f(t) = 1$, η δεύτερη γραμμή δίνει τις τιμές του $f(t) = t$ και η τρίτη δίνει τις τιμές του $f(t) = t^2$ στα μη μηδενικά στοιχεία του $\mathbb{F}_9$ ($a^8 = 1$ στο $\mathbb{F}_9$).

Σχόλια 4.4. Γενικά οι πίνακες γεννήτριες για τους Reed Solomon κώδικες σχηματίζονται παίρνοντας μια βάση του $\mathcal{L}_{k-1}$ και εκτιμώντας την μορφή των αντίστοιχων κωδικών λέξεων.

Για όλα τα $k < q$, οι πρώτες $k-$στήλες του πίνακα γεννήτρια που αντιστοιχούν στην βάση μονωνύμων του $\mathcal{L}_{k-1}$ δίνουν υποπίνακα με μη μηδενική ορίζουσα. Η απεικόνιση εκτίμησης είναι "1-1"και ο αντίστοιχος Reed Solomon κώδικας είναι ένας γραμμικός κώδικας με μήκος $n = q - 1$ και διάσταση $k = \dim \mathcal{L}_{k-1}$.

Οι συμβολισμοί που θα χρησιμοποιήσουμε στο κεφάλαιο αυτό είναι:

- $F/\mathbb{F}_q$ είναι ένα αλγεβρικό σώμα συναρτήσεων γένους g.
- $P_1, \ldots, P_n$ είναι θέσεις του $F/\mathbb{F}_q$ διαφορετικές μεταξύ τους, βαθμού 1.
- $D = P_1 + \ldots + P_n$.
- G είναι ένας διαιρέτης του $F/\mathbb{F}_q$ έτσι ώστε $suppG \cap suppD = \emptyset$.

Ορισμός 4.10. Ο *γεωμετρικός Goppa κώδικας* $C_{\mathcal{L}}(D, G)$ που συνδέεται με τους διαιρέτες του D και G ορίζεται ως εξής:

$$C_{\mathcal{L}}(D, G) := \Big\{ \big(x(P_1), \ldots, x(P_n)\big) \ / \ x \in \mathcal{L}(G) \Big\} \subseteq \mathbb{F}_q^n.$$

Παρατηρήσεις 4.3.

- Για $x \in \mathcal{L}(G)$ έχουμε $v_{P_i}(x) \geq 0$ $(i = 1, \ldots, n)$ γιατί $suppG \cap suppD = \emptyset$. Η κλάση υπολοίπων $x(P_i)$ του x modulo P_i είναι ένα στοιχείο του σώματος κλάσης υπολοίπων του P_i. Εφόσον $\deg P_i = 1$, το σώμα κλάσης υπολοίπων είναι το $\mathbb{F}_q$, έτσι $x(P_i) \in \mathbb{F}_q$.
- Μπορούμε να θεωρήσουμε την απεικόνιση εκτίμησης $ev_D : \mathcal{L}(G) \to \mathbb{F}_q^n$ με

$$ev_D(x) := \big(x(P_1), \ldots, x(P_n)\big) \in \mathbb{F}_q^n \tag{4.6}$$

  Η ev_D είναι $\mathbb{F}_q-$γραμμική και $C_{\mathcal{L}}(D, G)$ είναι η εικόνα του $\mathcal{L}(G)$ μέσω αυτής της απεικόνισης.

Οι Reed Solomon κώδικες είναι ειδική περίπτωση των γεωμετρικών κωδίκων Goppa γιατί τα $x(P_i)$ στον γεωμετρικό κώδικα Goppa $C_{\mathcal{L}}(D, G)$ ανήκουν στο $\mathbb{F}_q$ ενώ τα f του Reed Solomon κώδικα C_k ανήκουν στον $\mathbb{F}_q[x]$ και $\deg f \leq k - 1$. Η κατασκευή τώρα ενός γεωμετρικού κώδικα Goppa απαιτεί το σώμα συναρτήσεων $F/\mathbb{F}_q$ να επιλεγεί ώστε να έχει γένος g και οι θέσεις του $P_1, \ldots, P_n$ να είναι διαφορετικές και βαθμού 1. Όσο για τους διαιρέτες D και G πρέπει $D = P_1 + \ldots + P_n$ και $suppG \cap suppD = \emptyset$.

Οι κώδικες αυτοί παρουσιάζουν ενδιαφέρον γιατί μπορεί κανείς να υπολογίσει τις παραμέτρους n, k, d με το Θεώρημα Riemann-Roch και να πετύχει ένα χαμηλό φράγμα για την ελάχιστη απόστασή τους.

Θεώρημα 4.1. $C_{\mathcal{L}}(D,G)$ είναι ένας $[n,k,d]$ κώδικας με παραμέτρους $k=\dim G-\dim(G-D)$ και $d\geq n-\deg G$.

Απόδειξη:

Ο $C_{\mathcal{L}}(D,G)$ είναι κώδικας πάνω από το $\mathbb{F}_q$ εφόσον τα P_i είναι ρητά και το x έχει τους συντελεστές του στο $\mathbb{F}_q$.

Η απεικόνιση εκτίμησης ev_D είναι 1-1 και επί γραμμική απεικόνιση από το $\mathcal{L}(G)$ στο $C_{\mathcal{L}}(D,G)$ με πυρήνα

$$Ker(ev_D)=\big\{x\in\mathcal{L}(G)\ /\ v_{P_i}(x)>0\ \text{ για }\ i=1,\ldots,n\big\}=\mathcal{L}(D-G).$$

οπότε

$$\dim C_{\mathcal{L}}(D,G)=\dim\mathcal{L}(G)-\dim\mathcal{L}(G-D)$$

άρα

$$k=\dim G-\dim(G-D).$$

Για να αποδείξουμε την δεύτερη σχέση υποθέτουμε ότι $C_{\mathcal{L}}(D,G)\neq 0$. Έστω λοιπόν $x\in\mathcal{L}(G)$ με $w(ev_D(x))=d$.

Τότε $n-d$ θέσεις $P_{i_1},\ldots,P_{i_{n-d}}$ στο φορέα του D είναι οι ρίζες του x, άρα

$$0\neq x\in\mathcal{L}\big(G-(P_{i_1}+\ldots+P_{i_{n-d}})\big).$$

Άρα από το Πόρισμα (1.6) συμπεραίνουμε ότι

$$0\leq\deg\big(G-(P_{i_1}+\ldots+P_{i_{n-d}})\big)=\deg G-n+d$$

άρα

$$d\geq n-\deg G.\qquad\blacksquare$$

Πόρισμα 4.1. Έστω ότι ο βαθμός του G είναι αυστηρά μικρότερος του n. Τότε η απεικόνιση εκτίμησης $ev_D:\mathcal{L}(G)\to C_{\mathcal{L}}(D,G)$ είναι 1-1 και έχουμε:

α) $C_{\mathcal{L}}(D,G)$ είναι ένας $[n,k,d]$ κώδικας με $d\geq n-\deg G$ και $k=\dim G\geq\deg G+1-g$ άρα $k+d\geq n+1-g$.

β) Αν επιπλέον $2g-2<\deg G<n$, τότε $k=\deg G+1-g$.

γ) Αν $\{x_1,\ldots,x_n\}$ είναι βάση του $\mathcal{L}(G)$ τότε ο πίνακας

$$M=\begin{pmatrix}x_1(P_1) & x_1(P_2) & \ldots & x_1(P_n)\\ \vdots & \vdots & \vdots & \vdots\\ x_k(P_1) & x_k(P_2) & \ldots & x_k(P_n)\end{pmatrix}.$$

είναι ένας πίνακας γεννήτρια για τον $C_{\mathcal{L}}(D,G)$.

Απόδειξη:

Έχουμε ότι $\deg(G-D)=\deg G-\deg D=\deg G-n<0$ άρα $\mathcal{L}(G-D)=0$ και ο $\mathcal{L}(G-D)=0$ είναι ο πυρήνας της ev_D και η ev_D είναι 1-1 απεικόνιση.

α) Ο $C_{\mathcal{L}}(D,G)$ σύμφωνα με το Θεώρημα 4.1 είναι επίσης ένας $[n,k,d]$ κώδικας με $d \geq n - \deg G$ και

$$\begin{aligned} k &= \dim G - \dim(G-D) \\ &= \dim G - 0 \\ &= \dim G \\ &\geq \deg G + 1 - g \end{aligned}$$

από το Θεώρημα Riemann.

Τώρα προσθέτω κατα μέλη τις

$$d \geq n - \deg G$$

και

$$k \geq \deg G + 1 - g$$

άρα

$$k + d \geq n + 1 - g.$$

β) Ξέρουμε ότι για κάθε διαιρέτη A του F/K με βαθμό $\geq 2g-1$ ισχύει

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

άρα αν $\deg G \geq 2g-1$ τότε

$$k = \dim G = \deg G + 1 - g.$$

γ) Οι γραμμές του M αποτελούν βάση για τον $C_{\mathcal{L}}(D,G)$ άρα ο M είναι ένας πίνακας γεννήτρια για τον $C_{\mathcal{L}}(D,G)$.

Παρατηρήσεις 4.4. Ισχύουν

$$k + d \geq n + 1 - g \quad \text{(Πόρισμα 4.1)}$$

και

$$k + d \leq n + 1 \quad \text{(Singleton Bound)}$$

για $\deg G < n$, άρα

$$n + 1 - g \leq k + d \leq n + 1. \tag{4.7}$$

Επομένως

$$k + d = n + 1$$

όταν $g = 0$, δηλαδή αν F είναι σώμα συναρτήσεων γένους μηδέν.

Άρα οι γεωμετρικοί Goppa κώδικες είναι κώδικες MDS όταν κατασκευάζονται στο ρητό σώμα συναρτήσεων $\mathbb{F}_q(z)$.

Ορισμός 4.11. Ο ακέραιος $d^* := n - \deg G$ ονομάζεται *designed απόσταση* του κώδικα $C_{\mathcal{L}}(D,G)$.

Σχόλια 4.5. Η ελάχιστη απόσταση ενός γεωμετρικού κώδικα Goppa δεν μπορεί να είναι μικρότερη από την designed απόστασή του. Αυτό προκύπτει από το Θεώρημα 4.1, δηλαδή ισχύει $d^* \leq d$. Πότε ισχύει το ίσον;

Αν $\dim G > 0$ και $d^* = n - \deg G > 0$ τότε $d^* = d$ αν και μόνο αν υπάρχει ένας διαιρέτης D' με $0 \leq D' \leq D$, $\deg D' = \deg G$ και $\dim(G - D') > 0$.

Απόδειξη:

Ευθύ: Υποθέτουμε ότι $d^* = d$.

Τότε υπάρχει ένα στοιχείο $0 \neq x \in \mathcal{L}(G)$ έτσι ώστε η κωδική λέξη $\big(x(P_1), \ldots, x(P_n)\big) \in C_{\mathcal{L}}(D, G)$ να έχει ακριβώς $n - d = n - d^* = \deg G$ μηδενικες συνιστώσες τις $x(P_{i_j}) = 0$ για $j = 1, \ldots, \deg G$.

Θέτω

$$D' := \sum_{j=1}^{\deg G} P_{i_j}$$

τότε

$$0 \leq D' \leq D, \;\; \deg D' = \deg G$$

και

$$\dim(G - D') > 0$$

γιατί $x \in \mathcal{L}(G - D')$.

Αντίστροφο: Αν D' διαιρέτης με $0 \leq D' \leq D, \deg D' = \deg G$ και $\dim(G - D') > 0$ τότε διαλέγουμε ένα στοιχείο $0 \neq y \in \mathcal{L}(G - D')$.

Τότε το βάρος της αντίστοιχης κωδικής λέξης $\big(y(P_1), \ldots, y(P_n)\big)$ είναι $n - \deg G = d^*$ άρα $d = d^*$. ■

Παρατηρήσεις 4.5. Για έναν διαιρέτη $A \in D_F$, $\Omega_F(A)$ είναι ο χώρος των Weil διαφορικών ω με $(\omega) \geq A$. Αυτός είναι ένας πεπερασμένης διάστασης διανυσματικός χώρος πάνω από το $\mathbb{F}_q$ με διάσταση $i(A)$ (the index of speciality του A). Για ένα Weil διαφορικό ω και μια θέση $P \in \mathbb{P}_F$, $\omega_P : F \to \mathbb{F}_q$ εκφράζει την τοπική συνιστώσα του ω στο P. Την οποία χρησιμοποιώντας μπορούμε να βρούμε και έναν άλλο κώδικα ο οποίος συνδέεται με τους διαιρέτες G και D.

Ορισμός 4.12. Έστω G και $D = P_1 + \ldots + P_n$ διαιρέτες με $suppG \cap suppD = \emptyset$ και P_i διαφορρετικές μεταξύ τους θέσεις βαθμού 1. Τότε ορίζουμε τον κώδικα:

$$C_\Omega(D, G) := \Big\{ \big(\omega_{P_1}(1), \ldots, \omega_{P_n}(1)\big) \;/\; \omega \in \Omega_F(G - D) \Big\}.$$

Θεώρημα 4.2. (Ανάλογο του Θεωρήματος 4.1)
Ο $C_\Omega(D, G)$ είναι ένας $[n, k', d']$ κώδικας με παραμέτρους

$$k' = i(G - D) - i(G) \;\; \text{και} \;\; d' \geq \deg G - (2g - 2).$$

Αν επιπλέον ισχύει $\deg G > 2g - 2$ έχουμε ότι:

$$k' = i(G - D) \geq n + g - 1 - \deg G.$$

Επίσης αν $2g - 2 < \deg G < n$ τότε:

$$k' = n + g - 1 - \deg G.$$

Απόδειξη:

Έστω $P \in \mathbb{P}_F$ μια θέση βαθμού 1 και ω ένα Weil διαφορικό με $v_P(\omega) \geq -1$. Ισχυριζόμαστε ότι:

$$\omega_P(1) = 0 \Leftrightarrow v_P(\omega) \geq 0. \tag{4.8}$$

($\Leftarrow$) Ισχύει ότι για έναν ακέραιο $r \in \mathbb{Z}$

$$v_P(\omega) \geq r \Leftrightarrow \omega_P(x) = 0 \ \text{ για όλα τα } \ x \in F \ \text{ με } \ v_P(x) \geq -r \qquad (4.9)$$

οπότε για $r = 0$ προκύπτει ότι αν $v_P(\omega) \geq 0$ τότε $\omega_P(1) = 0$.

($\Rightarrow$) Υποθέτω ότι $\omega_P(1) = 0$.

Έστω $x \in F$ με $v_P(x) \geq 0$. Εφόσον $\deg P = 1$ μπορούμε να γράψουμε $x = a + y$ με $a \in \mathbb{F}_q$ και $v_P(y) \geq 1$.

Τότε

$$\omega_P(x) = \omega_P(a) + \omega_P(y) = a \cdot \omega_P(1) + 0 = 0$$

($\omega_P(y) = 0$ γιατί $v_P(\omega) \geq -1$ και $v_P(y) \geq 1$). Έτσι έχουμε αποδείξει την (4.8).

Τώρα θεωρούμε την $\mathbb{F}_q-$γραμμική απεικόνιση

$$\varrho_D : \begin{cases} \Omega_F(G-D) \to C_\Omega(D,G) \\ \\ \omega \mapsto \big(\omega_{P_1}(1), \ldots, \omega_{P_1}(1)\big) \end{cases}$$

η ϱ_D είναι 1-1 και επί και ο πυρήνας της είναι ο $\Omega_F(G)$ (από την 4.8).

Επομένως

$$k' = \dim \Omega_F(G-D) - \dim \Omega_F(G) = i(G-D) - i(G). \qquad (4.10)$$

Έστω $\varrho_D(\omega) \in C_\Omega(D,G)$ κωδική λέξη με βάρος $m > 0$. Τότε $\omega_{P_i}(1) = 0$ για κάποιους δείκτες $i = i_1, \ldots, \imath_{n-m}$, έτσι

$$\omega \in \Omega_F\Big(G - \big(D - \sum_{j=1}^{n-m} P_{i_j}\big)\Big)$$

(από την 4.8). Εφόσον $\Omega_F(A) \neq 0$ συνεπάγεται

$$\deg A \leq 2g - 2$$

(από το Θεώρημα 3.4), οπότε έχουμε:

$$2g - 2 \geq \deg G - (n - (n-m)) = \deg G - m.$$

Επομένως η ελάχιστη απόσταση d' του $C_\Omega(D,G)$ ικανοποιεί την ανισότητα

$$d' \geq \deg G - (2g-2).$$

Υποθέτω τώρα ότι $\deg G > 2g-2$. Από το Θεώρημα 3.4 έχουμε $i(G) = 0$. Οπότε η 4.10 με το Θεώρημα Riemann-Roch δίνουν

$$\begin{aligned} k' &= i(G-D) - 0 \\ &= \dim(G-D) - \deg(G-D) + g - 1 \\ &= \dim(G-D) + n + g - 1 - \deg G. \end{aligned}$$

Άρα

$$k' \geq n + g - 1 - \deg G.$$

Αν επιπλέον $\deg G < n$ τότε $\dim(G-D) = 0$ οπότε $k' = n + g - 1 - \deg G$. ■

Ορισμός 4.13. Ο αριθμός $\deg G - (2g-2)$ λέγεται designed απόσταση του $C_\Omega(D,G)$.

Θεώρημα 4.3. Οι κώδικες $C_\mathcal{L}(D,G)$ και $C_\Omega(D,G)$ είναι ο ένας δυϊκός του άλλου, δηλαδή

$$C_\Omega(D,G) = C_\mathcal{L}(D,G)^\perp.$$

Απόδειξη:

Ισχυρισμός

Έστω $P \in \mathbb{P}_F$ θέση βαθμού 1, ω ένα Weil διαφορικό με $v_P(\omega) \geq -1$ και ένα στοιχείο $x \in F$ με $v_P(x) \geq 0$, τότε

$$\omega_P(x) = x(P) \cdot \omega_P(1). \tag{4.11}$$

Απόδειξη Ισχυρισμού

Γράφουμε $x = a + y$ με $a = x(P) \in \mathbb{F}_q$ και $v_P(y) > 0$, τότε

$$\begin{aligned} \omega_P(x) &= \omega_P(a) + \omega_P(y) \\ &= a \cdot \omega_P(1) + 0 \\ &= x(P) \cdot \omega_P(1) \end{aligned}$$

Τώρα θα δείξουμε ότι $C_\Omega(D,G) \subseteq C_\mathcal{L}(D,G)^\perp$.

Έστω λοιπόν $\omega \in \Omega_F(G-D)$ και $x \in \mathcal{L}(G)$, τότε

$$\begin{aligned} 0 = \omega(x) &= \sum_{P \in \mathbb{P}_F} \omega_P(x) \\ &= \sum_{i=1}^{n} \omega_{P_i}(x) \end{aligned}$$

(γιατί για $P \in \mathbb{P}_F \backslash \{P_1, \ldots, P_n\}$ έχουμε $v_P(x) \geq -v_P(\omega)$ (εφόσον $x \in \mathcal{L}(G)$ και $\omega \in \Omega(G-D)$) έτσι $\omega_P(x) = 0$ από την 4.9)

$$= \sum_{i=1}^{n} x(P_i) \cdot \omega_{P_i}(1)$$

(έπεται από την (4.11))

$$= \Big\langle \big(\omega_{P_1}(1), \ldots, \omega_{P_n}(1)\big), \big(x(P_n), \ldots, x(P_n)\big) \Big\rangle$$

άρα $C_\Omega(D,G) \subseteq C_\mathcal{L}(D,G)^\perp$.

Τώρα θα δείξουμε ότι οι κώδικες $C_\Omega(D,G)$ και $C_\mathcal{L}(D,G)^\perp$ έχουν την ίδια διάσταση

$$\begin{aligned} \dim C_\Omega(D,G) &= i(G-D) - i(G) \text{ (από Θεώρημα4.2)} \\ &= \dim(G-D) - \deg(G-D) - 1 + g - (\dim G - \deg G - 1 + g) \end{aligned}$$

(από Θεώρημα Riemann-Roch και ορισμό του $i(A)$)

$$\begin{aligned} &= \deg D + \dim(G-D) - \dim G \\ &= n - (\dim G - \dim(G-D)) \\ &= n - \dim C_\mathcal{L}(D,G) \\ &= \dim C_\mathcal{L}(D,G)^\perp. \qquad \blacksquare \end{aligned}$$

Λήμμα 4.1. Υπάρχει ένα Weil διαφορικό η έτσι ώστε $v_{P_i}(\eta) = -1$ και $\eta_{P_i}(1) = 1$ για $i = 1, \ldots, n$.

Απόδειξη:

Διαλέγουμε ένα Weil διαφορικό $\omega_0 \neq 0$. Από το Θεώρημα Ασθενούς Προσέγγισης, υπάρχει ένα στοιχείο $z \in F$ με $v_{P_i}(z) = -v_{P_i}(\omega_0) - 1$ για $i = 1, \ldots, n$. Θέτοντας $\omega := z\omega_0$ παίρνουμε $v_{P_i}(\omega) = -1$. Επομένως $a_i := \omega_{P_i}(1) \neq 0$ (από την 4.8). Ξανά από το Θεώρημα Ασθενούς Προσέγγισης βρίσκουμε $y \in F$ έτσι ώστε $v_{P_i}(y - a_i) > 0$. Έπεται ότι

$$v_{P_i}(y) = 0 \quad \text{και} \quad y(P_i) = a_i.$$

Θέτουμε $\eta := y^{-1}\omega$ και έχουμε

$$v_{P_i}(\eta) = v_{P_i}(\omega) = -1$$

και

$$\begin{aligned} \eta_{P_i}(1) &= \omega_{P_i}(y^{-1}) \\ &= y^{-1}(P_i) \cdot \omega_{P_i}(1) \\ &= a_i^{-1} \cdot a_i \\ &= 1 \end{aligned}$$ ■

Πρόταση 4.2. Έστω η ένα Weil διαφορικό έτσι ώστε $v_{P_i}(\eta) = -1$ και $\eta_{P_i}(1) = 1$ για $i = 1, \ldots, n$. Τότε

$$C_{\mathcal{L}}(D, G)^{\perp} = C_{\Omega}(D, G) = C_{\mathcal{L}}(D, H) \text{ με } H := D - G + (\eta).$$

Απόδειξη:

Παρατηρούμε ότι

$$supp(D - G + (n)) \cap suppD = \emptyset$$

εφόσον $v_{P_i}(\eta) = -1$ για $i = 1, \ldots, n$. Άρα ο $C_{\mathcal{L}}(D, D - G + (\eta))$ ορίζεται.

Από το Θεώρημα 3.2 υπάρχει ένας ισομορφισμός

$$\mu : \mathcal{L}(D - G + (\eta)) \to \Omega_F(G - D)$$

που ορίζεται από $\mu(x) := x\eta$.

Για $x \in \mathcal{L}(D - G + (\eta))$ έχουμε:

$$\begin{aligned} (x\eta)_{Pi}(1) &= \eta_{P_i}(x) \\ &= x(P_i) \cdot \eta_{P_i}(1) \\ &= x(P_i). \end{aligned}$$

Άρα

$$C_{\Omega}(D, G) = C_{\mathcal{L}}(D, D - G + (\eta)).$$ ■

Πόρισμα 4.2. Υποθέτουμε ότι υπάρχει ένα Weil διαφορικό η έτσι ώστε $(\eta) = 2G - D$ και $\eta_{Pi}(1) = 1$ για $i = 1, \ldots, n$. Τότε ο κώδικας $C_{\mathcal{L}}(D, G)$ είναι αυτοδυϊκός.

Απόδειξη:

Έχουμε

$$(\eta) = G + G - D \quad \text{ή} \quad G = D - G + (\eta).$$

Άρα από την Πρόταση 4.2 έπεται ότι:

$$C_{\mathcal{L}}(D,G)^{\perp} = C_{\mathcal{L}}(D, D - G + (\eta)) = C_{\mathcal{L}}(D,G). \quad \blacksquare$$

Σχόλια 4.6. Χρησιμοποιώντας την πρόταση 4.2 μπορούμε να μετατρέψουμε το Θεώρημα 4.2 στο Θεώρημα 4.1. Οπότε έχουμε μια δεύτερη απόδειξη του Θεωρήματος 4.2.

Ορισμός 4.14. Δύο κώδικες $C_1,\ C_2 \subseteq \mathbb{F}_q$ λέγονται *ισοδύναμοι* αν υπάρχει ένα διάνυσμα $a = (a_1, \ldots, a_n) \in \big(\mathbb{F}_q \backslash \{0\}\big)^n$ έτσι ώστε $C_2 = a \cdot C_1$, δηλαδή

$$C_2 = \big\{(a_1 c_1, \ldots, a_n c_n) \ / \ (c_1, \ldots, c_n) \in C_1\big\}.$$

Παρατηρήσεις 4.6. Ισοδύναμοι κώδικες έχουν την ίδια διάσταση, την ίδια ελάχιστη απόσταση και την ίδια κατανομή βάρους. Πάντως αυτή η ισοδυναμία δεν μεταφέρει όλες τις ιδιότητες ενός κώδικα.

Πρόταση 4.3.

α) Έστω G_1 και G_2 διαιρέτες με $G_1 \sim G_2$ και $suppG_1 \cap suppD = suppG_2 \cap suppD = \emptyset$. Τότε οι κώδικες $C_{\mathcal{L}}(D,G_1)$ και $C_{\mathcal{L}}(D,G_2)$ είναι ισοδύναμοι. Το ίδιο ισχύει και για τους $C_{\Omega}(D,G_1)$, $C_{\Omega}(D,G_2)$.

β) Αντιστρόφως, αν ένας κώδικας $C \subseteq \mathbb{F}_q^n$ είναι ισοδύναμος με τον $C_{\mathcal{L}}(D,G)$ (αντίστοιχα με τον $C_{\Omega}(D,G)$) τότε υπάρχει ένας διαιρέτης $G' \sim G$ έτσι ώστε $suppG' \cap suppD = \emptyset$ και $C = C_{\mathcal{L}}(D,G')$ (αντίστοιχα $C = C_{\Omega}(D,G')$).

Απόδειξη:

α) $G_1 \sim G_2$ άρα $G_2 = G_1 - (z)$ με $v_{P_i}(z) = 0$ για $i = 1, \ldots, n$. Άρα

$$a := \big(z(P_1), \ldots, z(P_n)\big) \in \big(\mathbb{F}_q \backslash \{0\}\big)^n$$

και η απεικόνιση

$$x \mapsto xz$$

από το $\mathcal{L}(G_1)$ στο $\mathcal{L}(G_2)$ είναι 1-1 (Λήμμα 1.3). Από αυτό συνεπάγεται ότι:

$$C_{\mathcal{L}}(D,G_2) = a \cdot C_{\mathcal{L}}(D,G_1).$$

Δηλαδή οι κώδικες $C_{\mathcal{L}}(D,G_1)$ και $C_{\mathcal{L}}(D,G_2)$ είναι ισοδύναμοι.

Με τον ίδιο τρόπο αποδεικνύεται ότι και οι κώδικες $C_{\Omega}(D,G_1)$ και $C_{\Omega}(D,G_2)$ είναι ισοδύναμοι.

β) Έστω $C = a \cdot C_{\mathcal{L}}(D,G)$ με $a = (a_1, \ldots, a_n) \in \big(\mathbb{F}_q \backslash \{0\}\big)^n$. Διαλέγουμε $z \in F$ με $z(P_i) = a_i$, $i = 1, \ldots, n$ και θέτουμε $G' := G - (z)$. Τότε

$$C = C_{\mathcal{L}}(D,G'). \qquad \blacksquare$$

Σχόλια 4.7. Αν G είναι ένας διαιρέτης για τον οποίο $suppG \cap suppD = \emptyset$, μπορούμε να ορίσουμε έναν γεωμετρικό Goppa κώδικα $C_{\mathcal{L}}(D,G)$ που συνδέεται με τους D και G ως εξής: διαλέγουμε έναν διαιρέτη $G' \sim G$ με $suppG' \cap suppD = \emptyset$ (αυτό είναι δυνατόν από το Θεώρημα Προσέγγισης) και θέτουμε $C_{\mathcal{L}}(D,G) := C_{\mathcal{L}}(D,G')$. Η επιλογή του G' δεν είναι κανονική, άρα ο $C_{\mathcal{L}}(D,G)$ είναι καλά ορισμένος από την ισοδυναμία της Πρότασης 4.3.

4.3 Γεωμετρικοί κώδικες Goppa ενός ρητού σώματος συναρτήσεων

Σ' αυτή την παράγραφο θα μελετήσουμε γεωμετρικούς κώδικες Goppa που συνδέονται με διαιρέτες ενός ρητού σώματος συναρτήσεων. Στην κωδικοποίηση αυτή η κατηγορία κωδίκων είναι γνωστή ως Generalized Reed Solomon κώδικες.

Ορισμός 4.15. Ένας γεωμετρικός κώδικας Goppa $C_{\mathcal{L}}(D,G)$ που συνδέεται με τους διαιρέτες G και D ενός ρητού σώματος συναρτήσεων $\mathbb{F}_q(z)/\mathbb{F}_q$ λέγεται ρητός. (Όπως και στην παράγραφο 4.2, $D = P_1 + \ldots + P_n$ με $P_1, \ldots, Pn$ διαφορετικές μεταξύ τους θέσεις, βαθμού 1 και $suppG \cap suppD = \emptyset$).

Παρατηρήσεις 4.7. Το μήκος του $C_{\mathcal{L}}(D,G)$ φράσσεται από το $q+1$ γιατί το $\mathbb{F}_q(z)$ έχει μόνο $q+1$ θέσεις βαθμού 1. Αυτές είναι ο πόλος P_∞ του z και για κάθε $\alpha \in \mathbb{F}_q$ η ρίζα P_α του $z-\alpha$ (Πρόταση 1.3).

Πρόταση 4.4. Έστω $C = C_{\mathcal{L}}(D,G)$ ένας ρητός γεωμετρικός κώδικας Goppa πάνω από το $\mathbb{F}_q$ και έστω n, k, d οι παράμετροι του C. Τότε έχουμε:

α) $n \leq q+1$.

β) $k = 0 \Leftrightarrow \deg G < 0$ και $k = n \Leftrightarrow \deg G > n-2$.

γ) Για $0 \leq \deg G \leq n-2$

$$k = 1 + \deg G \ \text{ και } \ d = n - \deg G$$

οπότε ο C είναι MDS κώδικας αφού $k + d = n + 1$.

δ) Ο $C^\perp$ είναι επίσης ρητός γεωμετρικός κώδικας Goppa.

Πρόταση 4.5. Έστω $C = C_{\mathcal{L}}(D,G)$ είναι ένας ρητός γεωμετρικός κώδικας Goppa πάνω από το $\mathbb{F}_q$ με παραμέτρους n, k και d.

α) Αν $n \leq q$ υπάρχουν στοιχεία $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ ανα δύο διαφορετικά μεταξύ τους και $v_1, \ldots, v_n \in \mathbb{F}_q \backslash \{0\}$ (όχι απαραίτητα διαφορετικά) έτσι ώστε

$$C = \Big\{ \big(v_1 \cdot f(\alpha_1), v_2 \cdot f(\alpha_2), \ldots, v_n \cdot f(\alpha_n)\big) \ / \ f \in \mathbb{F}_q[z] \ \text{ και } \ \deg f \leq k-1 \Big\}.$$

Ο πίνακας

$$M = \begin{pmatrix} v_1 & v_2 & \ldots & v_n \\ \alpha_1 v_1 & \alpha_2 v_2 & \ldots & \alpha_n v_n \\ \alpha_1^2 v_1 & \alpha_2^2 v_2 & \ldots & \alpha_n^2 v_n \\ \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{k-1} v_1 & \alpha_2^{k-1} v_2 & \ldots & \alpha_n^{k-1} v_n \end{pmatrix} \tag{4.12}$$

είναι ένας πίνακας γεννήτρια για τον C.

β) Αν $n = q+1$, ο C έχει πίνακα γεννήτρια τον

$$M = \begin{pmatrix} v_1 & v_2 & \ldots & v_{n-1} & 0 \\ \alpha_1 v_1 & \alpha_2 v_2 & \ldots & \alpha_{n-1} v_{n-1} & 0 \\ \alpha_1^2 v_1 & \alpha_2^2 v_2 & \ldots & \alpha_{n-1}^2 v_{n-1} & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha_1^{k-1} v_1 & \alpha_2^{k-1} v_2 & \ldots & \alpha_{n-1}^{k-1} v_{n-1} & 1 \end{pmatrix} \tag{4.13}$$

όπου $\mathbb{F}_q = \{\alpha_1, \ldots, \alpha_{n-1}\}$ και $v_1, \ldots, v_{n-1} \in \mathbb{F}_q \backslash \{0\}$.

Απόδειξη:

α) Έστω $D = P_1 + \ldots + P_n$. Εφόσον $n \leq q$ υπάρχει μια θέση P βαθμού 1 η οποία δεν είναι στον φορέα του D. Διαλέγουμε μια θέση $Q \neq P$ βαθμού 1 (π.χ. $Q = P_1$). Τότε $\dim(Q - P) = 1$ (από Θεώρημα Riemann-Roch) άρα $Q - P$ είναι κύριος διαιρέτης (Πόρισμα 1.6). Έστω $Q - P = (z)$, τότε το z είναι το παραγόμενο στοιχείο του ρητού σώματος συναρτήσεων πάνω από το $\mathbb{F}_q$ και P είναι ο πόλος διαιρέτης του z, δηλαδή $P = P_\infty$.

Από την προηγούμενη πρόταση (4.4) μπορούμε να υποθέσουμε ότι $\deg G = k - 1 \geq 0$ (η περίπτωση $k = 0$ είναι τετριμμένη). Ο διαιρέτης $(k-1)P_\infty - G$ έχει βαθμό μηδέν άρα είναι κυρτός (από Θεώρημα Riemann-Roch και Πόρισμα 1.6). Έστω $(k-1)P_\infty - G = (u)$ με $0 \neq u \in F$. Τα k στοιχεία $u, z \cdot u, \ldots, z^{k-1} \cdot u$ είναι στον $\mathcal{L}(G)$ και είναι γραμμικώς ανεξάρτητα πάνω από το $\mathbb{F}_q$. Εφόσον $\dim G = k$ αποτελούν μια βάση του $\mathcal{L}(G)$, δηλαδή

$$\mathcal{L}(G) = \{u \cdot f(z) \ / \ f \in \mathbb{F}_q[z] \ \text{ και } \ \deg f \leq k-1\}.$$

Θέτοντας $\alpha_i := z(P_i)$ και $v_i := u(P_i)$ έχουμε

$$\big(u \cdot f(z)\big)(P_i) = u(P_i) \cdot f\big(z(P_i)\big) = v_i \cdot f(\alpha_i) \ \text{ για } \ i = 1, \ldots, n.$$

Επομένως

$$C = C_{\mathcal{L}}(D, G) = \big\{\big(v_1 \cdot f(\alpha_1), \ldots, v_n \cdot f(\alpha_n)\big) \ / \ \deg \leq k-1\big\}.$$

Η κωδική λέξη του C που αντιστοιχεί στο $u \cdot z^j$ είναι $(v_1 \cdot \alpha_1^j, v_2 \cdot \alpha_2^j, \ldots, v_n \cdot \alpha_n^j)$ οπότε ο πίνακας (4.12) είναι πίνακας γεννήτρια του C.

β) Η απόδειξη είναι παρόμοια με την περίπτωση $n \leq q$. Τώρα έχουμε $n = q+1$ και μπορούμε να διαλέξουμε z έτσι ώστε $P_n = P_\infty$ ο πόλος του z. Όπως και πριν $(k-1)P_\infty - G = (u)$ με $0 \neq u \in F$ και $\{u, z \cdot u, \ldots, z^{k-1} \cdot u\}$ είναι μια βάση του $\mathcal{L}(G)$. Για $1 \leq i \leq n-1 = q$, τα στοιχεία $\alpha_i := z(P_i) \in \mathbb{F}_q$ είναι διαφορετικά μεταξύ τους άρα $\mathbb{F}_q = \{\alpha_1, \ldots, \alpha_{n-1}\}$. Επιπλέον $v_i := u(P_i) \in \mathbb{F}_q \backslash \{0\}$ για $i = 1, \ldots, n-1$. Για $0 \leq j \leq k-2$ έχουμε:

$$\big((u \cdot z^j)(P_1), \ldots, (u \cdot z^j)(P_n)\big) = (\alpha_1^j \cdot v_1, \ldots, \alpha_{n-1}^j \cdot v_{n-1}, 0),$$

αλλά για $j = k-1$ ισχύει:

$$\big((u \cdot z^{k-1})(P_1), \ldots, (u \cdot z^{k-1})(P_n)\big) = (\alpha_1^{k-1} \cdot v_1, \ldots, \alpha_{n-1}^{k-1} \cdot v_{n-1}, \gamma)$$

όπου $0 \neq \gamma \in \mathbb{F}_q$. Αντικαθιστώντας το u με $\gamma^{-1}u$ προκύπτει ο πίνακας γεννήτρια (4.13). ■

Ορισμός 4.16. Έστω $\alpha = (\alpha_1, \ldots, \alpha_n)$ όπου τα α_i είναι διαφορετικά στοιχεία του $\mathbb{F}_q$ και έστω $v = (v_1, \ldots, v_n)$ όπου τα v_i είναι μη μηδενικά στοιχεία (όχι απαραίτητα διαφορετικά) στοιχεία του $\mathbb{F}_q$. Τότε ο Generalized Reed Solomon κώδικας συμβολίζεται με $\mathrm{GRS}_k(\alpha, v)$ και αποτελείται από όλα τα διανύσματα $\big(v_1 \cdot f(\alpha_1), \ldots, v_n \cdot f(\alpha_n)\big)$ με $f(z) \in \mathbb{F}_q[z]$ και $\deg f \leq k-1$ (για σταθερό $k \leq n$).

Παρατηρήσεις 4.8.

(i) Ένας ορισμός ισοδύναμος με τον ορισμό 4.16 είναι ο εξής: $\mathrm{GRS}_k(\alpha, v)$ είναι ο κώδικας πάνω από το $\mathbb{F}_q$ με πίνακα γεννήτρια τον 4.12.

(ii) Αν $\alpha = (\beta, \beta^2, \ldots, \beta^n)$ (όπου $n = q-1$ και β είναι πρωτεύον νιοστή ρίζα της μονάδας) και $v = (1, 1, \ldots, 1)$ τότε ο $\mathrm{GRS}_k(\alpha, v)$ είναι ένας Reed Solomon κώδικας.

Βιβλιογραφία

[1] Algebraic Function Fields and Codes, *Henning Stichtenoth* Springer Verlag Undergraduate Texts in Mathematics, 1993.

[2] Ideals Varieties and Algorithms, *David Cox, John Little, Donal O' Shea* Springer-Verlag, Undergraduate Texts in Mathematics, 1992

[3] Arithmetic of Elliptic Curves, *J.H. Silvermann* Springer-Verlag, 1986

[4] Algebraic Numbers and Algebraic Functions *P.M. Cohn* Chapman and Hall, 1991

[5] Handbook of Algebra M.Hazewinkel (editor), Volume I, North - Holland, 1996

[6] Algebra *Michael Artin* Prentice - Hall Inc., 1991

[7] Algebraic Geometry I, encyclopedia of Mathematical Sciences Volume 29 *I.R Shafarevitch* (ed.), 1991

[8] Error Correcting Codes, a mathematical introduction, *John Baylis* Chapman and Hall, 1998

[9] Using Algebraic Geometry, *cox, Little, O'Shea* Springer, 1998

[10] A First Course in Coding Theory *Raymond Hill* Clarendon Press - Oxford, 1986