Σταυρούλα Χατζηδάβαρη

Εισαγωγή στα Drinfeld Modules

Μεταπτυχιακή Εργασία

Πανεπιστήμιο Αθηνών, Τμήμα Μαθηματικών

Αθήνα 22 Σεπτεμβρίου 2018

Εισηγητής: Αριστείδης Κοντογεώργης

Επιτροπή

Αριστείδης Κοντογεώργης

Μιχάλης Μαλιάκας

Ιωάννης Εμμανουήλ

Στους γονείς μου

Περιεχόμενα

Εισαγωγή

Η στοιχειώδης θεωρία Αριθμών ασχολείται με τις αριθμητικές ιδιότητες του δακτυλίου των ακεραίων $\mathbb{Z}$ και του σώματος των ρητών $\mathbb{Q}$. Είναι σαφές ότι ο δακτύλιος $\mathbb{Z}$ έχει πολλές κοινές ιδιότητες με τον δακτύλιο $\mathbf{A} = k[x]$ των πολυωνύμων πάνω από ένα σώμα k, ιδιαίτερα αν το σώμα k είναι ένα πεπερασμένο σώμα. και οι δύο δακτύλιοι είναι περιοχές κυρίων ιδεωδών, τα σώματα που προκύπτουν αν θεωρήσουμε το πηλίκο με ένα πρώτο-μέγιστο ιδεώδες είναι πεπερασμένα, και οι δύο δακτύλιοι έχουν άπειρους πρώτους και πεπερασμένες μονάδες. Είναι φυσιολογικό να περιμένουμε ότι πολλά από τα αποτελέσματα τα οποία μπορούμε να αποδείξουμε για το $\mathbb{Z}$ έχουν ανάλογα για τον δακτύλιο $\mathbf{A}$. Η αλγεβρική θεωρία αριθμών ασχολείται με τις αλγεβρικές επεκτάσεις του σώματος των ρητών αριθμών και μελετά τις ιδιότητες του δακτυλίου των ακεραίων (που ορίζεται ως η ακέραια κλειστότητα του $\mathbb{Z}$ στο σώμα αριθμών) των σωμάτων αριθμών, τα πρώτα ιδεώδη και τις σχέσεις μεταξύ τους. Παρόμοια μπορούμε να θεωρήσουμε αλγεβρικές επεκτάσεις του σώματος $k = \mathbb{F}_q(T)$, το οποίο παίζει τον ρόλο των ρητών αριθμών και να ορίσουμε τα αλγεβρικά σώματα συναρτήσεων. Αυτά όχι μόνο αναλογούν στα αλγεβρικά σώματα αριθμών αλλά μπορούν να θεωρηθούν και ως συναρτήσεις πάνω σε αλγεβρικές καμπύλες ορισμένες πάνω από πεπερασμένα σώματα. Οι ομοιότητες αυτές ήταν εδώ και πολύ καιρό γνωστές, για παράδειγμα το κλασικό βιβλίο του H. Hasse [5] πραγματεύεται και τις δύο θεωρίας με ενιαίο τρόπο. Από την άλλη η θέαση ως καμπύλες επιτρέπει την χρήση γεωμετρικών εργαλείων τόσο στα σώματα όσο και στα σώματα αριθμών, την λεγόμενη φιλοσοφία της «Αριθμητικής Γεωμετρίας». Για μια μοντέρνα προσέγγιση, γεωμετρική και αναλυτική ο ενδιαφερόμενος αναγνώστης μπορεί να συμβουλευτεί το [9] όπως και το άρθρο επισκόπησης [16].

Στην εργασία αυτή θα μελετήσουμε την τεχνική των Drinfeld modules σε σχέση με την θεωρία κλάσεων σωμάτων. Στην αλγεβρική θεωρία αριθμών, το Θεώρημα των Kronecker-Weber αναφέρει ότι οι αβελιανές επεκτάσεις του $\mathbb{Q}$ παράγονται από τιμές της εκθετικής συνάρτησης $\exp : \tau \to e^{2\pi i\tau}$ για $\tau \in \mathbb{Q}$. Στο τρίτο κεφάλαιο θα ορίσουμε μια αναλυτική εκθετική συνάρτηση η οποία θα παίξει τον ρόλο της εκθετικής συνάρτησης για τα αλγεβρικά σώματα συναρτήσεων.

Αν θεωρήσουμε ως $\mathbb{Q}^{\text{ab}}/\mathbb{Q}$ την μέγιστη αβελιανή επέκταση του $\mathbb{Q}$, τότε το Θεώρημα των Kronecker-Weber έχει ως συνέπεια ότι $\text{Gal}(\mathbb{Q}^{\text{ab}}/\mathbb{Q}) = \widehat{\mathbb{Z}}^*$. Η μελέτη των αβελιανών επεκτάσεων ενός δεδομένου σώματος K είναι το αντικείμενο της *θεωρίας κλάσεων σωμάτων*. Γενικά K είναι ένα σώμα αριθμών, ή ένα σώμα συναρτήσεων μίας μεταβλητής (καθολικά σώματα) ή ένα τοπικό σώμα. Η θεωρία κλάσεων σωμάτων έχει πολλές διαφορετικές διατυπώσεις σε πολλές διαφορετικές γλώσσες. Γενικά, τα βασικά θεωρήματα αυτής δίνουν μία αντί-ισοδυναμία $\psi : \mathbf{Ab}_K \to \mathbf{Sub}_X$ ανάμεσα στην κατηγορία των αβελιανών επεκτάσεων του K και την κατηγορία $\mathbf{Sub}_X$ των ανοιχτών υποομάδων μιας τοπικά συμπαγούς αβελιανής ομάδας $X = X(K)$, η οποία ορίζεται

αποκλειστικά σε όρους του σώματος K. Η ομάδα $X(K)$ στην περίπτωση των καθολικών σωμάτων είναι η idèle class group ή η πολλαπλασιαστική ομάδα K^* στην περίπτωση που το K είναι τοπικό σώμα. Ο ορισμός της αντί-ισοδυναμίας απεικονίζει μια αλγεβρική επέκταση L/K στην εικόνα της $N_{L/K}X(L) \subset X(K)$. Το θεώρημα ύπαρξης εξασφαλίζει ότι κάθε ανοιχτή υποομάδα $H \subset X(K)$ είναι της μορφής $N_{L/K}X(L)$ για κάποια L/K αβελιανή επέκταση, το λεγόμενο σώμα κλάσεων της H. Το πρόβλημα της ακριβούς περιγραφής του $L = \psi^{-1}(H)$ αποτελεί το λεγόμενο *12ο πρόβλημα του Hilbert*. Το πρόβλημα αυτό παραμένει ανοιχτό, ενώ είναι γνωστές μερικές ειδικές περιπτώσεις, όπως όταν το $K = \mathbb{Q}$ (η ακριβής περιγραφή εδώ δίνεται μέσω του θεωρήματος Kronecker-Weber), η περίπτωση των μιγαδικών τετραγωνικών σωμάτων αριθμών αλλά και μερικές περιπτώσεις από σώματα συναρτήσεων όπου η ακριβής περιγραφή δίνεται με την βοήθεια των τάξεως-1 προτύπων Drinfeld.

Για να φτάσουμε να ορίσουμε τα Drinfeld modules θα εισαγάγουμε πρώτα τα προσθετικά πολυώνυμα στο 1ο κεφάλαιο και μερικές βασικές ιδιότητες από την μη αρχιμήδεια ανάλυση στο 2ο κεφάλιο. Η μη-αρχιμήδεια ανάλυση είχε την αφετηρία στην προσπάθεια να ορίσουμε το ανάλογο των σωμάτων μερομόρφων συναρτήσεων από την θεωρία των συμπαγών επιφανειών Riemann - θεωρία ισοδύναμη με την θεωρία των προβολικών αλγεβρικών καμπυλών πάνω από το σώμα των μιγαδικών αριθμών - στα σώματα αριθμών. Η θεωρία αυτή ξεκίνησε από τον Kurt Hensel και έδειξε την δυναμική της μετά την απόδειξη του local-global principle από τον μαθητή του Hensel, H. Hasse. Στο 3ο κεφάλαιο εισαγάγουμε το Carlitz module με βάση την ομώνυμη εκθετική συνάρτηση. Η μελέτη αυτή από τον Carlitz ξεκίνησε το 1932 από τον L. Carlitz [1] αλλά έγινε γνωστή από τον D. Hayes ο οποίος το 1974, [6] περιέγραψε την θεωρία του Carlitz και έδειξε πως μπορεί να οδηγήσει σε μια ακριβή θεωρία κλάσεων σωμάτων, δες τα άρθρα των V. Drinfeld [2] και D. Hayes [7], δίνοντας μια πλήρη λύση για τα 9ο και 12ο προβλήματα του Hilbert στην περίπτωση των σωμάτων συναρτήσεων. Αξίζει να σημειωθεί εδώ ότι δεν υπάρχει μια εξίσου ικανοποιητική θεωρία για σώματα αριθμών παρά μόνο στην περίπτωση που το σώμα είναι το $\mathbb{Q}$ ή ένα μιγαδικό τετραγωνικό σώμα αριθμών, η λεγόμενη θεωρία του μιγαδικού πολλαπλασιασμού, [11].

Η θεωρία των Drinfeld modules ήταν εξαιρετικά γόνιμη αφού επέτρεψε στον V. Drinfeld να αποδείξει τις εικασίες του Langlands για την GL_2 ενός αλγεβρικού σώματος συναρτήσεων σε μερικές περιπτώσεις και οδήγησε και στην απόδειξη των εικασιών για την GL_n από τον L. Lafforgue.

Το τελευταίο κεφάλαιο είναι αφιερωμένο σε μια σειρά από αναλογίες που σκοπό έχουν να συγκρίνουν τα κυκλοτομικά σώματα αριθμών με τα κυκλοτομικά σώματα σε σώματα συναρτήσεων όπως και στην διατύπωση και εξήγηση του αναλόγου του θεωρήματος των Kronecker-Weber για σώματα συναρτήσεων. Στα τρία πρώτα κεφάλαια ακολουθούμε το βιβλίο του D. Goss, [4] ενώ το τελευταίο κεφάλαιο είναι βασισμένο στα βιβλία των M. Rosen [10] και V. Salvador- G. Daniel [13].

Σ. Χατζηδάβαρη, Αθήνα 2018.

Κεφάλαιο 1

Προσθετικά πολυώνυμα

Σκοπός αυτού του κεφαλαίου είναι να παρουσιάσουμε ιδιότητες των προσθετικών πολυωνύμων καθώς και για μερικά αποτελέσματα απο την θεωρία πολυωνύμων, τις εκδοχές τους σε χαρακτηριστική $p > 0$.

1.1 Ιδιότητες

Έστω k ένα σώμα, με $\overline{k}$ θα συμβολίζουμε την αλγεβρική κλειστότητα του k. Εκτός αν αναφέρεται διαφορετικά, θεωρούμε πως η χαρακτηριστική p του k είναι θετική $p > 0$.

Ορισμός 1.1.1. *Ένα πολυώνυμο $P(x) \in k[x]$ λέγεται προσθετικό αν $P(a+b) = P(a)+P(b)$ για $a, b \in k$. Το $P(x)$ θα λέγεται απόλυτα προσθετικό αν είναι προσθετικό πάνω στο $\overline{k}$.*

Παρατήρηση 1.1.2. *Σε σώμα χαρακτιριστικής $p > 0$, εξαιτίας του δυωνυμικό θεωρήματος , $(x+y)^p = \sum_{i=0}^{p} \binom{p}{i} x^i y^{p-i}$ και του $p|\binom{p}{i}$, $\forall i = 1, \ldots, p-1$ το πολυώνυμο $\tau_p(x) = x^p$ είναι (απόλυτα) προσθετικό.*

Επίσης άμεσα από τον ορισμό προκύπτει ότι το σύνολο των προσθετικών πολυωνύμων $A(k)$ με συντελεστές από το k, είναι κλειστό ως προς την πρόσθεση, το πολλαπλασιασμό με στοιχεία του k και τη σύνθεση, άρα όλα τα πολυώνυμα της μορφής $P(x) = a_0 x + x^{p^2} + \ldots + x^{p^r}$ είναι και αυτά (απόλυτα προσθετικά).

Άρα όλα τα μονώνυμα της μορφής $\tau_p^i(x) = x^{p^i}$ και όλα τα πολυώνυμα που παράγονται από αυτά είναι προσθετικά.

Ορισμός 1.1.3. *Θα συμβολίζουμε με $\langle \tau_p \rangle$ τον υπόχωρο του $k[x]$ που παράγεται απο όλους τους γραμμικους συνδιασμούς των τ_p^i, $\quad i = 0, 1, 2, \ldots$*

Απο την πάνω παράγραφο έχουμε οτι ο χώρος $\langle \tau_q \rangle$ είναι δακτύλιος με πολλαπλασιασμό τη σύνθεση πολυωνύμων. Έστω $q = p^h$. Ο δακτύλιος $\langle \tau_q \rangle$, αν $k \neq \mathbb{F}_q$, δεν είναι μεταθετικός αφού

$$\tau_q a = a^q \tau_q \quad \forall a \in k$$

Παρατήρηση 1.1.4. *Η παραπάνω παρατήρηση σε συνδυασμό με την θεωρία των μη μεταθετικών τελεστών που χρησιμοποιούνται στην κβαντομηχανική οι οποίοι όμως γίνονται μεταθετικοί τελεστές όταν η σταθερά Planck γίνει 0, οδήγησε σειρά μαθηματικών (Connes, Manin κ.α.) να εξετάσουν την οριακή κατάσταση ενός μυθικού αντικειμένου του*

σώματος με ένα στοιχείο, το οποίο αντιστοιχεί στην οριακή κατάσταση $q = 1$, δηλαδή $h = 0$, και στην οποία δακτύλιος τ_q γίνεται αντιμεταθετκός.

Στα πλαίσια της παραπάνω θεωρίας το όριο της γραμμικής άλγεβρας πάνω από ένα σώμα $\mathbb{F}_q$ όταν $q \to 1$ γίνεται η συνδυαστική (για παράδειγμα $\mathrm{GL}(n, \mathbb{F}_1) = S_n$).

Για μια εισαγωγή στην σημασία των μη αντιμεταθετικών τελεστών στην κβαντομηχανική όπως και στο πως η μη αντιμετάθεση οδηγεί στην αρχή απροσδιοριστίας προτείνουμε το [3]. Για μια εισαγωγή στον κόσμο του σώματος με ένα στοιχείο προτείνουμε το άρθρο των Kapranov Smirnov [8], στο οποίο αναφέρεται και η σχέση με τα Drinfeld modules, όπως και την πτυχιακή εργασία [17].

Πρόταση 1.1.5. *Έστω $P(x) \in k[x]$ είναι ένα προσθετικό πολυώνυμο.*

- *Αν το k είναι χαρακτηριστικής μηδέν τότε $P(x) = ax$ για κάποιο $a \in k$*
- *Αν το k είναι άπειρο σώμα χαρακτηριστικής $p > 0$ τότε $P(x) \in \langle \tau_p \rangle$, δηλαδή υπάρχουν $a_1 \in k$ με $0 \leq i \leq r$ ώστε*

$$P(x) = a_0 x + a_1 x^p + \ldots + a_r x^{p^r}.$$

Απόδειξη. Η κατεύθυνση ($\Leftarrow$) είναι η παρατήρηση 1.1.2 άρα μένει να δείξουμε την κατεύθυνση ($\Rightarrow$). Για τον σκοπό αυτό θεωρούμε την παράγωγο του $P(x)$ ως προς το x, $P'(x)$. Η οποία ορίζεται ως συνήθως, $P'(x) = \sum a_i i x^{i-1}$ αν $P(x) = \sum a_i x^i$.

Αρχικά ισχυριζόμαστε ότι αν το $P(x)$ είναι προσθετικό τότε

$$P'(x) \equiv c$$

για $c \in k$. Πράγματι, αν $a \in k$ τοτε το πολυώνυμο

$$P(x + a) - P(x) - P(a)$$

ισούται με μηδέν για κάθε $x \in k$, και αφού το k είναι άπειρο είναι ταυτοτικά μηδέν. Επίσης

$$P'(a) = \frac{d}{dx} P(x + a)\Big|_{x=0} = \frac{d}{dx}(P(x) + P(a))\Big|_{x=0} = P'(x)$$

Άρα, πάλι από το γεγονός ότι το k είναι άπειρο, βλέπουμε ότι

$$P'(x) \equiv P'(0) \equiv c.$$

Επομένως

$$P(x) = cx + \sum_{j=2}^{n} a_j x^{n_j}$$

με $n_j = 0(p)$. Γράφουμε

$$P(x) = P_0(x) + P_1(x)$$

όπου

$$P_0(x) = cx + \{\text{όροι που το } n_j \text{ είναι δύναμη του } p\}$$

και

$$P_1(x) = \{\text{όροι που το } n_j \text{ διαιρείται και από πρώτους διαφορετικούς του } p\}.$$

Θέλουμε να δείξουμε ότι $P_1(x) \equiv 0$. Αφού $P_0(x) \in \langle \tau_p \rangle$ έχουμε ότι και το $P_1(x) = P(x) - P_0(x)$ είναι προσθετικό. Έστω $\overline{k}$ η αλγεβρική κλειστότητα του k. Αρκεί να δείξουμε ότι $P_1(x) \equiv 0$ στην $\overline{k}$. Η απεικόνηση $\tau_p : \overline{k} \to \overline{k}$, $x \mapsto x$ είναι αυτομορφισμός. Έστω p^e να είναι η μεγαλύτερη δύναμη του p που διαιρεί όλα τα n_j και

$$P_2(x) = P_1(x)^{1/p^e} \in \overline{k}[x].$$

Η απεικόνηση $x \mapsto x^{1/p^e}$ είναι προσθετική (αν και όχι πολυώνυμο) απο το $\overline{k}$ στον εαυτό του, άρα το $P_2(x)$ είναι προσθετικό, ως συνάρτηση, απο το k στο $\overline{k}$. Από την προσθετικότητα του $P_2(x)$ στο k βλέπουμε ότι $P_2'(x) \equiv 0$. Από την κατασκευή του $P_2(x)$ αυτό μπορεί να συμβαίνει μόνο αν το $P_2(x)$ είναι ίσο με μηδέν. □

Αν μπορούμε να πάρουμε $p-$οστές ρίζες στο k,(όπως στο $\overline{k}$) τότε η παραπάνω απόδειξη μπορεί να απλοποιηθεί ως εξής, έχουμε ότι $P(x) = cx + H(x)^p$ και με επαγωγή καταλήγουμε στην επιθυμητή μορφή για το $H(x)$.

Αν το k είναι πεπερασμένο σώμα τότε το σύνολο των προσθετικών πολυωνύμων είναι υπερσύνολο του $\langle \tau_p \rangle$. Για παράδειγμα αν $k = \mathbb{F}_3$ τότε το $x + (x^3 - x)^2 = x + x^2 + x^4 + x^6$ είναι προσθετικό.

Πόρισμα 1.1.6. *Έστω σώμα k χαρακτηριστικής $p > 0$ τότε το σύνολο των απόλυτα προσθετικών πολυωνύμων είναι ίσο με το $\langle \tau_p \rangle$.*

Απόδειξη. Η αλγεβρική κλειστότητα ενός σώματος είναι άπειρο σώμα. Αν υποθέσουμε το αντίθετο έχουμε ότι το πολυώνυμο $f(x) = 1 + \prod_{a \in \overline{k}} (x - a)$ δεν έχει ρίζα στο $\overline{k}$, το αποίο είναι άτοπο. Επομένως από την πρόταση 1.1.5 έχουμε το ζητούμενο. □

Από δω και πέρα με τον όρο προσθετικό πολυώνυμο θα εννοούμε ένα στοιχείο του $\langle \tau_p \rangle$. Αν $\tau_p(x) = x^p$, υπάρχει ισομορφισμός μεταξύ του δακτυλίου των προσθετικών πολυωνύμων $A(k)$ και του $\langle \tau \rangle$

$$P(x) = \sum_{i=0}^{n} a_i x^{p^i} \longrightarrow P(\tau_p) = \sum_{i=0}^{n} a_i \tau_p^i$$

Έστω $\mathbb{F}$ ένα σώμα με $q = p^s$ στοιχεία, $\mathbb{F}_q \subset k$

Θέτουμε $\tau := {\tau_p}^s$, δηλαδή $\tau(x) = x^q$. Έτσι έχουμε ότι αν $P \in \langle \tau \rangle$ τότε $P(ax) = aP(x) \quad \forall a \in \mathbb{F}_q$. Δηλαδή το $\langle \tau \rangle$ είναι $\mathbb{F}_q$-άλγεβρα. Αν το $P(x)$είναι$\mathbb{F}_q$-γραμμικό με $P(\tau)$ θα συμβολίζουμε την αναπαράσταση του P στο $\langle \tau \rangle$. (Παρατηρούμε ότι η αναπαράσταση αυτή δεν είναι αποτέλεσμα της αντικατάστασης του x με τ στο $P(x)$). Επίσης έχουμε ότι $q^{\deg P(\tau)} = \deg P(x)$.

Έστω $k \supset \mathbb{F}_q$ να είναι ένα αλγεβρικά κλειστό σώμα,

Θεώρημα 1.1.7 (Θεμελιώδες θεώρημα προσθετικών πολυωνύμων)**.** *Έστω $P(x) \in k[x]$ ένα διαχωρίσημο πολυώνυμο, και $\{w_1, \ldots, w_n\}$ οι ρίζες του. Το $P(x)$ είναι προσθετικό αν και μόνο αν το σύνολο των ριζών του αποτελεί υποομάδα της προσθετικής ομάδας k.*

Απόδειξη. Αρχικά παρατηρούμε ότι η κατεύθυνση $\Rightarrow$ ισχύει γενικά, δηλαδή ακόμα και αν το πολυώνυμο δεν είναι διαχωρίσημο.

Για το αντίστροφο αρκεί να δείξουμε ότι αν $W = \{w_1, \ldots, w_n\}$ είναι προσθετική υποομάδα του k τότε το πολυώνυμο

$$P_W(x) := \prod_{i=1}^{m}(x - w_i)$$

είναι προσθετικό. Παρατηρούμε ότι, για $w \in W \quad P(x + w) = P(x) + P(w)$. Για $y \in k$ ορίζουμε

$$H(x) = P(x + y) - P(x) - P(y)$$

Για το $H(x)$ έχουμε $H(w) = 0, \forall x \in W$ και deg$P(x) >$ deg$H(x)$, άρα $H(x) \equiv 0$. Εστω τώρα y άγνωστος και

$$H_1(x) = P(x + y) - P(x) - P(y) \in K[x][y] = k[x, y]$$

Άρα $H(a) = 0, \forall a \in k$. Αφού το k είναι άπειρο σώμα (ως αλγεβρικά κλειστό) $H_1(y) = 0$. □

Πόρισμα 1.1.8. *Έστω $P(x)$ όπως πριν. Το $P(x)$ είναι $\mathbb{F}_q-$ γραμμικό αν και μονο αν το σύνολο των ριζών του W αποτελεί $\mathbb{F}_q-$ διανυσματικό υπόχωρο του k.*

Απόδειξη. Αρκεί να δείξουμε ότι αν ο W είναι $\mathbb{F}_q$-γραμμικός χώρος τότε το $P(x)$ είναι $\mathbb{F}_q$-γραμμικό. Έστω $\zeta \in \mathbb{F}_q$ και $H(x) = P(x) - \zeta P(x)$. Αν $|W| = q^i$ τότε deg$P(x) = q^i$. Αφού $\zeta \in \mathbb{F}_q$, $\zeta^{q^i} = \zeta$, άρα deg$H(x) < q^i$. Σε συνδυασμό με το ότι $H(w) = 0$ για κάθε $w \in W$. Άρα το $H(x)$ πρέπει να είναι ταυτοτικά μηδέν, $H(x) \equiv 0$. □

1.2 Ορίζουσες

Σε αυτή την παράγραφο θα επεκτείνουμε μία σειρά από τύπους σχετικά με τις ορίζουσες οι οποίοι για $q = 1$ ανάγωνται σε γνωστούς τύπους οριζουσών από την συνδυαστική.

Απο τον τύπο του Vandermonde για τον πίνακα

$$\begin{bmatrix} 1 & 1 & 1 & \ldots & 1 \\ x_1 & x_2 & x_3 & \ldots & x_n \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x_1^{n-1} & x_2^{n-1} & x_3^{n-1} & \ldots & x_n^{n-1} \end{bmatrix}$$

έχουμε

$$\det(A) = \prod_{j<i}(x_i - x_j).$$

Θα παρουσιάσουμε ενα ανάλογο αποτέλεσμα σε χαρακτηριστική p. Συνεχίσουμε να ακολουθούμε την ορολογία της πρώτης παραγράφου, $W \subset k$ είναι $\mathbb{F}_q$-υπόχωρος και $\{w_1, \ldots w_n\} \subset W$. Έστι ορίζουμε την Ορίζουσα Moore:

$$D(w_1, w_2, \dots, w_n) := \det \begin{pmatrix} w_1 & w_2 & \dots & w_n \\ w_1^q & w_2^q & \dots & w_n^q \\ \vdots & \vdots & \ddots & \vdots \\ w_1^{q^{n-1}} & w_2^{q^{n-1}} & \dots & w_n^{q^{n-1}} \end{pmatrix} \tag{1.1}$$
$$= \begin{pmatrix} \tau^0(w_1) & \tau^0 w_2 & \dots & \tau^0 w_n \\ \tau(w_1^q) & \tau(w_2^q) & \dots & \tau(w_n^q) \\ \vdots & \vdots & \ddots & \vdots \\ \tau^{n-1}(w_1^{q^{n-1}}) & \tau^{n-1}(w_2^{q^{n-1}}) & \dots & \tau^{n-1}(w_n^{q^{n-1}}) \end{pmatrix}$$

Πρόταση 1.2.1. *Τα $\{w_1, \dots, w_n\}$ είναι γραμμικά ανεξάρτα πάνω από το $\mathbb{F}_r$ αν και μονο αν $D(w_1, \dots, w_n) \neq 0$, όπου D είναι η ορίζουσα Moore.*

Αρα αν η διάσταση του υποχώρου W είναι ίση με το πλήθος των w_i τότε αυτά αποτελούν μια $\mathbb{F}_r$ βάση του.

Έστω $W \subseteq k$ να είναι ενας πεπερασμένα παραγόμενος $\mathbb{F}_r$ διανυσματικός χώρος με τα $w_1, \dots w_n$ να είναι μια $\mathbb{F}$ βάση του W. Ορίζουμε $W_i = \langle w_1, \dots w_i \rangle$ για κάθε i απο 1 έως n και για κάθε τέτοιο W_i

$$P_i(x) = \prod_{a \in W_i} (x - a)$$

Και $P_i(\tau)$ θα είναι η γραφή του $P_i(x)$ στο $k\{\tau\}$

Πρόταση 1.2.2. (i) $P_i(\tau) = (\tau - P_{i-1}(w_i)^{r-1}\tau^0)P_{i-1}(\tau)$.

(ii) $P_i(x) = \frac{D(w_1, \dots w_i, x)}{D(w_1, \dots w_i)}$.

(iii) $P_W(\tau) = P_{\overline{W}}(\tau)P_i(\tau)$

Πόρισμα 1.2.3. *Τύπος της ορίζουσας Moore*

$$(w_1, \dots w_n) = \prod_{i=1}^{n} \prod_{k_{i-1}\mathbb{F}_q} \cdots \prod_{k_1 \in \mathbb{F}_q} (w_i + k_{i-1}w_{i-1} + \cdots + k_1 w_1) \tag{1.2}$$

Απόδειξη. Απο την πάνω πρόταση άμεσα προκύπτει ότι

$$\frac{D(w_1, \dots, w_{n-1}, x)}{D(w_1, \dots w_{n-1})} = \prod_{1=1}^{n-1} \prod_{k_1 \in \mathbb{F}_q} (x - (k_1 w_1 + \dots k_{n-1}w_{n-1})) \tag{1.3}$$

Αν $x = w_n$

$$D(w_1, \dots, w_{n-1}, w_n) = D(w_1, \dots w_n) \prod_{i=1}^{n-1} \prod_{k_i \in \mathbb{F}_q} (w_n - (k_1 w_1 + \cdots + k_{n-1}w_{n-1}))$$

και με επαγωγή σε αυτή τη σχέχη έπεται το ζητούμενο. □

Εξισώνοντας τους συντελεστές του x στην σχέση 1.3 παίρνουμε το εξής ανάλογο του θεωρήματος του Wilson

Πόρισμα 1.2.4.

$$\prod_{w\in W} w = (-1)^n D(w_1,\dots,w_n)^{q-1}$$

Παρατήρηση 1.2.5. *Αφού το $\{w_1,\dots w_n\}$ μπορεί να είναι οποιοδήποτε γραμμικά ανεξάρτητο σύνολο, η* 1.2.3 *είναι ισοδύναμη με το ακόλουθο. Αν $\{x_1,\dots x_n\}$ είναι γραμμικά ανεξάρτητες μεταβλητές τότε έχουμε ισότητα στοιχείων του $\mathbb{F}_q[x_1,\dots x_n]$:*

$$\Delta(x_1,\dots x_d) = \prod_{i=1}^{d} \prod_{k_{i-1}\in\mathbb{F}_q} \cdots \prod_{k_1\in\mathbb{F}_q} (x_i + k_{i-1}x_{i-1} + \cdots + k_1x_1)$$

και η πάνω σχέση στο δεξί μέλος περιέχει ακριβώς έναν αντιπρόσωπο modulo $\mathbb{F}_q^*$ από κάθε μη μηδενική γραμμική απεικόνιση των $\{x_1,\dots x_n\}$ πάνω από το $\mathbb{F}_q$.

1.3 Η σχέση ανάμεσα στους δακτύλιους k[x] και k{τ}.

Θεώρημα 1.3.1. *Για ένα $f(x)\in k[x]$ υπάρχει ένα $g(\tau)\in k\{\tau\}$ ώστε $f(x)|g(x)$.*

Απόδειξη. Έστω $\overline{k}$ να είναι η αλγεβρική κλειστότητα του k. Έστω W να είναι ο $\mathbb{F}_q$ υπόχωρος που παράγεται απο τις ρίζες $w_1,\dots,w_m$ του $f(x)$, χωρίς να λάβουμε υπόψην την πολλαπλότητα.Ορίζουμε το $\mathbb{F}_q$-γραμμικό πολυώνυμο

$$P_W(x) = \prod_{w\in W} (x-w).$$

Επιλέγουμε το t να είναι η μεγαλύτερη πολλαπλότητα ρίζας του $f(x)$ και r είναι ο μικροτερος ακέραιος ώστε $q^r \geq t$. Τότε για $g(\tau) = \tau^r P_W(\tau)$ εχουμε ότι το $f(x)$ διαιρεί το $g(x)$ □

Απο την απόδειξη που αναφέρεται φαίνεται ότι κάθε πεπερασμένη επέκταση του $\mathbb{F}_q \subset k$ μπορει να υλοποιηθεί ως το σώμα διασπάσεως ενός $\mathbb{F}_q$-γραμμικού πολυωνύμου. Έστω $h(x)$ να είναι ένα οποιοδήποτε άλλο προσθετικό πολυώνυμο ώστε το $f(x)$ να διαιρεί τη έκφραση του $h(x)$. Τότε ο $\mathbb{F}_q$-υπόχωρος των ριζών W, περιέχεται στο σύνολο των ριζών του $h(x)$. Επομένως απο την πρόταση 1.2.2 υπάρχει πολυώνυμο $q(\tau)$ ώστε $h(\tau) = q(\tau)g(\tau)$

Αρα το σύνολο που αποτελείται από αυτά τα $g(\tau)$ είναι κύριο (αριστερό) ιδεώδες του $k\{\tau\}$, το οποίο οπως φαίνεται απο την απόδειξη είναι μη τετριμένο αφου κατασκευάσαμε εναν μη τετριμένο γεννητορα του ιδεώδους.

1.4 p-resultants

Έστω δυο πολυώνυμα στο $k[x]$

$$\begin{aligned} f(x) &= a_m x^m = +\cdots + a_1x + a_0 \\ g(x) &= b_n x^n + \cdots + b_1x + b_0 \end{aligned}$$

Η resultant των πολυωνύμων αυτών, $R(f,g)$ είναι η ορίζουσα του παρακάτω, $m+n$ τετραγωνικού, πίνακα.

$$\begin{pmatrix} a_m & \dots & a_0 & & & & & \\ & a_m & \dots & a_0 & & & & \\ & & & & \ddots & & & \\ & & & & & a_m & \dots & a_0 \\ b_n & \dots & b_0 & & & & & \\ & b_n & \dots & b_0 & & & & \\ & & & & \ddots & & & \\ & & & & & b_n & \dots & b_0 \end{pmatrix}$$

Αν $\{u_1, \dots, u_m\}$ και $\{v_1, \dots, v_n\}$ είναι οι ρίζες των f και g αντίστοιχα τότε έχουμε

Πρόταση 1.4.1.

$$R(f,g) = a_m^m {b_n}^n \prod_{i=1}^{m}\prod_{j=1}^{n}(u_i - v_j).$$

Παρατήρηση 1.4.2. (i) *Αν οι $a_m \neq 0$ και $b_n \neq 0$ τότε η resultant, $R(f,g) = 0$ αν και μόνο αν τα f και g έχουν κάποια κοινή ρίζα.*

(ii) *Η διακρίνουσα ενός πολυωνύμου $f(x))$ είναι η resultant του πολυωνύμου και της παραγώγου του $R(f, f')$*

Σκοπός εδώ είναι να ορίσουμε κάτι ανάλογο για $\mathbb{F}_q$- γραμμικά πολυώνυμα. Έστω $\{w_1, \dots w_n\}$ βάση για τον $\mathbb{F}_q-$ γραμμικό χώρο των λύσεων του $f(x)$ και όμοια θεωρούμε μια βάση $\{v_1, \dots v_m\}$ για τον χώρο των λύσεων του $g(x)$.

Ορισμός 1.4.3. *Η* p*-resultant είναι η ποσότητα:*

$$R(f(\tau)g(\tau)) := \frac{D(w_1, \dots, w_n, v_1, \dots, v_m)}{D(w_1, \dots, w_n)D(v_1, \dots, v_m)}.$$

Πρόταση 1.4.4. (i)

$$R(f(\tau)g(\tau))^{r-1} = R\left(\frac{f(x)}{x}, \frac{g(x)}{x}\right),$$

(ii)

$$R(f(\tau)g(\tau)) = \frac{D(f(v_1), \dots, f(v_m))}{D(v_1, \dots, V_m)} = \frac{D(g(w_1), \dots, g(w_n))}{D(w_1, \dots, w_n)}.$$

Άρα $R(f(\tau)g(\tau))^{r-1}$ είναι μηδέν αν και μόνο αν τα $f(x)$ και $g(x)$ είχουν μη τετριμένη ρίζα κοινή.

1.5 Αλγόριθμοι Διαίρεσης

Έστω $f(\tau), g(\tau) \in k\{\tau\}$.

Ορισμός 1.5.1. *Θα λέμε οτι το $f(\tau)$ διαιρείται απο αριστερά απο το $g(\tau)$ αν υπάρχει $h(\tau) \in k\{\tau\}$ ώστε $f(\tau) = h(\tau)g(\tau)$.*
Αντίστοιχα Θα λέμε οτι το $f(\tau)$ διαιρείται απο δεξιά απο το $g(\tau)$ αν υπάρχει $h(\tau) \in k\{\tau\}$ ώστε $f(\tau) = g(\tau)h(\tau)$.

Πρόταση 1.5.2 (αλγόριθμος δεξιάς διαίρεσης)**.**
Έστω $f(\tau), g(\tau) \in k\{\tau\}$ με $g(\tau) \neq 0$. Τότε υπάρχουν πολυώνυμα $h(\tau), r(\tau) \in k\{\tau\}$ με $\deg r(\tau) < \deg g(\tau)$ τέτοια ώστε
$f(\tau) = h(\tau)g(\tau) + r(\tau)$.

Απόδειξη. Είναι όμοια με την απόδειξη του κλασικού αλγόριθμου διαίρεσης. □

Παρατήρηση 1.5.3. *Αν το $f(\tau)$ διαιρείται από δεξιά από το $g(\tau)$ τότε το $f(x)$ διαιρείται από δεξιά από το $g(x)$. Επίσης το υπόλοιπο της διαίρεσης $r(\tau)$ είναι η αναπαράσταση στο $k\{\tau\}$ του υπολοίπου $r(x)$ της καλασικης διαίρεσης του $f(x)$ με το $g(x)$.*

Πόρισμα 1.5.4. *Κάθε αριστερό ιδεώδες του $k\{\tau\}$ είναι κύριο.*

Ορισμός 1.5.5. *Είναι σώμα k λέγεται τέλειο αν και μόνο αν $\tau(k) = k$.*
Η τελειοποιηση (perfection ή perfect closure) του k, k^{perf} ορίζεται ώς το υπόσωμα του $\overline{k}$, $\{x \in \overline{k} | \exists i \geq 0, x^{p^i} \in k\}$

Για παράδειγμα κάθε πεπερασμένο σώμα είναι τέλειο. Επίσης κάθε σωμα χαρακτηριστικής μηδέν είναι τέλειο.

Ορισμός 1.5.6. *Μια επέκταση L/k ονομάζεται πλήρως μη διαχωρίσιμη αν και μόνο αν για κάθε $a \in L$ το ελάχιστο πολυώνυμο του a πάνω από το k είναι δεν είναι διαχωρίσιμο.*

Αν το k είναι τέλειο τότε κάθε πεπερασμένη επέκταση του k θα είναι διαχωρίσιμη και κάθε αλγεβρικά κλειστό σώμα είναι τέλειο. Άρα η k^{perf}/k είναι πλήρως μη διαχωρίσιμη και περιέχει κάθε πλήρως μη διαχωρίσιμη επέκταση του k.

Πρόταση 1.5.7 (αλγόριθμος αριστερής διαίρεσης)**.**
Έστω να είναι τέλειο σώμα. Έστω $f(\tau), g(\tau) \in k\{\tau\}$ με $g(\tau) \neq 0$. Τότε υπάρχουν πολυώνυμα $h(\tau), r(\tau) \in k\{\tau\}$ με $\deg r(\tau) < \deg g(\tau)$ τέτοια ώστε

$$f(\tau) = g(\tau)h(\tau) + r(\tau)$$

Άρα ανάλογα με πριν έχουμε ότι τα $r(\tau)$ και $h(\tau)$ είναι μοναδικά.

Πόρισμα 1.5.8. *Αν k είναι τέλειο σώμα τότε κάθε δεξί ιδεώδες του είναι κύριο.*

Μπορούμε να ορίσουμε τον *δεξί* μέγιστο κοινό διαιρέτη των $f(\tau)$ και $g(\tau)$ ως τον μονικό γεννήτορα του αριστερού ιδεώδους που παράγεται από τα $f(\tau)$ και $g(\tau)$, $(h(\tau)) = (f(\tau)g(\tau))$, και τότε αφού τα υπόλοιπα στον αλγόριθμο της διαίρεσης στο $k\{\tau\}$ συμφωνούν με τα υπόλοιπα στο $k\{x\}$, το $h(x) \in k\{x\}$ είναι ο μέγιστος κοινός δαιρέτης των $f(x)$ και $g(x)$.

Ορισμός 1.5.9. *Θα λέμε ότι τα $f(\tau)$ και $g(\tau)$ είναι μεταξύ τους δεξιά πρώτα αν και μόνο αν $(f(\tau)g(\tau)) = \tau^0$*

Λήμμα 1.5.10. *Έστω $a \in \overline{k}$, $a \neq 0$. Το $f(\tau) = \sum_{j=0}^{n} a_j \tau^j$ διαιρείται απο δεξιά απο το $\tau - a\tau^0$ αν και μόνο αν το a είναι $(q-1)-$οστή δύναμη ρίζας του $f(x) = 0$.*

Πρόταση 1.5.11. *Κάθε $\mathbb{F}_q-$ γραμμική απεικόνιση απο το $\mathbb{F}_{q^n}$ στον εαυτό του προσέρχεται απο κάποιο πολυώνυμο $P(\tau) \in \mathbb{F}_{q^n}\{\tau\}$.*

Απόδειξη. Η διάσταση του $\mathbb{F}_q-$γραμμικού χώρου των $\mathbb{F}_q-$γραμμικών απεικονίσεων από το $\mathbb{F}_{q^n}$στον εαυτό του είναι n^2. Από την άλλη έχουμε ότι δύο $\mathbb{F}_q-$γραμμικά πολυώνυμα $f(\tau)$ και $g(\tau)$ δίνουν την ίδια $\mathbb{F}_q-$γραμμική απεικόνιση στο $\mathbb{F}_{q^n}$ αν και μόνο αν το $f(\tau) - g(\tau)$ διαιρείται από δεξιά με το $\tau^n - \tau^0$. Άρα οι απεικονίσιες $\tau^0, \ldots, \tau^n$ είναι γραμμικά ανεξάρτητες πάνω από το $\mathbb{F}_{q^n}$ ως συναρτήσεις. Ο χώρος που παράγουν πάνω από το $\mathbb{F}_{q^n}$ έχει διάσταση n^2 πάνω από το $\mathbb{F}_q$. □

1.6 τ - adjoint

Έστω $f(\tau) \in k\{\tau\}$ με $\deg(f(\tau)) = n$ $W \subset \overline{k}$ ο $\mathbb{F}_q-$διανυσματικός χώρος των ριζων του $f(x)$.

Ορισμός 1.6.1. *Έστω* $f(\tau) = \sum_{i=0}^{n} a_i \tau^i$, $a_n \neq 0$

(i) $f^*(\tau) = \sum_{i=0}^{n} a_i^{\frac{1}{q^i}} \tau^{-i} \in k^{\text{perf}}\{\tau^{-1}\}$, *(μορφή* τ^{-1}*)*

(ii) $f^{\text{ad}}(\tau) = \tau^n f^*(\tau) = \sum_{i=0}^{n} a_i^{q^{n-i}} \tau^{n-i} \in k\{\tau\}$, *(μορφή* τ*)*

Παράδειγμα 1.6.2. *Στο* $\mathbb{F}_q(T)$ *για το* $f(\tau) = T^2 + (T + T^q)\tau + \tau^2$ *έχουμε*

$$f^*(\tau) = T^2\tau^0 + (T + T^{\frac{1}{q}})\tau^{-1} + \tau^{-2}$$

και

$$f^{\text{ad}}(\tau) = T^{2q^2}\tau^2 + (T^{q^2} + T^q)\tau + \tau^0.$$

Λήμμα 1.6.3. *Έστω* $f(\tau), g(\tau) \in k\{\tau\}$, *τότε* $(f(\tau)g(\tau))^* = g^*(\tau)f^*(\tau)$.

Απόδειξη. Έστω $a, b \in k$. Παρατηρούμε ότι

$$\begin{aligned}(a\tau^m b\tau^j)^* &= (ab^{q^m}\tau^{m+j})^* \\ &= a^{q^{-m-j}} b^{q^{-j}} \tau^{-m-j} \\ &= (b^{q^{-j}}\tau^{-j})(a^{q^{-m}}\tau^{-m}).\end{aligned}$$

Το ζητούμενο έπεται άμεσα.

□

Ο σχηματισμός των τ-adjoints (αντ. τ^{-1}-μορφών) αντι-αντιμετατίθεται. Αυτό οδηγεί σε ένα αντι-ισομορφισμό του $\bar{k}\{\tau\}$ με το $\bar{k}\{\tau^{-1}\}$. Παρατηρούμε ότι τα $f^*(x)$ και $f^{\text{ad}}(x)$ έχουν τις ίδιες ρίζες.

Πόρισμα 1.6.4. *οι ρίζες του* $(f^{\text{ad}}(x))^{\text{ad}} = 0$ *είναι* q^n*-οστές δυνάμεις των ριζών του* $f(x) = 0$.

Θεώρημα 1.6.5. *Έστω* $f(\tau) = \sum_{i=0}^{n} a_i\tau^i$ *με* $a_n a_0 \neq 0$, *το* $f(x)$ *είναι διαχωρίσιμο. Τότε οι ρίζες του* $f(x)$ *και* $f^*(x)$ *δίνουν την ίδια επέκταση του* k.

Απόδειξη. Αρχικά μπορούμε να υποθέσουμε ότι το $f(\tau)$ είναι μονικό. Αν δεν είναι τότε γράφουμε $f(\tau) = af_1(\tau)$ με $a \in k^*$ και έχουμε ότι η ρίζες του $f^*(x)$ και $f_1^*(x)$ δίνουν την ίδια επέκταση του k αφού $f^*(\tau) = f_1^*(\tau)a\tau^0$. Αν το b είναι ρίζα του $f^*(x)$ έχουμε ότι το $b^{\frac{1-q}{q}}\tau^0 - \tau$ διαιρεί από αριστερά το $f(\tau)$ δηλαδή υπάρχει $Q(\tau) \in k\langle\tau\rangle$ ώστε

$$f(\tau) = (b^{\frac{1-q}{q}}\tau^0 - \tau)Q(\tau).$$

Έστω W να είναι οι ρίζες του $f(x) = 0$ και W_1 οι ρίζες του $Q(x) = 0$. Άρα $Q(x) = -P_{w_1}(x) = \prod_{w \in W_1}(x + w)$. Καθώς έχουμε υποθέσει το $f(\tau)$ να είναι μονικό από τη πρόταση 1.2.2 έχουμε ότι για κάθε $w \notin W_1$

$$f(\tau) = (\tau - P_{W_1}(w)^{q-1}\tau^0)P_{W_1}(\tau).$$

Άρα $b^{\frac{1-q}{q}} = P_{W_1}(w)^{q-1}$, ή $b = aP_{W_1}(w)^{-q}$. Αν L είναι το σώμα διασπάσεως του $f(x)$ από την υπόθεση για το f έχουμε ότι η L/k είναι διαχωρίσιμη.Το σώμα διασπάσεως του $f^{ad}(x)$, L_1, είναι υπόσωμα του L και αντίστοιχα το σώμα διασπάσεως του $(f^{ad}(x))^{ad} = 0$, L_2 είναι υπόσωμα του L_1. Απο το προηγούμενο πόρισμα έχουμε ότι οι ρίζεις του $(f^{\text{ad}}(x))^{\text{ad}} = 0$ είναι οι q^n-οστές δυνάμεις ριζών του $f(x) = 0$, δηλαδή η επέκταση L/L_2 είναι πλήρως μη διαχωρίσιμη. Η L/k είναι διαχωρίσιμη άρα πρέπει $[L : L_2] = 1$ δηλαδή $L = L_1 = L_2$.

□

1.7 Διαφορικές εξισώσεις

Σε αυτή την παράγραφο θα παρουσιάσουμε την αναλογία μερικών απο τα παραπάνω αποτελέσματα με τη θεωρία των διαφορικών εξισώσεων.

Έστω k σώμα χαρακτηριστικής p, ώστε $\mathbb{F}_q \subset k$ ($q = p^s$), στο οποίο έχουμε τον γραμμικό τελεστή

$$\tau : x \longrightarrow x^q$$

Αντίστοιχα, στο σώμα $K = \mathbb{C}(t)$ έχουμε τον $\mathbb{C}$-γραμμικό τελεστή

$$D = \frac{d}{dt}$$

Ο δακτύλιος $\{K(D)\}$, δηλαδή οι εκρφάσεις της μορφής $\sum_{i=0}^{n} f_i(t)D^i$, $f_i(t) \in \mathbb{C}(t)$, είναι ανάλογος με τον δακτύλιο των προσθετικών πολυωνύμων αφού η σχέση

$$\tau a = a^q \tau$$

είναι ανάλογη με την

$$Df = f'D.$$

Αν $f(\tau) = \sum_{i=0}^{n} a_i \tau^i$ με $a_i \in k$ και $a_0 a_n \neq 0$ η $f(z) = 0$, τότε έχει βάση n γραμμικά ανεξάρτητων λύσεων πάνω από το σώμα $\mathbb{F}_q$, δηλαδή τις σταθερές για τον τ. Έτσι όπως και η διαφορική εξίσωση τάξης n, $F(D)y = 0$ όπου $F(D) = \sum_{i=0}^{n} f_i(t)D^i$ έχει n γραμμικά ανεξάρτητες λύσεις πάνω από τις D-σταθερές $\mathbb{C}$.

Από την πρόταση 1.2.2 γνωρίζουμε ότι η τυχαίες λύσεις της $f(z) = 0$, $w_1, \ldots, w_n$ είναι γραμμικά ανεξάρτητες πάνω απο το $\mathbb{F}_q$ αν και μόνο αν η ορίζουσα Moore είναι μη μηδενική, $D(w_i, \ldots w_n) \neq 0$. Ομοιος έχουμε ότι αν $y_1(t), \ldots y_n(t)$ είναι n λύσεις της $F(D)y = 0$ τότε αυτές είναι γραμμικά ανεξαρτητες αν και μόνο αν η ο ορίζουσα Wronski δεν είναι μηδέν.

$$\begin{aligned} W(t) &= W(y_1(t), \ldots y_n(t) \\ &= \begin{pmatrix} y_1(t) & \ldots & y_n(t) \\ y_1'(t) & \ldots & y_n'(t) \\ \vdots & \vdots & \vdots \\ y_1^{n-1}(t) & \ldots & y_n^{n-1}(t) \end{pmatrix} \end{aligned}$$

Ακόμα περισσότερο μπορούμε να έχουμε σχέση για την ορίζουσα του Moore ανάλογη με αυτή του Abel για την Wronskian

$$W'(t) + \frac{f_{n-1}(t)}{f_n(t)} W(t) = 0 \tag{1.4}$$

Για $n = 2$στην περίπτωση της παραγώγου έχουμε

$$f_2(t)y'' + f_1(t)y' + f_0(t)y = 0 \tag{1.5}$$

Αν υποθέσουμε ότι στην περιοχή που μας ενδιαφέρει $f_2(t) \neq 0$ τότε μπορούμε να μετασχηματίσουμε την 1.5 στην

$$y'' + g_1(t)y' + g_0(t)y = 0$$

Έστω τα y_1, y_2 να είναι μια βάση για το χώρο των λύσεων τότε

$$y_1'' + g_1(t)y_1' + g_0(t)y_1 = 0 \tag{1.6}$$
$$y_2'' + g_1(t)y_2' + g_0(t)y_2 = 0 \tag{1.7}$$

Απο τις 2 πάνω εξισώσεις έχουμε

$$(y_1y_2'' - y_2Y_1'') + g_1(t)(y_1y_2' - y_2)y_1' = 0$$

και επειδή $W'(t) + g_1(t)W(t) = 0$ παίρνουμε τον τύπο του Abel για την ορίζουσα Wronsky

$$W'(t) + g_1(t)W(t) = 0$$

Ακριβώς ανάλογα η $f(z) = 0$ για $n = 2$ είναι

$$a_2z^{q^2}n + a_1z^q + a_0z = 0,$$

με ${}_{02} \neq 0$, και με τον ίδιο τρόπο παίρνουμε

$$z^{q^2} + b_1z^q + b_0z = 0$$

Αν w_1, w_2 είναι μια βάση για τις λύσεις της απο πάνω εξίσωσης έχουμε

$$w_1^{q^2} + b_1w_1^q + b_0w_1 = 0 \tag{1.8}$$
$$w_2^{q^2} + b_1w_2^q + b_0w_2 = 0 \tag{1.9}$$

και απο αυτές παίρνουμε την

$$(w_2^{q^2}w_1^q - w_1^{q^2}w_2^q) + b_0(w_2w_1^q - w_1w_1^q) = 0$$

ή

$$D(w_1, w_2)^q - b_0D(w_1, w_2) = 0,$$

δηλαδή η ορίζουσα Moore ικανοποιεί την ακόλουθη σχέση ανάλογη με τον τύπο του Abel

$$z^q - b_0z = 0$$

Γενίκευση αυτής της σχέσης είναι η ακόλουθη πρόταση η οποία είναι ανάλογη της 1.4. Ο παρακάτω τύπος χρησιμοποιεί τον συντελεστή που αντιστοιχεί στη νόρμα, $(-1)^n a_0$, εκεί που ο 1.4 χρησιμοποιεί το συντελεστή του ίχνους, $-a_{n-1}$.

Πρόταση 1.7.1. *Έστω* $f(\tau) = \sum_{i=0}^{n} a_i \tau^i$ *και* $w_1, \dots w_n$ *είναι τυχαίες ρίζες του* $f(z) = 0$. *Αν* $D = D(w_1, \dots w_2)$ *είναι η ορίζουσα Moore των ριζών αυτών τότε*

$$a_n D^q + (-1)^{n+1} a_0 D = 0$$

Συνεχίζουμε παρατηρόντας ότι οι τ-adjoints είναι ανάλογες με τη θεωρία των adjoints γραμμικών διαφορικών εξισώσεων του Lagrange. Αν

$$F(D)y = f_2 y'' + f_1 y' + f_0 y$$

τότε η adjoint είναι

$$F^*(D) = (f_2 y)'' + (f_1 y)' + f_0 y$$

Η οποία είναι παρόμοια με την $f^*(x)$ όταν deg $f(\tau) = 2$.

Οι σταθερες για την παραγώγηση D, το $\mathbb{C}$, είναι οι λύσεις της διαφορικής εξίσωσης $Dy = 0$. Ενώ οι σταθερες $\mathbb{F}_q$ του τ είναι λύσεις της $\tau y = y$. Αν προσπάθήσουμε να βρούμε κάποιον τελεστη δ ώστε $\mathbb{F}_q = \{y | \delta y = 0\}$ καταλήγουμε στον $\delta y = \tau(y) - y = y^q - y$ ο ποίος θυμίζει Artin-Schreier πολυώνυμο. Επίσης παρατηρούμε οτι ο δ αποτελεί μια «τ-διαφόριση» αφού

$$\delta(xy) = x\delta y + \tau(y)\delta x$$

Αν $u \in k - \mathbb{F}_q$ και $y \in k$ τότε

$$\frac{\delta y}{\delta u} = \frac{\tau y - y}{\tau u - u}$$

και έτσι παίρνουμε ένα κανόνα αλυσίδας

$$\frac{\delta y}{\delta x} = \frac{\delta y}{\delta u}\frac{\delta u}{\delta x}$$

Τέλος θα παρουσιάσουμε αναλογία με την διαφορική αλγεβρα. Ένα διαφορικό σώμα (differential field)K είναι ένα σώμα εφοδιασμένο με μια παραγώγιση, $\forall a \in K$

$$a \longrightarrow a'$$

και k το σώμα των σταθερών του, $k = \{a \in K | a' = 0\}$ το οποίο υποθέτουμε αλγεβρικά κλειστό. Για παράδειγμα το σώμα των ρητων συναρτήσεων μια μεταβήτής πάνω από το σώμα των μηγαδικών αριθμών $K = \mathbb{C}(T)$αποτελεί διαφορικό σώμα, με σταθερό σωμα το $\mathbb{C}$ και η διαφόριση είναι η συνήθης παραγωγος ως προς τη μεταβλητή .

$$f(T) \longrightarrow \frac{d}{dT} f(T)$$

.

Έστω ένα διαφορικό σώμα πάνω από το , δηλαδή το έχει μια διαφόριση και το K είναι σταθερό σωμα για αυτή τη διαφόριση.Η διαφορική ομάδα Galois της M/K είναι η ομάδα όλων των διαφορικών αυτομορφισμών, δηλαδή όλων των αυτομορφισμών της M/K που μετατίθενται με μια δεδομένη παραγώγιση.

Έστω η γραμμικη διαφορική εξίσωση τάξης n

$$L(y) = y^{(n)} + a_1 y^{(n-1)} + a_2 y^{(n-2)} \dots + a_n y = 0 \tag{1.10}$$

Ένα διαφορικό σώμα M πάνω από το K λέγεται Picard-Vessiot επέκταση αν και μόνο αν

(i) Το M παράγεται πάνω απο το K απο τα $v_1, \dots v_n$ τα οποία ικανοποιούν την εξίσωση 1.10 και είναι γραμμικά ανεξάρτητα πάνω απο το K.

(ii) Το M έχει το ίδιο σώμα σταθερών με το K.

Από την υπόθεση για την κλειστότητα του k μπορούμε πάντα να φτιάξουμε τέτοια επέκταση. Η διαφορική ομάδα Galois θα είναι πάντα γραμμική ομάδα.

Παράδειγμα 1.7.2. *Έστω $M = \mathbb{C}(x_1, \dots, x_n)$ το σώμα που παράγεται απο ν διαφορικούς αγνώστους , δηλαδή στο σώμα $\mathbb{C}$ επισυνάπτουμε πρώτα τα $x_1, \dots, x_n$ μετα τα $x_1', \dots, x_n'$ συνεχίζουμε έτσι και τελικά το M είναι το σώμα πηλίκων. Αν $(a_{ij}) \in \mathrm{GL}_n(\mathbb{C})$ τότε*

$$ax_i^{(m)} = \sum a_{ij} x_j^{(m)}, \quad m = 0, ..$$

ετσι παίρνουμε διαφορικούς αυτομορφισμούς του M.

Έστω να είναι το σταθερό σώμα της $\mathrm{GL}_n(\mathbb{C})$ κάτω απο το . Η

$$L(y) = \frac{W(y, x_1, \dots, x_n)}{W(x_1, \dots, x_n)} \tag{1.11}$$

είναι διαφορική εξίσωση με συντελεστές από το K και κάθε $x_1, \dots, x_n$ ικανοποιεί την $L(y) = 0$. Επομένως η M/K αποτελεί Picard-Vessiot επέκταση με διαφορική ομάδα Galois να είναι όλη η $\mathrm{GL}_n(\mathbb{C})$.

Επιστρέφοντας στα προσθετικά πολυώνυμα η διαφορική ομάδα Galois αντιστοιχεί στην ομάδα Galois. Έστω $f(\tau) \in k\{\tau\}$ ένα διαχωρίσιμο πολυώνυμο όπου $\mathbb{F}_q \subset k$ και το σώμα διασπάσεως του $f(x)$. Αν τα $w_1, \dots w_n$ είναι μια $\mathbb{F}_q$ βάση για τις λύσεις του $f(x)$

Στο επόμενο παράδειγμα φαίνεται πως αν αντικαταστήσουμε την ορίζουσα Wronski με την ορίζουσα Moore παίρνουμε όλη την $\mathrm{GL}_n(\mathbb{F}_q)$ ώς την ομάδα Galois της επέκτασης

Παράδειγμα 1.7.3. *Ακριβώς όπως στο προηγούμενο παράδειγμα θέτουμε $M = k(x_1, \dots x_n)$. Έστω $a = (a_{ij}) \in \mathrm{GL}_n(\mathbb{F}_q)$, τότε*

$$ax_i = \sum a_{ij} xj$$

δηλαδή έχουμε έναν αυτομορφισμό του M. Αν είναι το σταθερό σώμα της $\mathrm{GL}_n(\mathbb{F}_q)$ εύκολα έχουμε ότι το M είναι το σώμα διασπάσεως του πολυωνύμου με συντελεστές από το K

$$\frac{D(y, x_1, \dots, x_n)}{D(x_1, \dots x_n)}.$$

Κεφάλαιο 2

Μη-αρχιμήδεια ανάλυση

2.1 Βασικοί ορισμοί

Ορισμός 2.1.1. *Μια απόσταση d σε ένα σύνολο E θα λέγεται υπερμετρική αν ικανοποιεί τις συνήθεις ιδιότητες*

(i) $d(a,b) \geq 0$ *και* $d(a,b) = 0 \iff a = b$

(ii) $d(a,b) = d(b,a)$

και η τριγωνική ανισότητα έχει αντικατασταθεί απο την εξης ισχυρότερη

$$d(a,c) \leq \max\{d(a,b), d(b,c)\} \tag{2.1}$$

Η 2.1 καλείται υπερμετρική ανισότητα.

Παρατήρηση 2.1.2. *Ως συνέπεια της 2.1 έχουμε ότι :*

$$d(a,b) < d(b,c) \implies d(a,c) = d(b,c)$$

Ενδιαφέρουσες είναι οι γεωμετρικές συνέπειες της 2.1. Όλα τα τρίγωνα είναι ισοσκελή και ότι κάθε σημείο σε ένα δίσκο είναι το κέντρο του. Έστω

$$D_a(r) = \{x | d(a,x) \leq r\}$$

$$D_a(r^-) = \{x | d(a,x) < r\}$$

τότε για κάθε $b \in D_a(r)$ έχουμε $D_b(r) = D_a(r)$. Αν η «περίμετρος» δεν είναι άδεια τότε περιέχει κάθε «ανοικτό δίσκο» $D_b(r^-)$ για κάθε σημείο της b.

Εξίσου ενδιαφέρουσες είναι και οι τοπολογικές συνέπειες.

Πρόταση 2.1.3. *Κάθε δίσκος $D_a(r)$ ή $D_a(r^-)$ είναι και κλειστός και ανοικτος ταυτόχρονα.*

Απόδειξη. Έστω $D_a(r^-)$ ανοικτός δίσκος και $y \in D_a(r^-)^{\mathsf{c}}$ τότε $d(a,y) \geq r$ και $D_a(r^-) \cap D_(r^-) = \emptyset$. Πράγματι έστω z που να ανήκει σε αυτή την τομή, τότε

$$d(a,y) \leq \max\{d(a,z), d(y,z)\} < r$$

το οποίο είναι άτοπο. Άρα $y \notin \mathrm{cl}D_a(r^-)$ και ο $D_a(r^-)$ είναι ανοικτός. □

Βλέπουμε ότι με την επαγώμενη τοπολογία κάθε σημείο στον χώρο έχει μια βάση περιοχών αποτελούμενη από δισκους που είναι και ανοικτοί και κλειστοί. Ένας τέτοιος τοπολογικός χώρος θα λέγεται πλήρως μη συνεκτικός.

Παρατήρηση 2.1.4. *Αν το σύνολο E είναι μεταθετικός δακτύλιος, είναι φυσικό να απαιτήσουμε η απόσταση d να σέβεται την πρόσθεση, δηλαδή*

$$d(a+c, b+c) = d(a, b).$$

Τότε η απόσταση είναι πλήρως καθορισμένη απο την $d(a, 0) = d(0, a)$

Ορισμός 2.1.5. *Μια απόλυτη τιμή $|\quad| : K \to \mathbb{R}_{\geq 0}$ ικανοποιεί τις ιδιότητες*

(i) $|x| = 0 \iff x = 0$

(ii) $|ab| = |a||b| \quad \forall a, b \in K^*$

(iii) $|a + b| \leq |a| + |b| \quad \forall a, b \in K^*$

Αν μια απόλυτη τιμή αντί για την σχεση (ii) ικανοποιεί την ισχυρότερη

$$|a + b| \leq \max(|a|, |b|) \quad \forall a, b \in K^*$$

τότε θα λέγεται επίσης υπερμετρική ή μη-αρχιμήδεια (σε αναφορά της αρχιμήδειας ιδιότητας του R, όπου κάποιος μπορεί να φτάσει από το μηδέν σε οποιονδήποτε αριθμό με βήματα οποιουδήποτε μήκους). Η σχέση αυτή αντίστοιχα θα λέγεται υπερμετρική ή μη-αρχιμήδεια ανισότητα.

Ορισμός 2.1.6. *Ένα σώμα αυθαίρετης χαρακτηριστικής λέμε ότι είναι πλήρες ως προς μια πραγματική εκτίμηση v αν υπάρχει απεικόνιση $v : K \to \mathbb{R} \cup \{\infty\}$ τέτοια ώστε για κάθε $x, y \in K$,*

(i) $v(x) = \infty \iff x = 0$*,*

(ii) $v(xy) = v(x) + v(y)$*, και*

(iii) $v(x + y) \geq \inf(v(x), v(y))$.

Η v μπορεί να κάνει το σώμα K τοπολογικό χώρο με την εξής έννοια, ένα στοιχείο $x \in K$ θα είναι «μικρό» αν το $v(x)$ είναι μεγάλο (με την συνήθη έννοια στο R) και αντίστοιχα δυο στοιχεία του είναι «κοντά» αν η εκτίμηση είναι μεγάλη. Άρα έχει νόημα να μιλάμε για ακολουθείες Cauchy στο K,και η έννοια της πληρότητας, ως συνήθως, σημαίνει ότι κάθε ακολουθία Cauchy από στοιχεία του K συγκλίνει σε ένα στοιχείο του K.

Έστω $\alpha \in \mathbb{R}$ με $0 < \alpha < 1$ μπορούμε να ορίσουμε απόλυτη τιμή $|\quad|_v : K \to \mathbb{R}_{\geq 0}$ θέτοντας

$$|x|_v = \alpha^{v(x)}.$$

Εύκολα παρατηρούμε ότι για αυτή την απόλυτη τιμή ισχύουν οι ιδιότητες μια μη-αρχιμήδειας απόλυτης τιμής.

Η υπερμετρική απόσταση που παίρνουμε από την εκτίμηση v είναι

$$d(a, b) = |a - b|_v = \alpha^{v(a-b)}.$$

Παρατήρηση 2.1.7. *Αντίστοιχη κατασκευή μπορούμε να έχουμε και για μεταθετικό δακτύλιο R αν και μόνο αν δεν έχει μηδενοδιαιρέτες. Για παράδειγμα μπορούμε να εφοδιάσουμε κάθε δακτύλιο με την τετριμμένη εκτίμηση*

$$v(a) = 0 \quad \forall a \in R \quad a \neq 0$$

Σε τέτοια περίπτωση λέμε οτι έχουμε εναν δακτύλιο εκτίμησης. Αν επιπλέον η εκτίμηση είναι στο $\mathbb{N}$ τότε θα λέγεται δακτύλιος διακρητής εκτίμησης. Την εκτίμηση αυτή μπορούμε να την επεκτείνουμε φυσιολογικά στο σώμα πηλίκων του δακτυλίου

$$v\left(\frac{a}{b}\right) = v(a) - v(b)$$

Έστω ο δακτύλιος

$$R = R_K = \{x \in K || x|_v \leq 1\},$$

ο δακτύλιος των «ακεραίων» του K ο οποίος είναι τοπικός με μέγιστο ιδεώδες το:

$$M = M_K = \{x \in K || x|_v < 1\}.$$

Προφανώς, αφού κάθε στοιχείο του που δεν ανήκει στο M θα έχει απόλυτη τιμή ίση με 1 και αρα θα είναι αντιστρέψιμο στο R. Άρα το σύνολο

$$k = R/M$$

είναι σώμα και αποκαλείται τω σώμα των υπολοίπων του K.

2.2 Γενικός τροπος κατασκευης υπερμετρικών χώρων

Θα εξετάσουμε ένα αντικείμενο σε διάφορα επίπεδα μεγένθυσης. Σε κάθε επίπεδο το αντικείμενο αποτελείται από ένα σύνολο σημείων (πεπερασμένων ή όχι). Για παράδειγμα σε επίπεδο «μηδενικής» μεγένθυσης έχουμε το ίδιο το αντικείμενο. Καθώς μεγενθύνουμε κάθε «σημείο» φαίνεται να είναι σύμπλεγμα από μικρότερα «σημεία» τα οποία με τη σειρά τους αποτελούνται από «υποσημεία». Σκοπος είναι να περιγράψουμε το αντικείμενο κάτω από άπειρη μεγένθυση.Το μαθηματικό μοντέλο χτίζεται ως εξής: έστω E_n, $n = 0, 1, ...$ άπειρη ακολουθία συνόλων που συνδέονται από απεικονίσεις $\phi_n : E_{n+1} \mapsto E_n$. Γραφικά μπορούμε να παρουσιάσουμε την κατάσταση αυτή ως ένα δέντρο του οποίου οι κορυφές είναι στοιχεία του $\cup E_n$ και οι ακμές του συνδέουν το $a_{n+1} \in E_{n+1}$ με το $\phi(a_{n+1})$.

Για να αναπαραστήσουμε το αντικείμενό μας χρησιμοποιούμε τα «φύλλα» του δέντρου (ή άπειρα μονοπάτια που ξεκινάνε απο την «ρίζα» E_0), πιό συγκεκριμένα το σύνολο των ακολουθιών $a = \{a_n\}$ τέτοιες ώστε $a_n \in E_n : \phi(a_{n+1}) = a_n$. Τότε το E λέγεται το αντίστροφο όριο του συνόλου E_n

$$E = \varprojlim E_n$$

Θα ορίσουμε μια «φυσιολογική» απόσταση στο δέντρο ώστε το E να εφοδιαστεί με μια υπερμετρική τοπολογία. Έστω $\{d_n\}$ μια οποιαδήποτε ακολουθία που φθίνει γνησίως στο 0 (για παράδειγμα $d_n = a^n$ με $a < 1$) και ορίζουμε οτι κάθε ακμή που συνδέει κορυφή στο E_{n+1} με κορυφή στο E_n θα έχει μήκος $\frac{1}{2}(d_n - d_{n+1})$. Τότε κάθε άπειρο μονοπάτι που ξεκινάει απο φύλλο και τερματίζει στο E_n έχει μήκος $\frac{1}{2}d_n$. Μπορούμε

λοιπόν να ορίσουμε ως απόσταση στο E το μήκος του μικρότερου μονοπατιού που πηγαίνει από ένα "φύλλο" σε ένα άλλο και περνάει μέσα απο το δέντρο. Έστω a, b δύο στοιχεία του E δηλαδή δυο ακολουθίες $\{a_n\}, \{b_n\}$ τότε:

$$v(a,b) = \sup\{n : a_n = b_n\}$$

(δηλαδή n είναι το επίπεδο όπου βρίσκεται ο πρώτος κοινός πρόγονος των a και b και $a_n = b_n$ σημαίνει ότι $a_i = b_i$ για $i \leq n$) και αρα η σχέση

$$d(a,b) = \alpha^{v(a-b)}, \quad 0 < a < 1$$

ορίζει υπερμετρική απόσταση στο E.

Παρατήρηση 2.2.1. *Ο τοπολογικός χώρος E είναι ανεξάρτητος από την επιλογή της ακολουθίας $\{d_n\}$ και πλήρης. Πράγματι, αν $a(m)$ είναι μια ακολουθία Cauchy στον E τότε για αρκετά μεγάλο m η $a(m)$ θα περιορίζεται στον ίδιο δίσκο (λόγω της υπρμετρικής ανισότητας απαιτείται να κάνουμε βήμα μεγαλύτερο από την ακτίνα για να βγούμε έξω από τον δίσκο), άρα η ακολουθία $a(m)_n$ θα πρέπει να είναι τελικά σταθερή. Αν ορίσουμε $a_n = \lim a(m)_n$ για κάθε n, τότε $a = \lim a(m)$. Ο χώρος E είναι συμπαγής αν και μόνο αν τα σύνολα E_n είναι πεπερασμένα. Πράγματι, αν το E είναι συμπαγές τότε οι ανοικτοί δίσκοι ακτίνας d_n είναι σε ένα προς ένα και επί αντιστοιχία με τα στοιχεία του E_n, και αποτελούν μια ξένη κάλυψη του . Επομένως πρέπει να είναι πεπερασμένα. Αντίστροφα αν το E_n είναι πεπερασμένο τότε για κάθε ακολουθία $a(m)$ στο E υπάρχει $a \in E$ τέτοιο ώστε για όλα τα n έχουμε $a(m)_n = a_n$ για πεπερασμένο πλήθος m. Επομένως έχουμε το a να είναι όριο της ακολουθίας και ο E είναι συμπαγής. Αν η v είναι εκτίμηση μπορούμε να επιλέξουμε $d_n = \alpha^n$ και η απόσταση γίνεται απόλυτη τιμή.*

Σε πολλά απο τα παραδείγματα είναι δυνατόν να «σηκώσουμε» το E_n στο E_{n+1} επιλέγοντας μια απο τις ακμές που συνδέουν στοιχείο του E_n με στοιχείο του E_{n+1}. Υπάρχει δηλαδή υπάρχει $\psi_n : E_n \mapsto E_{n+1}$ ώστε η σύνθεση $\phi_n \circ \psi_n$ να είναι η ταυτοτική. Σε αυτή την περίπτωση τα στοιχεία του E μπορούν να δοθούν οπως περιγράφουμε παρακάτω. Έστω $E_{[n]}$ να είναι το πηλίκο $E_{n+1}/\psi_n(E_n)$ (ισομορφικό με τον πυρήνα του ψ_n), τότε το στοιχείο $\{a_n\}$ του E_n είναι πλήρως καθορισμένο απο τη ακολουθία $a_{[0]}, \ldots a_{[n]}, \ldots$ όπου $a_{[0]} = a_1$ και $a_{[n]}$ είναι η εικόνα του a_{n+1} στο $E_{n+1}/\psi_n(E_n)$. Αυτή η αναπαράσταση είναι κάτι σαν γενικευμένη μορφή του δεκαδικού αναπτύγματος. Για κάθε n υπάρχει μια "κανονική ανύψωση" Φ του E_n στο E όπου του $\Phi(a_n)$ δίνεται από το άπειρο μονοπάτι που περνάει από το a_n και αποτελείται από τις επιλιγμένες ακμές.

2.3 Δύο βασικά παραδείγματα

θα δούμε 2 βασικά παραδείγματα αυτης της κατασκευής.

1. $K = \mathbb{Q}_p$ όπου p πρώτος αριθμός.

   Θα περιγράψουμε αρχικά πως προκύπτουν οπως στην πάνω κατασκευή.

   Έστω $E_n = \mathbb{Z}/p^n\mathbb{Z}$ ο δακτύλιος των ακεραίων modulo p^n. Η προβολή από το E_{n+1} στο E_n δίνεται από το υπόλοιπο με της δαίρεσης με το p^n και μπορούμε έτσι να κατασκευάσουμε έναν δακτύλιο E οπως στην προηγούμενη παράγραφο, τον συμβολίζουμε με $\mathbb{Z}_p$ και καλείται ο δακτύλιος των $p-$αδικών ακεραίων.

   Αν χρησιμοποιήσουμε το $[0, 1, ..., p-1]$ ως σύνολο αντιπροσώπων το E_n είναι υποσύνολο του E_{n+1}. Παρ'ολο που αυτή η εμφύτευση δεν είναι ομορφισμός

δακτυλίων (για παράδειγμα το $1 + (p^n - 1)$ είναι ίσο με το 0 στο E_n άλλα όχι στο E_{n+1}) μπορούμε να εφαρμόσουμε αυτά που περιγράψαμε στην τελευταία παράγραφο του 2.2. Ο δακτύλιος $\mathbb{Z}_p$ είναι το σύνολο των σειρών

$$a = \sum_{n=0}^{\infty} a_{[n]} p^n, \quad a_{[n]} \in [0, \ldots, p-1]$$

Με αυτό το συμβολισμό η ($p-$αδική) εκτίμηση ενός $p-$αδικού ακεραίου είναι ο μικρότερος ακέραιος n ώστε $a_{[n]} \neq 0$. Ο αριθμός που χρησιμοποιούμε για να ορίσουμε την αντίστοιχη απόλυτη τιμή είναι ο $\frac{1}{p}$ και άρα η $p-$αδική απόσταση ανάμεσα σε δύο $p-$αδικούς αριθμούς a και b είναι $\left(\frac{1}{p}\right)^{v(a-b)}$.

Το σώμα πηλίκων του $\mathbb{Z}_p$, το $\mathbb{Q}_p$,ονομάζεται το σώμα των $p-$αδικών αριθμών Η $p-$αδική εκτίμηση $v(r)$ για έναν ρητό αριθμό $r \in Q$ δίνεται απο την

$$p^{v(r)} \frac{m}{d} \text{ όπου } m \text{ και } d \text{ πρώτοι ως προς τον } p$$

και η αντίστοιχη απόλυτη τιμή δίνεται, όπως και στον $\mathbb{Z}_p$ απο την

$$|r|_p = \left(\frac{1}{p}\right)^{v(r)}$$

Το σώμα $\mathbb{Q}_p$ είναι η πλήρωση του $\mathbb{Q}$ ως προς την εκτίμηση αυτή.

Για κάθε πρώτο p έχουμε ορίσει μια εκτίμηση (άρα και απόλυτη τιμή) στο $\mathbb{Q}$. Ολες οι $p-$ αδικές μαζί με την κλασική απόλυτη τιμή είναι ουσιαστικά οι μοναδικές, με την έννοια ότι κάθε μη τετριμμένη εκτίμηση στο $\mathbb{Q}$ είναι ισοδύναμη είτε με την κλασική ή με κάποια $p-$αδική. Επίσης συνδέονται με τον εξής τύπο

$$|r|_\infty \prod_{p \text{ πρώτος}} |r|_p = 1$$

Παρατήρηση 2.3.1. *Έστω $x_n \in \mathbb{Q}$ που συγκλίνει στο $x \in \mathbb{Q}_p$ από την υπερμετρική ανισότητα παρατηρούμε ότι, για μεγάλο n έχουμε $|x_n|_v = |x|$. Δηλαδή με την πλήρωση δεν προσθέσαμε νεες τιμές το οποίο προφανώς δεν ισχύει για την συνήθη απόλυτη τιμή και την πλήρωση του $\mathbb{Q}$ ως προς αυτήν $\mathbb{R}$.*

Πρόταση 2.3.2. *Ο $\mathbb{Q}_p$ ως τοπολογικός χώρος είναι τοπικά συμπαγής.*

2. $K = \mathbb{F}_q((\frac{1}{T}))$ το σώμα των τυπικών σειρών Laurent πάνω από το πεπερασμένο σώμα $\mathbb{F}_q$ με q στοιχεία.

   Ξεκινάμε με το $k = \mathbb{F}_q(T)$. Ορίζουμε $v(0) = \infty$ και αν $f(T) \in k^*$ τοτε

   $$f(T) = \left(\frac{1}{T}\right)^e \frac{P(T)}{Q(T)}, \quad P(0) \neq 0, \quad Q(0) \neq 0$$

   δηλαδή τα $P(T)$ και $Q(T)$ είναι σχετικά πρώτοι με το T. Έτσι ορίζουμε

   $$v(f) = e.$$

   Τότε το K είναι η πλήρωση του k ως προς τη $v(f)$.Η οποία επεκτείνεται συνεχώς στο K.(είναι συνηθέστερο να δουλεύει κανεις με το ισομορφικό του $\mathbb{F}_q((\frac{1}{T}))$ σώμα $\mathbb{F}_q((T))$). Η εκτίμηση αυτή μπορεί να επεκταθεί συνεχώς στο K. Γενικότερα μπορούμε να έχουμε μια εκτίμηση για κάθε ανάγωγο πολυώνυμο του $k = \mathbb{F}_q(T)$.

2.4 Επεκτάσεις

Ένα πλήρες σώμα K θα λέγεται *τοπικό σώμα* αν είναι τοπικά συμπαγές ως προς την τοπολογία που επάγεται από την v. Στην μη-αρχιμήδεια περίπτωση αυτό είναι το κίνητρο ώστε να κάνουμε την επιλογή του a όπως παραπάνω.

Άρα ο δακτύλιος των ακεραίων R είναι συμπαγής και το ιδεώδες M ανοικτό άρα το σώμα R/M είναι πεπερασμένο, έστω $|R/M| = q$. θέτουμε $a = \frac{1}{q}$ και λέμε ότι η σχετική απόλυτη τιμή είναι *κανονικοποιημένη*.

Άρα όποια πεπερασμένη επέκταση του K, L θα είναι τοπικά συμπαγές. Σε αυτή την περίπτωση έχουμε ότι όλες οι νόρμες του L πάνω από το K είναι ισοδύναμες. Άρα έχουμε το παρακάτω αποτέλεσμα.

Ορισμός 2.4.1. *Έστω L μια πεπερασμένη επέκταση του K. Μπορούμε να επεκτείνουμε την v στο L μοναδικά ως εξής, για $x \in L$ ορίζουμε*

$$v(x) = \frac{1}{[L:K]} v(a).$$

όπου $a = N_{L/K}(x)$ η νόρμα του x.

Ο λόγος που ορίσαμε έτσι την επέκταση της εκτίμησης στην αλγεβρική κλειστότητα του K, $\overline{K}$ έχει ως εξής: Έστω $\overline{K}$ να είναι η αλγεβρική κλειστότητα του K που περιέχει το L. Επίσης με v θα συμβολίζουμε μια επέκταση της v στο $\overline{K}$. Έστω σ ενας τυχαίος αυτομορφισμός του $\overline{K}$ πάνω από το K. Η απεικόνιση $x \to v(\sigma x)$ είναι και αυτή μια εκτίμηση η οποία επεκτείνει την v άρα οι $v(\sigma x)$ και $v(x)$ θα πρέπει να είναι ίσες. Έστω p^t ο βαθμός μη-διαχωρισημότητας της επέκτασης $L|K$. Τότε γνωρίζουμε ότι

$$a = N_{L/K}(x) = \prod \sigma(x)^{p^t}$$

Αυτή η επέκταση της $v(x)$ μας δίνει και μια επέκταση για το L το οποίο είναι πλήρες ως προς αυτή την εκτίμηση.

$$|x|_v = |a|_v^{\frac{1}{[L:K]}}$$

Ας υποθέσουμε οτι το είναι δακτύλιος διακριτής εκτίμησης, δηλαδή το $v(K)$ είναι διακριτό υποσύνολο του $\mathbb{R}$ (για παράδειγμα $v(\mathbb{Q}_p) = \mathbb{Z}$) και L μια πεπερασμένη επέκταση του K όπως από πάνω. Απο την κατασκευή του, το $v(L)$ είναι προσθετική υποομάδα του $\frac{1}{[L:K]} v(K)$. Υπάρχει λοιπόν κάποιος ακέραιος e ώστε $v(L) = \frac{1}{e} v(K)$. Ο ακέραιος αυτός καλείται δείκτης *διακλάδωσης* (ramification indext) της L/K.

Τα σώματα K που χρησιμοποιούνται είναι είτε πεπερασμένες επακτάσεις κάποιου από τα παραπάνω βασικά παραδείγματα ή η πλήρωση καποιας αλγεβρικής κλειστότητας $\overline{K}$ του K. Στην μη-αρχιμήδεια περίπτωση κάθε πεπερασμένη επέκταση είναι πλήρης, ωστόσο αυτό δεν ισχύει για την αλγεβρική κλειστότητα άρα σε αυτή την περίπτωση θα πρέπει να περάσουμε σε πλήρωση. Είναι επίσης δυνατό να δουλέψουμε στην $\overline{K}$ αν γνωρίζουμε ότι οι τελεστες μας στέλνουν ακολουθείες Cauchy που συγκλίνουν στο $\overline{K}$ σε ακολουθίες Cauchy που συγκλίνουν στο $\overline{K}$.

Πρόταση 2.4.2. *Έστω K ένα πλήρες σώμα με εκτίμηση v. Έστω $\overline{K}$ μια αλγεβρική κλειστότητα του μαζί με την κανονική επέκταση της v. Έστω $\hat{\overline{K}}$ η πλήρωση ως προς την v. Τότε το $\hat{\overline{K}}$ παραμένει αλγεβρικά κλειστό.*

Η πλήρωση της αλγεβρικής κλειστότητας του $\mathbb{Q}_p$ συνήθως συμβολίζεται με $\mathbb{C}_p = \hat{\overline{\mathbb{C}}}_p$ επειδή το σώμα αυτό παίζει, κατά μια έννοια, το ρόλο του $\mathbb{C}$. Το $\mathbb{C}_p$ δεν είναι σωμα

διακριτής εκτίμησης αφου $v(\mathbb{C}_p) = \mathbb{Q}$. Παρατηρούμε ότι σε αυτή την περίπτωση ο δακτύλιος των ακεραίων $\{x \in \mathbb{C}_p || x|_v \leq 1\}$ δεν είναι πλέον συμπαγής 'άρα το σώμα $\mathbb{C}_p$ δεν είναι με τη σειρά του τοπικά συμπαγές.

2.5 Σειρές

Έστω K σώμα, πλήρες ως προς μια εκτίμηση v. Αν $\sum_{j=0}^{\infty} a_j$ μια σειρά με συντελεστές από το K τότε ορίζουμε τη σύγκληση ή τη μη-σύγκληση της χρησιμοποιόντας όρια μερικών αθροισμάτων, ακριβώς όπως στην κλασική περίπτωση. Σε αντίθεση ομως με τη Αρχιμήδεια θεωρία εδώ έχουμε το εξής αποτέλεσμα.

Πρόταση 2.5.1. *Η $\sum_{j=0}^{\infty} a_j$ συγκλίνει σε ένα στοιχείο του K αν και μόνον αν $\lim_{j\to\infty} a_j = 0$*

Απόδειξη. Η κατεύθυνση μόνον αν είναι ίδια με την απόδειξη στην κλασική περίπτωση. Για την κατεύθυνση αν μπορούμε να δείξουμε ότι η ακολουθία των μερικών αθροισμάτων είναι Cauchy με την μη-αρχιμήδεια ιδιότητα. □

Έστω $f(x) = \sum a_n x^n$ μια δυναμοσειρά με συντελεστές από το K, το οποίο υποθέτουμε αλγεβρικά κλειστό και πλήρες. Έστω $\alpha \in K$, για να συγκλίνει η $f(x)$ στο α θα πρέπει να ισχύει ότι

$$\lim_{j\to\infty} a_j \alpha^j = 0$$

ή

$$\lim_{j\to\infty} v(a_j) + jv(\alpha) = \infty$$

ή, χρησιμοποιόντας την απόλυτη τιμή που προκύπτει από την εκτίμηση v μπορούμε να καταλήξουμε στην ποιο οικεία σχέση

$$\lim_{j\to\infty} |a_j|_v |\alpha|_v^j = 0.$$

Ορισμός 2.5.2. *Ορίζουμε $\rho(f)$ την τάξη σύγκλησης της δυναμοσειράς $f(x)$ ως*

$$\rho(f) = -\lim_{j\to\infty} \frac{v(a_j)}{j}$$

Η τάξη σύγκλισης αποτελεί το ανάλογο της ακτίνας σύγκλησης.
Άμεσα φαίνεται τώρα η παρακάτω πρόταση

Πρόταση 2.5.3. *Έστω $\alpha \in K$. Τότε η $f(x)$ συγκλίνει στο α αν $v(\alpha) > \rho(f)$ και αποκλίνει αν $v(a) < \rho(f)$*

Παρατήρηση 2.5.4. *Αν υποθέσουμε ότι το K είναι πλήρες αλλά όχι απαραίτητα αλγεβρικά κλειστό. Έστω $f(x) = \sum a_j x^j$ δυναμοσειρά με συντελεστές από το K , συμβολίζουμε το σύνολο αυτών των σειρών, ως συνήθως, με $K[[x]]$. Αν $a \in \overline{K}$ με $v(a) > \rho(f)$ και $L = K(a)$ τότε το $f(a)$ συγκλίνει σε ενα στοιχείο του L. Η κατάσταση αυτή θυμίζει την περίπτωση όπου το $f(x)$ είναι πολυώνυμο.*

Παράδειγμα 2.5.5. *Αν $f(x) = 1 + x + \cdots + x^n + \cdots$ τότε αφού $v(1) = 0$ έχουμε ότι $\rho(f) = 0$ άρα για $a \in K$ με $v(a) > 0$ η $1 + a + \cdots + a^n + \cdots$ συγκλίνει, και μάλιστα στο $1/(1-a)$*

2.6 Πολύγωνο του Newton

Ορισμός 2.6.1. *Έστω*

$$f(x) = \sum_{j=0}^{\infty} a_j x^j \in K[[x]]$$

Έστω $S = \{A_i\} \subset \mathbb{R}^2$, το σύνολο των σημείων $A_i = (i, v(a_i))$. Απο κάθε σημείο του S φέρουμε μια κάθετη ευθεία γραμμή και μετά θεωρούμε την κυρτή θήκη του συνόλου αυτού. Η κυρτή αυτή θήκη είναι φραγμένη από κάτω από μία πολυγωνική γραμμή με κορυφές κάποια από τα σημεία Ai. Η πολυγωνική αυτή γραμμή ορίζεται να είναι το πολύγωνο του Newton

Έστω $x \in K$, από τη σχέση $v(a_i x^i) = v(a_i) + iv(x)$ έχουμε ότι το σημείο A_i βρίσκεται πάνω στην ευθεία

$$Y + v(x)X = v(a_i x^i)$$

Πρόταση 2.6.2. *Έστω $\{m_i\}$ να είναι η ακολουθία των κλίσεων του πολυγώνου του Newton του $f(x) = \sum_{j=0}^{\infty} a_j x^j$. Τότε η $\{m_i\}$ είναι αύξουσα και $-\lim_{i\to\infty} m_i = \rho(f)$.*

Θα μελετήσουμε τις ρίζες του $f(x)$. Χωρίς βλάβη της γενικότητας μπορούμε να υποθέσουμε ότι $a_0 = 1$. Αυτό συμβαίνει επειδή το πολύγωνο του Newton του $\sum_{j=0}^{\infty} a_j/a_0 x^j$ είναι ίδιο με το πολυώνυμο του $f(x)$ μόνο που έχει μετακινηθεί στην κάθετη διεύθυνση κατά $-v(a_0)$. Ψάχνουμε τις ρίζες του $f(x) = 0$ στον κύκλο $v(x) = t$ Διακρίνουμε 2 περιπτώσεις:

1. Δεν υπάρχει καμία πλευρά του πολυγώνου Newton του $f(x)$ με κλήση $-t$. Τότε υπάρχει μόνο ένας μοναδικός όρος στο πολυώνυμο με την ελάχιστη εκτίμηση. Πράγματι, αν δεν ισχύει αυτό, δηλαδή υπάρχουν $i \neq j$ δείκτες με

   $$a = v(a_i x^i) = v(a_j x^j) = \inf_k \{v(a_k x^k)\}$$

   τότε όλα τα σημεία A_i βρίσκονται πάνω από την ευθεία $Y + tX = a$ και άρα η ευθεία από το A_i στο A_j είναι πλευρά του πολυγώνου Newton και έχει κλίση $-t$. Το οποίο είναι άτοπο άρα υπάρχει όντως μοναδικός όρος του αθροίσματος με την ελάχιστη εκτίμηση. $v(f(x)) = v(a_i x^i)$ για μοναδικό i και $v(x) = t$. Άρα δεν μπορεί να υπάρχει ρίζα του $f(x) = 0$ στον κύκλο $\{x \in K | v(x) = t\}$.

2. Έστω ότι υπάρχει πλευρά στο πολύγωνο του Newton από το σημείο A_i στο A_j για $i < j$ με κλήση $-t$. Από αυτά που είδαμε στην πρώτη περίπτωση έχουμε ότι υπάρχουν τουλάχιστον δύο όροι με την μικρότερη εκτίμηση αρά ενδέχεται να υπάρχει ρίζα της $f(x) = 0$ στον κύκλο $\{x \in K | v(x) = t\}$. Έστω $x_0 \in K$ με $v(x_0) = t$ και $c = v(a_i x_0^i) = v(a_j x_0^j)$. Θεωρούμε τη δυναμοσείρά

   $$f^*(u) = \sum b_e u^e = a_i^{-1} x_0^{-i} f(x_0 u).$$

   και έχουμε $v(b_i) = v(b_j) = 0$, $v(b_e) > 0$ για κάθε $e \neq i, j$ και $v(u) = 0$ όταν $v(x) = t$.

   Έστω R_K ο τοπικός δακτύλιος του K με $M_K \subset R_K$ το μεγιστικό του ιδεώδες. Έχουμε ότι το $f^*(u)$ είναι δυναμοσειρά με συντελεστες από το R_K και με $\overline{f^*}(u)$ συμβολίζουμε το υπόλοιπό του modulo M_K. Επίσης με $\overline{a}$ θα συμβολίζουμε το υπόλοιπο του $a \in R_K$ modulo .

Μπορούμε να έχουμε $v(b_e) = 0$ το πολύ για πεπερασμένα e, αρα, χωρίς βλάβη της γενικότητας, μπορούμε να υποθέσουμε ότι $v(b_e) > 0$ για $e < i$ και $e > j$ άρα έχουμε ότι

$$\begin{aligned}\overline{f^*}(u) &= u^j + \cdots + \overline{b_i}u^i \\ &= u^i(u^{j-i} + \cdots + \overline{b}_i)\end{aligned}$$

όπου $\overline{b}_i \neq 0$ άρα τα u^i και $u^{j-i} + \cdots + \overline{b}_i$

Θεώρημα 2.6.3. *Hensel's lemma Έστω πλήρες υπερμετρικό σώμα και έστω $P = \sum a_i x^i$ ένα πολυώνυμο με στοιχεία από το R_K. Έστω ότι υπάρχουν 2 πολυώνυμα q και r με συντελεστές από το σώμα των υπολοίπων R_K/M_K και σχετικά πρώτα. Για τα πολυώνυμα αυτά επίσης να ισχύει $\overline{P} = \sum \overline{a}_i x^i = qr$. Τότε υπάρχουν δυο πολυώνυμα Q και R με συντελεστές από το R_K τέτοια ώστε $P = QR$, $\overline{Q} = q$, $\overline{R} = r$, $\deg(Q) = \deg(q)$*

Παρατήρηση 2.6.4. *(α΄) Η υπόθεση ότι τα πολυώνυμα είναι σχετικά πρώτα δεν μπορεί να παραληφθεί. Για παράδειγμα για το πολυώνυμο $P(x) = x^2 + p \in \mathbb{Z}_p[x]$ ισχύει $\overline{P}(x) = xx$ και το $\overline{P}(x)$ είναι ανάγωγο.*

(β΄) Υπάρχουν και άλλες εκδοχές του λήμματος (για αναλυτικές συναρτήσεις, διαφορικους τελεστές...). Όλες αυτές συμπεραίνουν πως αν ισχύει κάποια συνθήκη (οπως στην περίπτωσή μας τα πολυώνυμα να είναι σχετικά πρώτα) τότε μία «διάσπαση» στο σώμα των υπολοίπων είναι «ολοκληρωτική διάσπαση».

(γ΄) Αν το πολυώνυμο q είναι βαθμού ένα τότε το λήμμα γίνεται: Έστω K να είναι ένα πλήρες υπερμετρικό σώμα και $P(x)$ ένα πολυώνυμο με συντελεστές από το R_K. Έστω a μια απλή ρίζα του $\overline{P}$ (δηλαδή είναι πολλαπλότητας ένα, $\overline{P}(a) = 0$ και $\overline{P}'(a) \neq 0$). Τότε υπάρχει μια ρίζα του $P(x) = 0$, $\alpha \in R_K$ τέτοια ώστε $\overline{a} = \alpha$

Άρα από την παραπάνω συχήτηση και το λήμμα του Hensel έχουμε ότι υπάρχει πολυώνυμο $g(u)$ βαθμού $j - i$ και δυναμοσειρά $h(u) \in R_K[[u]]$ ώστε

$$\overline{g}(u) = u^{j-i} + \cdots + \overline{b}_i$$

$$\overline{h}(u) = u^i$$

και

$$f^*(u) = h(ug(u))$$

Η $h(u)$ συγκλίνει για $v(u) \leq 0$ και $h(u) \neq 0$ όταν $v(u) = 0$. Αν $g(u) = \sum_{m=0}^{j-i} g_m u^m$. Τότε $g_0 \equiv \overline{b}_i \not\equiv 0 mod M_K$. Αφού το K είναι αλγεβρικά κλειστό, το $g(u)$ αναλύεται πλήρως στο K. Αφού $v(g_0) = 0$ τότε όλες οι ρίζες του $g(u)$, a θα πρέπει να έχουν την ίδια εκτίμηση $v(a) = 0$. Αυτό σημαίνει ότι η $f(x) = 0$ έχει ακριβώς $j - 1$ ρίζες στον κύκλο $\{x | v(x) = t\}$ όπου $j - 1$ είναι η προβολή στον $x-$ άξονα της πλευράς του πολυγώνου Newton με κλίση $-t$.

Συνοψήζοντας τα παραπάνω έχουμε το ακόλουθο αποτέλεσμα:

Πρόταση 2.6.5. *1. Αν δεν υπάρχει πλευρά του πολυγώνου του Newton του $f(x)$ με κλήση $-t$ ($t > \rho(f)$), τότε δεν υπάρχουν ρίζες της $f(x) = 0$ πάνω στον κύκλο $\{x \in K | v(x) = t\}$.*

2. *αν υπάρχει πλευρά του πολυγώνου με κλήση $-t$ τότε το $f(x) = 0$ έχει ακριβώς τόσες ρίζες στον κύκλο $\{x \in K | v(x) = t\}$ όσο είναι το μήκος της προβολής της πλευράς του πολυγώνου με κλίση $-t$ στον X-άξονα.*

Παράδειγμα 2.6.6. *Για παράδειγμα έστω ότι το $f(x)$ είναι πολυώνυμο του Eisenstein βαθμού n, $f(x) = \sum_{i=0}^{n} a_i x^i$. Τότε $v(a_o) = 1, v(a_i) > 0$ για $0 < i < n$ και $v(a_n) = 0$. Σε αυτή την περίπτωση βλέπουμε ότι το πολύγωνο του Newton είναι μια ευθεία γραμμή από το σημείο $(0, 1)$ στο $(d, 0)$ και άρα το $f(x)$ έχει d ρίζες γ τέτοιες ώστε $v(\gamma) = \frac{1}{d}$*

Παρατήρηση 2.6.7.

1. *Το πολύγωνο του Newton που αντιστοιχεί σε ένα ανάγωγο πολυώνυμο του $K(x)$ αποτελείται από μια μόνο πλευρά.*

2. *Αν το $f(x)$ είναι δυναμοσειρά και r είναι μία ρίζα της $f(x) = 0$ με $v(r) > \rho(f)$ τότε*
$$\frac{f(x)}{(x-r)} \in K[[x]]$$
και
$$\rho(f(x)) = \rho\left(\frac{f(x)}{(x-r)}\right).$$

3. *Αν το $f(x)$ έχει συντελεστές σε ένα πλήρες σώμα L και K είναι η πλήρωση της αλγεβρικής κλειστότητας του L τότε από τα παραπάνω έχουμε ότι οι ρίζες του $f(x)$ είναι αλγεβρικές πάνω από το L το οποίο θυμίζει τη θεωρία των πολυωνύμων.*

4. *Έστω ότι το K είναι χαρακτηριστικής $p > 0$ και ότι, όπως πριν, το K είναι η πλήρωση της αλγεβρικής κλειστότητας του L. Έστω $L^{\text{sep}} \subset K$ να είναι η διαχωρίσιμη κλειστότητα του L (η L^{sep} είναι η μέγιστη επέκταση Galois του L). Τότε το K είναι πλήρωση και του L^{sep}. Άρα μπορούμε να υποθέσουμε ότι το x_0 είναι αλγεβρικό και μάλιστα διαχωρίσιμο πάνω από το L. Αν το $f(x)$ είναι της μορφης $\sum a_i x^{p^i}$ με συντελεστές από το L και $a_0 \neq 0$ τότε όλες οι ρίζες του είναι στο L^{sep} αφού $f'(x) \equiv a_0 \neq 0$. Με αυτή την παρατήρηση και την επιλογή του x_0 η παραπάνω συζήτηση μας δίνει διαχωρίσιμες ρίζες για το $f(x)$.*

5. *Αν η $f(x) = 0$ δεν έχει ρίζες στο $\{x \in K | v(x) \geq t\}$, $(t > \rho(f))$.Τότε $f(0) \neq 0$ και μπορούμε να κατασκευάσουμε τη δυναμοσειρά $\frac{1}{f(x)}$ η οποία συγκλίνει για $v(x) > t$.*

Έστω $t > \rho(f)$

Πρόταση 2.6.8. *Υπάρχει μόνο πεπερασμένο πλήθος ριζών του $f(x)$ στο δίσκο $\{x \in K | v(x) \geq t\}$.*

Απόδειξη. Έστω $t_1 > \rho(f)$. Από τα προηγούμενα έχουμε οτι η $f(x) = 0$ θα έχει ρίζες στον κύκλο $\{x \in K | v(x) = t_1\}$ αν και μόνο αν υπάρχει πλευρά του πολυγώνου του Newton με κλήση $-t_1$. Αν $\{m_i\}$ είναι, όπως πριν, η ακολουθία των κλήσεων των πλευρών τότε
$$-\lim m_i = \rho(f)$$
Άρα υπάρχουν μόνο πεπερασμένο πλήθος πλευρών του πολυγώνου του Newton με κλήση $L < -t$ απ όπου παίρνουμε και το αποτέλεσμα. □

Ορισμός 2.6.9. *Έστω $f(x) = \sum_{i=0}^{\infty} a_i x^i$. Η $f(x)$ θα λέγεται entire αν και μόνο αν $\rho(f) = -\infty$, δηλαδή αν η $f(x)$ συγκλίνει για κάθε x.*

Πρόταση 2.6.10. *Μια entire συνάρτηση $f(x)$ χωρίς ρίζες είναι σταθερή.*

Το ακόλουθο θεώρημα είναι μια γενίκευση του κλασικού θεωρήματος παραγοντοποίησης του Weierstrass

Θεώρημα 2.6.11. *Έστω $f(x)$ να είναι μια entire συνάρτηση και έστω $\{\lambda_1, \dots, \lambda_t, \dots\}$ να είναι οι μη-μηδενικές ρίζες του στο K (το οποίο είναι πλήρες και αλγεβρικά κλειστό). Τότε*

$$-\infty = \lim_t v(\lambda_t)$$

και

$$f(x) = cx^n \prod_t (1 - \frac{x}{\lambda_t}), \quad n = \text{ord}_{x=0} f(x)$$

για κάποια σταθερά c. Αντίστροφα αν τα $\{\lambda_t\}$ είναι όπως πάνω τότε το γινόμενο αυτό ορίζει μια entire συνάρτηση.

Κεφάλαιο 3

Carlitz Module

3.1 Εισαγωγικά

Ορίζουμε $\mathbf{A} = \mathbb{F}_q[T]$, $q = p^m$ και $k = \mathbb{F}_q(T)$. Έστω $v_\infty : k \to \mathbb{R} \cup \{\infty\}$ να είναι η σχετική με το $1/T$ εκτίμηση, δηλαδή $v_{\infty(1/T)} = 1$. Η πλήρωση του k ως προς αυτή την εκτίμηση θα συμβολίζεται με K. Το σώμα K είναι επομένως πλήρες και τοπικά συμπαγές με την τοπολογία που ενάγεται από την εκτίμηση.

Πρόταση 3.1.1. *Ο δακτύλιος* $\mathbf{A}$ *είναι διακριτός υποδακτύλιος του* K *και το* $K/\mathbf{A}$ *είναι συμπαγές.*

Αν παρατηρήσουμε ότι

- το $\mathbf{A}$ και το $\mathbb{Z}$ έχουν αλγορίθμους διαίρεσης
- το $\mathbb{Z}$ είναι διακριτό μέσα στο $\mathbb{R} = \mathbb{Q}_\infty$ και επιπλέον το $\mathbb{R}/\mathbb{Z} \equiv S^1$ είναι συμπαγές.

τότε βλέπουμε την εξής αναλογία

$$\mathbf{A} \sim \mathbb{Z} \quad k \sim \mathbb{Q} \quad K \sim \mathbb{R}$$

Με $\overline{K}$ θα συμβολίζουμε την αλγεβρική κλειστότητα του με την κανονική επέκταση της v_∞. Θα σκεφτόμαστε το $\overline{K}$ ως ανάλογο του $\mathbb{C}$. Το $\overline{K}$ δεν είναι ούτε συμπαγές ούτε πλήρες, με $\mathbf{C}_\infty$ θα συμβολίζουμε την πλήρωση του $\overline{K}$. Απο αποτέλεσμα της προηγούμενης παραγράφου έχουμε οτι η πλήρωση είναι και αλγεβρικά κλειστή.

Ορίζουμε $d \geq 0$ και $\mathbf{A}(d) = \{a \in \mathbf{A} | \deg(a) < d\}$ δηλαδή $\mathbf{A}$ είναι $\mathbb{F}_r$-δανυσματικός χώρος διάστασης d. Προφανώς έχουμε ότι

$$\mathbf{A} = \bigcup \mathbf{A}(d)$$

Ορισμός 3.1.2. *θέτουμε* $e_0(x) = x$ *και για* $d > 0$

$$e_d(x) := \prod_{a \in \mathbf{A}(d)} (x - a) = \prod_{a \in \mathbf{A}(d)} (x + a)$$

Από αποτέλεσμα του 1ου κεφαλαίου έχουμε ότι το $e_d(x)$ είναι $\mathbb{F}_q$-γραμμικό. Άρα $e_d(\tau) \in \mathbf{A}\{\tau\}$

Ορισμός 3.1.3. (i) *Έστω $i > 0$ ορίζουμε*

$$[i] = T^{q^i} - T \in \mathbf{A}$$

(ii) *Ορίζουμε $D_0 = 1$ και για $i > 0$*

$$D_i = [i][i-1]^q \dots [1]^{q^{i-1}}$$

(iii) *Ορίζουμε $L_0 = 1$ και για $i > 0$*

$$L_i = [i][i-1] \dots [1]$$

παρατηρούμε ότι

$$\deg[i] = q^i, \quad \deg D_i = iq^i, \quad \deg L_i = q\frac{q^i - 1}{q-1}$$

και οι εκτιμήσεις τους στο άπειρο είναι οι αρνητικοί των αριθμών αυτών.

Θεώρημα 3.1.4 (Carlitz)**.**

$$e_d(x) = \prod_{a \in \mathbf{A}(d)} (x + a) = \sum_{i=0}^{d} (-1)^{d-i} x^{q^i} \frac{D_d}{D_i L_{d-i}^{q^i}}$$

Από τη σχέση αυτή έχουμε ότι οι συντελεστές $D_d/D_i L_{d-i}^{q^i}$ ανήκουν στο $\mathbf{A}$, (είναι ακέραιοι). Όπως θα φανεί και από την παρακάτω πρόταση τα D_i και L_i εχουν παρόμοια συμπεριφορά με το παραγοντικό. Ακολουθόντας αυτη την φιλοσοφία μερικές φορες συμβολίζουμε τους συντελεστές με $\binom{d}{i}$ ή $\binom{d}{i}_A$.

Πρόταση 3.1.5. (i)

$$[i] = \prod_{\deg f | i} f$$

οπου κάθε f είναι μονικό και πρώτο.

(ii)

$$D_i = [i] D_{i-1}^q$$

(iii)

$$D_i = \prod_{\deg g = i} g$$

και κάθε g είναι μονικό

(iv) *L_i είναι το ελάχιστο κοινό πολλαπλάσιο όλων των πολυωνύμων βαθμού i.*

Απόδειξη. (i) Αφού δουλεύουμε σε χαρακτηριστική p

$$\frac{d}{dT}[i] = -1$$

άρα το πολυώνυμο $[i]$ είναι διαχωρίσιμο και το ζητούμενο είναι άμεσο.

(ii) άμεσο από τον ορισμό.

(iii) άμεσο από το πόσες φορές διαιρεί ένα πολυώνυμο το γινόμενο όλων των μονικών πολυωνύμων βαθμού i.

(iv) όμοια με πάνω αλλά για το ελάχιστο κοινό πολλαπλάσιο.

□

Πόρισμα 3.1.6. *Για κάθε μονικό πολυώνυμο h βαθμού d έχουμε ότι $e_d(h) = D_d$*

Απόδειξη. Κάθε μονικό h βαθμού d μπορεί να γραφτεί ως $g = h + a$ με $dega < d$ και το ζητούμενο έπεται από το 3 της από πάνω πρότασης. □

3.2 Εκθετική συνάρτηση

Εύκολα έχουμε ότι

$$\prod_{0\neq a\in\mathbf{A}(d)} a = (-1)^d \frac{D_d}{L_d}$$

.

Αν διαιρέσουμε τον τύπο του Carlitz 3.1.4 με $\prod_{0\neq a\in\mathbf{A}(d)} a$ παίρνουμε

$$x \prod_{0\neq a\in\mathbf{A}(d)} \left(1+\frac{x}{a}\right) = \sum_{j=0}^{d} (-1)^j \frac{x^{q^j}}{D_j} \frac{L_d}{L_{d-j}^{q^j}}$$

Θέτουμε

$$\xi_d = \frac{[1]^{\frac{q^d-1}{q-1}}}{L_d}$$

Λήμμα 3.2.1.

$$\xi_d = \prod_{j=1}^{d-1} \left(1 - \frac{[j]}{[j+1]}\right)$$

Άρα η ακολουθία $\{\xi_d\}_{d=1}^{\infty}$ έχει όριο στο K το ξ_*. Για το οποίο έχουμε ότι

$$\xi_* = \prod_{j=1}^{\infty} \left(1 - \frac{[j]}{[j+1]}\right)$$

.

Βλέπουμε ότι το ξ_* είναι 1-αντιστρέψιμο (1-unit) στο K. (είναι αντιστρέψιμο στον $R_K = \{x \in K | v_\infty(x) \geq 0\}$ και ισοδύναμο με το 1 modulo το μέγιστο ιδεώδες $M_K = \{x \in K | v_\infty(x) > 0\}$). Για την ακρίβεια έχει εκτίμηση μηδέν, $v_\infty(\xi_*) = 0$.

Λήμμα 3.2.2. (i) $v_\infty(\xi_{d+1} - \xi_d) = q^d(q-1)$

(ii) *Θέτουμε $\delta_d = \xi_d - \xi_*$ τότε*

$$v_\infty(\delta_d) = q^d(q-1).$$

Αν θέσουμε $\beta_j = [1]^{\frac{q^j-1}{q-1}}$ τότε $\xi_d = \frac{\beta_d}{L_d}$.

Λήμμα 3.2.3.

$$\frac{L_d}{L_{d-j}^{q^j}} = \frac{\beta_j \xi_{d-j}^{q^j}}{\xi_d}$$

Από το παραπάνω λήμμα έχουμε ότι

$$x\prod_{0\neq a\in\mathbf{A}(d)}(1+\frac{x}{a})=\frac{1}{\xi_d}\sum_{j=0}^{d}(-1)^j\frac{x^{r^j}}{D_j}\beta_j\xi_{d-j}^{q^j}$$

χρησημοποιόντας τη σχέση $\delta_j=\xi_j-\xi_*$ παίρνουμε ότι

$$x\prod_{0\neq a\in\mathbf{A}(d)}(1+\frac{x}{a})=\frac{1}{\xi_d}\sum_{j=0}^{d}(-1)^j\frac{x^{q^j}}{D_j}\beta_j(\delta_{d-j}^{q^j}+\xi_*^{q^j})$$

Λήμμα 3.2.4. *Για κάθε $x\in\mathbf{C}_\infty$ αν $d\to\infty$ το*

$$\sum_{j=0}^{d}(-1)^j\frac{x^{q^j}}{D_j}\beta_j\delta_{d-j}^{q^j}\to 0$$

στο $\mathbf{C}_\infty$

Λήμμα 3.2.5. *Για κάθε $x\in\mathbf{C}_\infty$ η σειρά*

$$\sum_{j=0}^{d}(-1)^j\frac{x^{q^j}}{D_j}\beta_j\xi_*^{q^j}$$

συγκλίνει στο $\mathbf{C}_\infty$.

Πόρισμα 3.2.6. *Έστω $x\in\mathbf{C}_\infty$, τότε*

$$x\prod_{0\neq a\in\mathbf{A}(d)}(1+\frac{x}{a})=\frac{1}{\xi_d}\sum_{j=0}^{d}(-1)^j\frac{x^{q^j}}{D_j}\beta_j\xi_*^{q^j}$$

Απόδειξη. Άμεσο από τα 2 πάνω λήμματα και τη σχέση που δόθηκε πριν από αυτά. □

Ορισμός 3.2.7. (i) *Έστω λ να είναι μια οποιαδήποτε $(q-1)$-οστή ρίζα του $-[1]$ στο $\overline{K}$. Τότε θέτουμε*

$$\xi:=\xi_C=\lambda\xi_*$$

(ii) *Έστω $x\in\mathbf{C}_\infty$. Τότε ορίζουμε*

$$e_c(x)=\sum_{j=0}^{\infty}\frac{x^{q^j}}{D_j}\tag{3.1}$$

Η οποία συγκλίνει σε στοιχείο του $\mathbf{C}_\infty$. Η συνάρτηση $e_c(x)$ καλείται η εκθετική συνάρτηση του Carlitz.

Παρατήρηση 3.2.8. *Αν θυμηθούμε ότι $D_i=\prod g, monic, \deg g=ig$ τότε εύκολα δικαιολογείται η ονομασία εκθετική για την* 3.1 *καθώς*

$$e^x=\sum_{n=0}^{\infty}\frac{x^n}{n!}$$

μονο που η 3.1 *έχει μονώνυμα τη μορφής x^{q^i}*

Συνοψιζοντας τα προηγούμενα

Θεώρημα 3.2.9. *Έστω $x \in \mathbf{C}_\infty$. Τότε*

$$x \prod_{0 \neq a \in \mathbf{A}(d)} \left(1 - \frac{x}{a}\right) = \frac{1}{\xi} \sum \frac{(\xi x)^{q^j}}{D_j} = \frac{1}{\xi} e_c(\xi x)$$

Πόρισμα 3.2.10. *Αν $L = \xi\mathbf{A} \in \overline{K}$. Τότε για όλα τα $x \in \mathbf{C}_\infty$, έχουμε*

$$x \prod_{0 \neq a \in L} \left(1 - \frac{x}{a}\right) = e_C(x)$$

Απόδειξη. Αν αντικαταστήσουμε το x με x/ξ στο θεώρημα 3.2.9 παίρνουμε την

$$\frac{1}{\xi} e_c(x) = \frac{x}{\xi} \prod_{0 \neq a \in L} \left(1 - \frac{x}{a}\right).$$

□

Παρατήρηση 3.2.11. (i) *Παρατηρούμε ότι η παραγοντοποίηση που πετυχαίνει το πάνω πόρισμα είναι αυτή που μας δίνει το θεώρημα 2.6.11*

(ii) *Έστω $0 \neq a \in L$, $a \in L = \xi\mathbf{A}$. Αφού $\xi_* \in K$ βλέπουμε ότι*

$$K(a) = K(\lambda)$$

και το $K(\lambda)$ είναι διαχωρίσιμη πάνω από το K.

(iii) *Από το διωνυμικό θεώρημα μπορούμε να επιλέξουμε μια $(q-1)$-οστή ρίζα θ του $1 - T^{1-q}$ στο K που είναι '1-unit'. Εύκολα βλέπουμε ότι είναι και μοναδική. Αν θέσουμε*

$$\xi_u = \theta \xi_*$$

το στοιχείο είναι '1-unit'. Άρα

$$\xi = \sqrt[q-1]{-T^q}\, \xi_u$$

(iv) *Το στοιχείο ξ έχει δειχθεί ότι είναι υπερβατικό πάνω απο τον k, [14].*

3.3 Carlitz Module

Θα χρησιμοποιήσουμε την εκθετική $e_C(x)$ για να περιγράψουμε μια νέα δράση του $\mathbf{A} = \mathbb{F}_q[T]$ στο C_∞. Η νέα δράση αυτή θα λέγεται Carlitz module και αποτελεί το πιο απλό παράδειγμα Drinfeld module.

Πρόταση 3.3.1. *Έστω $x \in C\infty$, τότε*

$$e_c(Tx) = Te_c(x) + e_c(x)^q$$

Απόδειξη. Έχουμε ότι

$$e_C(x) = \sum_{i=0}^{\infty} \frac{x^{q^i}}{D_i}$$

Άρα

$$e_C(Tx) = \sum_{i=0}^{\infty} T^{q^i} \frac{x^{q^i}}{D_i}$$

και

$$e_C(Tx) - Te_C(x) = \sum_{i=0}^{\infty} (T^{q^i} - T)\frac{x^{q^i}}{D_i}.$$

Όμως, γνωρίζουμε ότι $D_i = (T^{q^i} - T)D_{i-1}^q$, άρα

$$e_C(Tx) - Te_C(x) = \sum_{i=1}^{\infty} \frac{x^{q^i}}{D_{i-1}^q} = \left(\sum_{i-1}^{\infty} \frac{x^{q^i}}{D_i}\right)^q$$

□

Θεωρούμε το $a \in \mathbf{A}$ με $a = \sum_{j=0}^{d} a_j T^j$, όπου κάθε $a_j \in \mathbb{F}_q$ και $a_d \neq 0$.

Πόρισμα 3.3.2. *Εστω $x \in C_\infty$ τότε*

$$e_c(ax) = ae_c(x) + \sum_{j=1}^{d} C_a^{(j)} e_c(x)^{q^j}$$

όπου για κάθε j, $C_a^{(j)} \in \mathbf{A}$ κατάλληλοι συντελεστές και $C_a^{(d)} = a_d$.

Απόδειξη. Παρατησούμε ότι για $i \geq 1$

$$e_C(T^i x) = e_C(T(T^{i-1}x))$$

και άρα μπορούμε να υπολογίσουμε τους συντελεστές $C_{T^j}^{(j)}$ με επαγωγή. Για παράδειγμα

$$\begin{aligned} e_C(T^2x) &= Te_C(Tx) + e_C(Tx)^q \\ &= T(Te_C(x) + e_C(x)^q) + (Te_C(x) + e_C(x)^q)^q \\ &= T^2 e_c(x) + (T^q + T)e_C^q(x) + e_C(x)^{q^2} \end{aligned}$$

Οι συντελεστές του $e_C(ax)$ μπορούν επομένως να υπολογιστούν από την $\mathbb{F}_q-$γραμμικότητα και το ζητούμενο έπεται άμεσα.

□

Ορισμός 3.3.3. *Εστω $C_a^{(j)}$ όπως στο πάνω πόρισμα, τότε θέτουμε*

$$C_a(\tau) = a\tau^0 + \sum_{j=1}^{d} C_a^{(j)} \tau^j$$

με $d = \deg a$.

Έχουμε έτσι τη βασική σχέση για το $e_c(x)$

$$e_C(ax) = C_a(e_C(x))$$

Θεώρημα 3.3.4. *Η απεικόνιση από το $\mathbf{A}$ στο $k\{\tau\}$, $a \mapsto C_a$ είναι μονομορφισμός $\mathbb{F}_q -$ αλγεβρών.*

Απόδειξη. Είναι άμεσο ότι η απεικόνιση $a \mapsto C_a$ είναι $\mathbb{F}_q -$ γραμμική. Το μόνο που μένει να δείξουμε είναι ότι σέβεται τη δομή της άλγεβρας, δηλαδή για κάθε $a, b \in \mathbf{A}$

$$C_{ab} = C_a C_b$$

όπου εννοούμε τον πολλαπλασιασμό των προσθετικών πολυωνύμων. Επίσης από τα παραπάνω έχουμε

$$C_{ab}(e_C(x)) = e_C(abx) = e_C(a(bx)) = C_a(e_C(bx) = C_a(C_b(e_C(x))))$$

από το οποίο έπεται το αποτέλεσμα. □

Ορισμός 3.3.5. *Ονομάζουμε την απεικόνισης* $\mathbf{A} \mapsto k\{\tau\}$, $a \mapsto C_a$, ***Carlitz module****, και το συμβολίζουμε με* C.

Παρατήρηση 3.3.6. (i) $C_a \in \mathbf{A}\{\tau\}$ *για κάθε* $a \in \mathbf{A}$

(ii) *από το θεώρημα 2.6.11 ξέρουμε ότι κάθε μη-σταθερή entire συνάρτηση είναι επί. Αν* $L = \mathbf{A}\xi$ *είναι οι ρίζεις του* $e_c(x)$ *έχουμε έναν ισομορφισμό*

$$C_\infty / L \to C_\infty$$

μέσω του $e_C(x)$. *Η ομάδα* C_∞ / L *είναι ένα* $\mathbf{A} -$ *module άρα μπορούμε να θεωρήσουμε νέα* $\mathbf{A} -$ *δράση sto* C_∞ *μέσω του ισομορφισμού αυτού. Αυτή η δράση είναι το Carlitz module.*

(iii) *Από την αναλογία με την εκθετική συνάρτηση που αναφέραμε στην προηγούμενη παράγραφο έχουμε ότι το Carlitz module είναι ένα* $\mathbf{A} -$ *ανάλογο της πολλαπλασιαστικής ομάδας* $\mathbb{G}_m$ *με τη συνήθη* $\mathbb{Z} -$ *δράση*

Ορισμός 3.3.7. *Τα* ***division values*** *(ή division points) του Calitz module ορίζεται να είναι τα* $\{e_c(a\xi) | a \in k\} \subset C_\infty$.

Αν $a = b/f \in k$, $b, f \in \mathbf{A}$ με $f \neq 0$. Τότε $e_C(a\xi)$ είναι ρίζα του $C_f(x) = 0$ άρα ανήκει στην αλγεβρική κλειστότητα του k στο C_∞. Στο παρακάτω αποτέλεσμα φαίνεται άμεσα η αναλογία με τα κυκλοτομικά σώματα

Πρόταση 3.3.8. *Έστω* $L \subset C_\infty$ *μια επέκταση του* k. *Έστω* $a \in k$ *και*

$$L_1 = L(e_C(a\xi))$$

Τότε η L_1 *είναι αβελιανή επέκταση της* L.

Απόδειξη. Αν $a = b/f$ ένα ανάγωγο κλάσμα , τότε

$$e_C(\frac{b}{f}\xi) = C_b(e_C(\xi/f))$$

άρα $L_1 \subset L(e_C(\xi/f))$, άρα μπορούμε να υποθέσουμε ότι $L_1 = L(e_C(\xi/f))$. Θέτουμε $\rho = e_C(\xi/f)$. Αφού όλοι οι συντελεστές του $C_g(\tau)$ ανήκουν στο g για κάθε g βλέπουμε ότι το L_1 περιέχει όλα τα division values,

$$e_C(\frac{g}{f}\xi),$$

το L_1 περιέχει όλα τα f-division points. Ως $\mathbf{A} -$ module η εκθετική του Carlitz μας δίνει ότι το $\mathbf{A} -$ module των $f -$ division points είναι ισόμορφο με το $\mathbf{A}/(f)$.

Αφού το L_1 περιέχει όλα τα $\mathbf{A}/(f)$ βλέπουμε ότι είναι Galois πάνω από το L. Έστω ότι το G είναι η ομάδα Galois. Αφού $C_g(\tau) \in \mathbf{A}\{\tau\}$ για κάθε g βλέπουμε ότι η δράση της G στα $(f)-$division points μετατίθεται με τη δράση του $\mathbf{A}$. Άρα για $\sigma \in G$ και η $\sigma(\rho)$ είναι $\mathbf{A}-$module γεννήτορας των $(f)-$division points. Άρα παίρνουμε μια 1-1 απεικόνιση $G \mapsto \mathbf{A}/(f)^*$. □

Ορισμός 3.3.9. *Έστω $g \in \mathbf{A}$. θέτουμε*

$$C[g] := \left\{ e_C\left(\frac{b}{g}\xi\right) | b \in \mathbf{A} \right\} \subset C_\infty$$

και το ονομάζουμε module των division points. Είναι $\mathbf{A}-$module ισομορφικό με το $\mathbf{A}/(g)$. Ένας γεννήτορας του $C[g]$ ως $\mathbf{A}-$module θα λέγεται primitive g-th division point.

Έχουμε δει ότι ως $\mathbf{A}-$module, $C[g] \simeq \mathbf{A}/(g)$. Επίσης αν $\zeta \in \mathbb{F}_q^*$ τότε

$$C[g] = C[\zeta g]$$

Επομένως το $C[g]$ εξαρτάται μόνο από το ιδεώδες του $\mathbf{A}$ που παράγεται από το g. Επομένως για ένα ιδεώδες του $\mathbf{A}$, I ορίζουμε

$$C[I] := C[i]$$

όπου i γεννήτορας του I.

Η παράγραφος αυτή κλείνει με έναν τύπο για τους συντελεστές $C_a^{(j)}$ του $C_a(\tau)$.

Έστω $a \in \mathbf{A}$,

$$C_a(\tau) = a\tau^0 + \sum_{j=1}^{d} C_a^{(j)} \tau^j$$

για λόγους απλότητας θέτουμε $a_j := C_a^{(j)}$

Πρόταση 3.3.10. *Έστω $a, a_j \ldots$ όπως πριν τότε έχουμε*

$$a_1 = \frac{a^q - a}{T^q - T}$$

$$\vdots$$

$$a_i = \frac{a_{i-1}^q - a_{i-1}}{T^{q^i} - T}$$

Επιπλέον αν $a = \zeta f$ για $\zeta \in \mathbb{F}_q^*$ και το f είναι μονικό βαθμού d τότε $a_d = \zeta$.

Απόδειξη. Γράφουμε το $C_a = a\tau^0 + \chi_a$ όπου $\chi_a \in \mathbf{A}\{\tau\}$. Άρα $\chi_T = \tau$. Αφού $C_a C_T = C_T C_a$ στο $k\{\tau\}$ έχουμε

$$(a\tau^0 + \chi_a)C_T = C_T(a\tau^0 + \chi_a),$$

ή

$$C_T a\tau^0 - a\tau^0 C_T = \chi_a C_T - C_T \chi_a. \tag{3.2}$$

Το ζητούμενο έπεται αν εξισώσουμε τους συντελεστές του τ^j στα δύο μέλη της παραπάνω εξίσωσης. □

Παρατήρηση 3.3.11. (i) *Αν* $a_d = \zeta$ *τότε* $a_{d+1} = a_{d+2} = a_{d+3} = .. = 0$.

(ii) $a_i \neq 0$ *για* $i = 1, ..., d$.

(iii) *Αν* $v, u \in k\{\tau\}$ *θέτουμε*

$$[v, u] = uv - vu$$

τον μεταθέτη των u *και* v. *Η απεικόνιση* $v \mapsto [u, v]$ *είναι παραγώγιση στο* $k\{\tau\}$. *Επίσης η εξίσωση 3.2 μπορεί να γραφτεί ως*

$$[C_T, a\tau^0] = -[C_T, \chi_a].$$

3.4 Λογάριθμος

Απο τις προηγούμενες παραγράφους έχουμε

$$e_C(x) = \sum_{i=0}^{\infty} \frac{x^{q^i}}{D_i}$$

και $D_0 = 1$, άρα $e'_C(x)$ είναι ταυτοτικά 1. Επομένως μπορούμε να ορίζουμε αντίστροφη της $e_C(x)$ περί το μηδέν με μη τετριμμένη ακτίνα συγκλισης. Ονομάζουμε αυτή την συνάρτηση $\log_C(x)$. Είναι $\mathbf{F}_q -$ γραμμική αφού η $e_C(x)$ είναι $\mathbb{F}_q$-γραμμική. Για τις $e_C(x)$ και $\log_C(x)$, ως τυπικές δυναμοσειρές, έχουμε

$$e_C(\log_C(x)) = \log_C(e_C(x)) = x$$

.

Αφού για την $e_C(x)$ ισχύει η εξίσωση

$$e_c(Tx) = Te_C(x) + e_C(x)^q$$

Τότε:

$$\log_c(e_C(Tx)) = Tx = \log_C(Te_C(x)) + \log_C(e_C(x)^q).$$

Άρα αντικαθιστόντας το x με $\log_C(x)$ για την $\log_C(x)$ έχουμε:

$$T\log_C(x) = \log_C(Tx) + \log_C(x^q).$$

Αφού $\log'_C$ είναι επίσης ταυτοτικά 1 έχουμε

$$\begin{aligned}\log_C(x) &= x + \frac{x^q}{-[1]} + \frac{x^{q^2}}{[1][2]} + \frac{x^{q^3}}{-[1][2][3]} + ... \\ &= \sum_{i=0}^{\infty} (-1)^i \frac{x^{q^i}}{L_i}\end{aligned}$$

Πρόταση 3.4.1. *Η τάξη σύγκλισης της δυναμοσειράς* $\log_C(x)$, $\rho(\log_C(x))$, *είναι* $-\frac{q}{q-1} = \frac{q}{1-q}$

Απόδειξη. Το ζητούμενο έπεται άμεσα από τις

$$v_\infty(L_i) = q\frac{1-q^i}{q-1}$$

και

$$\rho(f) = -\lim_{j\to\infty}\frac{v(a_j)}{j}$$

□

Παρατηρούμε ότι

$$v_\infty(\xi) = -\frac{q}{q-1}$$

δηλαδή ο λογάριθμος συγκλίνει μέχρι και την μικρότερη μη μηδενική «περίοδο» του $e_C(x)$

3.5 Τα πολυώνυμα $E_d(x)$

Αν οι $\log_C(x)$ και e^x οι συνηθεις μηγαδικές συναρτήσεις. Εύκολα βλέπουμε ότι

$$(1+t)^x = e^{x\log(1+t)},$$

η οποία επεκτείνεται γύρο από το $x = 0$ καθώς

$$(1+t)^x = \sum_{n=0}^{\infty}\binom{x}{n}t^n$$

Θα δούμε ανάλογη κατάσταση στην περίπτωση της εκθετικής του Carlitz.

Ορισμός 3.5.1. *Θέτουμε*

$$e_C(z\log_C(x)) = \sum_{j=0}^{\infty}E_j(z)x^{q^j}$$

Αφού η $e_C(x)$ είναι entire, η $e_C(z\log(x))$, σύμφωνα με την πιο πάνω πρόταση, συγκλίνει (τουλάχιστον) για $\{(z,x)\}$ με $v_\infty(x) > \frac{q}{q-1}$

Πρόταση 3.5.2. (i) *$E_j(z)$ είναι $\mathbb{F}_q$ − γραμμικό πολυώνυμο βαθμού q^j.*

(ii) *$E_j(a) = 0$ για όλα τα $a \in \mathbf{A}(j)$.*

(iii) *$E_j(T^j) = 1$*

Πόρισμα 3.5.3. *Έχουμε ότι*

$$E_j(z) = \frac{e_j(z)}{D_j}$$

Απόδειξη. Το $e_j(z)$ έχει βαθμό q^j, οι ρίζες του είναι το σύνολο $\mathbf{A}(j)$ και από προηγούμενο αποτέλεσμα έχουμε $\frac{e_j(T^j)}{D_j} = 1$. □

Εδώ βλέπουμε έναν ακόμα τύπο για τους συντελεστές $C_a^{(j)}$.

Πόρισμα 3.5.4.

$$C_a^{(j)} = E_j(a) = \frac{e_j(a)}{D_j}$$

Από την ακόλουθη πρόταση φαίνεται ακόμα περισσότερο η αναλογία ανάμεσα στα $E_j(z)$ και τους δυονυμικούς συντελεστές $\binom{x}{j}$.

Πόρισμα 3.5.5. *Αν $a \in \mathbf{A}$ τότε και $e_j(a)/D_j \in \mathbf{A}$.*

Απόδειξη. Οι συντελεστές του $C_a(x)$ ανήκουν στο $\mathbf{A}$. □

3.6 Carlitz module πάνω από αυθαίρετα A − σώματα

Θέλουμε να μελετήσουμε το Carlitz module πάνω από αυθαίρετο σώμα, που δεν περιέχει αναγκαστικά το k. Έστω L ένα σώμα που περιέχει το $\mathbb{F}_q$. Αναμένουμε το Carlitz module πάνω από το L να μας δώσει μια απεικόνιση από το $\mathbf{A}$ στο $L\{\tau\}$. Αν συνθέσουμε αυτή την απεικόνηση με την απεικόνηση της παραγώγου από το $L\{\tau\}$ στο L (δηλαδή τον ομομορφισμό δακτυλίων $L\{\tau\} \mapsto L$ που πηγαίνει τα $\mathbb{F}_q-$ γραμμικά πολυώνυμα στο συντελεστή του όρου τ^0) παίρνουμε τον ορισμό :

Ορισμός 3.6.1. *Έστω L σώμα. Θα λέμε ότι το L είναι $\mathbf{A}-$**σώμα** αν και μόνο αν υπάρχει μορφισμός $\iota : \mathbf{A} \mapsto L$. Έστω $\mathfrak{p} = \ker(\iota)$ τότε όνομάζουμε το p χαρακτηριστική του L. θα λέμε ότι το L είναι γενικής χαρακτηριστικής αν και μόνο αν $\mathfrak{p} = (0)$.*

Άρα αν το L είναι γενικής χαρακτηριστικής τότε περιέχει το k σαν υπόσωμα. Θεωρούμε $\overline{L}$ να είναι η αλγεβρική κλειστότητα του L με την $\mathbf{A}-$ δομή που έπεται από την ι. Η διαδικασία για να κατασκευάσουμε το Carlitz module πάνω από το $\mathbf{A}$ έχει ως εξής : αρχικά εφαρμόζουμε την απεικόνιση ι στους συντελεστές του $C_a(\tau)$ ($a \in \mathbf{A}$), τα οποία είναι στοιχεία του $\mathbf{A}$, για να πάρουμε στοιχεία του $L\{\tau\}$.

Έστω $a \in \mathbf{A}$, τότε

$$C'_a(x) = \iota(a)$$

.

Άρα αν $a \notin \mathfrak{p}$ το $C_a(x)$ εξακολουθεί να είναι διαχωρίσιμο πολυώνυμο.

Μέσω του C το σώμα $\overline{L}$ γίνεται τώρα $\mathbf{A}-$ module : Έστω $a \in \mathbf{A}$ και $\alpha \in \overline{L}$, τότε έχουμε

$$(a, \alpha) \mapsto C_a(\alpha).$$

Το α θα λέγεται **σημείο στρέψης** αν και μόνο αν $C_a(\alpha) = 0$. Θέτουμε το $C[a] \subset \overline{L}$ να είναι οι ρίζες του $C_a(x)$, δηλαδή το module των $a-$ σημείων στρέψης. Όπως πριν έχουμε ότι το $C[a]$ εξαρτάται μόνο από το ιδεώδες που παράγεται από το a. Αν το $I = (i)$ είναι $\mathbf{A}-$ ιδεώδες τότε

$$C[I] := C[i]$$

Γενικά, αν το είναι όποιο $\mathbf{A}-$ σώμα τότε με το συμβολισμό "$C(K)$" εννοούμε το K ως $\mathbf{A}-$ module μέσω του C. Ο βασικός σκοπός εδώ είναι να περιγράψουμε τα σημεία στρέψης του C στο $C(\overline{L})$ ως $\mathbf{A}-$ modules.

Θεώρημα 3.6.2. (i) *Έστω $a \notin \mathfrak{p} = \ker(i)$. Τότε το $C[a] \subset C(\overline{L})$ είναι ισομορφικό με το $\mathbf{A}/(a)$.*

(ii) *Έστω $(f) = \mathfrak{p}$. Τότε $C[f^i] = \{0\} \subset \overline{L}$*

Γνωρίζουμε ότι $\mathbb{Z}/(p)^* \simeq \mathbb{Z}/(p-1)$ ως αβελιανές ομάδες. Θα παρουσιάσουμε το ανάλογο αποτέλεσμα για την περίπτωση του Carlitz module. Έστω $f \in \mathbf{A}$ μονικό και πρώτο. Ορίζουμε $\mathfrak{p} = (f)$ και $\mathbb{F}_\mathfrak{p} = \mathbf{A}/\mathfrak{p}$. Έστω $\mathbb{F}_{\mathfrak{p}^n}$ να είναι η μοναδική επέκταση του $\mathbb{F}_\mathfrak{p}$ επέκταση του $\mathbb{F}_\mathfrak{p}$ βαθμού n. Άρα το $\mathbb{F}_{\mathfrak{p}^n}$ είναι $\mathbf{A}-$σώμα μέσω της απεικόνησης $\mathbf{A} \to \mathbf{A}/\mathfrak{p} \to \mathbb{F}_{\mathfrak{p}^n}$ και είναι $\mathbf{A}-$module μέσω του C.

Θεώρημα 3.6.3. *Μέσω της C, $\mathbb{F}_\mathfrak{p}$ είναι $\mathbf{A}-$module ισόμορφικό με το $\mathbf{A}/(f^n-1)$.*

Απόδειξη. Το $\mathbb{F}_{\mathfrak{p}^n}$ είναι πεπερασμένο $\mathbf{A}-$module και πρέπει να είναι κυκλικό απο το προηγούμενο θεώρημα. Τώρα, από το 2ο αποτέλεσμα του ίδιου θεωρήματος μπορούμε να δούμε ότι

$$C_{f^n-1} \equiv x^{q^{n^{\deg f}}} (\mathfrak{p}\mathbf{A}[x]).$$

Αρα το C_{f^n-1} μηδενίζει το $\mathbb{F}_{\mathfrak{p}^n}$. Μετρόντας στοιχεία έχουμε το ζητούμενο. □

3.7 Adjoint του Carlitz module

Έστω $K^{\text{perf}} \subset C_\infty$ η τελειότητα του k. Σκοπός εδώ είναι να δείξουμε πως τα αποτελέσματα για την $\tau-$ adjoint προσθετικών πολυωνύμων μας επιτρέπουν να συμπεράνουμε την ύπαρξη της $\tau-$adoint ή adjoint για το Carlitz module C.

Θυμόμαστε ότι

$$C_a(\tau) = a\tau^0 + \sum_{i=1}^{\deg(a)} C_a^{(i)}\tau^i \in K\{\tau\}$$

από τον ορισμό που δώσαμε για την adjoint προσθετικών πολυωνύμων καταλήγουμε στον

Ορισμός 3.7.1. *θέτουμε*

$$C_a^*(\tau) = \tau^0 + \sum_{i=1}^{\deg(a)} (C_a^{(i)})\tau^{-i} \in k^{\text{perf}}\{\tau^{-1}\}$$

όπου $k^{\text{perf}}\{\tau^{-1}\}$ ο δακτύλιος των πολυωνύμων του Frobenious στο τ^{-1}.

Λήμμα 3.7.2.

$$C_{ba}^*(\tau) = C_a^*(\tau)C_b^*(\tau) = C_b^*(\tau)C_a^*(\tau) = C_{ab}^*(\tau)$$

Απόδειξη. Έχουμε,

$$C_{ba}(\tau) = C_b(\tau)C_a(\tau) = C_a(\tau)C_b(\tau) = C_{ab}(\tau)$$

το αποτέλεσμα είναι άμεσο με χρήση του λήμματος 1.6.3 □

Παρατήρηση 3.7.3. (i) *Ακριβώς όπως το C παράγεται από το C_T το C_T^* παράγεται από το $C_T^* = T\tau^0 + \tau^{-1}$. Άρα*

$$\begin{aligned} C_{T^2}^* &= (T\tau^0 + \tau^{-1})(T\tau^0 + \tau^{-1}) \\ &= T^2\tau^0 + (T^{1/q} + T)\tau^{-1} + \tau^{-2}. \end{aligned}$$

Γενικά μπορούμε να πάρουμε το C_a^* από το C_a αν αντιμετωπίσουμε το q ως μεταβλητή και αντικαταστήσουμε το q^i με το q^{-i}.

(ii) *Όλες οι ιδέες για τα σημεία στρέψης βγάζουν νόημα και για το C^*.Τα σημεία στρέψης του C^* είναι αλγεβρικά πάνω από το k. Από ένα αποτέλεσμα της παραγράφου για τα προσθετικά πολυώνυμα παίρνουμε ότι τα $I-$ σημεία στρέψης των C και C^* παράγουν την ίδια επέκταση του k.*

Κεφάλαιο 4

Αναλογίες

4.1 Θεωρία Κυκλοτομικών σωμάτων

Θα ξεκινήσουμε παραθέτοντας χωρίς απόδειξη στοιχεία από την θεωρία των κυκλοτομικών σωμάτων αριθμών. Έστω $m > 2$ ένας θετικός ακέραιος και ζ_m μια πρωταρχική m-ρίζα της μονάδας. Το σώμα $K_m = \mathbb{Q}(\zeta_m)$ θα λέγεται το m-κυκλοτομικό σώμα αριθμών και το οποίο είναι το σώμα διάσπασης του (μη-αναγώγου) πολυωνύμου $x^m - 1$, συνεπώς η επέκταση $\mathbb{Q}(\zeta_m)/\mathbb{Q}$ είναι μια επέκταση Galois με ομάδα Galois η οποία αποδεικνύεται να είναι ισόμορφη με την πολλαπλασιαστική ομάδα $(\mathbb{Z}/m\mathbb{Z})^*$ κάτω από τον ισομορφισμό

$$\begin{aligned} (\mathbb{Z}/m\mathbb{Z})^* &\longrightarrow \text{Gal}(\mathbb{Q}(\zeta_m)/\mathbb{Q}) \\ n \mod m &\longmapsto \sigma_n := (\zeta_m \mapsto \zeta_m^n) \end{aligned}$$

Η επέκταση $K_m/\mathbb{Q}$ είναι αβελιανή επέκταση βαθμού $\phi(m)$, όπου ϕ είναι η συνάρτηση του Euler.

Παρατηρούμε ότι το σ_{-1} είναι η μιγαδική συζυγία στο K_m. Επίσης αν $p > 0$ είναι πρώτος $(p, m) = 1$ τότε το σ_p είναι ο Artin αυτομορφισμός του πρώτου ιδεώδους $p\mathbb{Z}$, δηλαδή η ανύψωση του αυτομορφισμού του Frobenius, [15]. Για να κατανοήσουμε το τελευταίο θα πρέπει να αναλύσουμε την διακλάδωση στην επέκταση $K_m/\mathbb{Q}$ και τον δακτύλιο των ακεραίων $\mathcal{O}_m$ του σώματος K_m.

Θεώρημα 4.1.1. *Έστω $m > 0$ ένας ακέραιος που δεν είναι το διπλάσιο ενός περιττού. Αν ζ_m είναι μια πρωταρχική m ρίζα της μονάδας και $K_m = \mathbb{Q}(\zeta_m)$. Τότε το $K_m/\mathbb{Q}$ είναι μια αβελιανή επέκταση βαθμού $\phi(m)$ με ομάδα ισόμορφη με το $(\mathbb{Z}/m\mathbb{Z})^*$. Ένας πρώτος p του $\mathbb{Z}$ διακλαδίζεται στο $K_m/\mathbb{Q}$ αν και μόνο αν $p \mid m$. Αν $p > 0$ δεν διαιρεί το m, τότε ο αυτομορφισμός του Artin που αντιστοιχεί στο πρώτο ιδεώδες $P = p\mathbb{Z}$ στέλνει το ζ_m στο ζ_m^p. Αν f είναι ο μικρότερος θετικός ακέραιος ώστε*

$$p^f \equiv 1 \mod m$$

τότε το $P = p\mathbb{Z}$ διασπάται στο $\mathcal{O}_m$ σε $\phi(m)/f$ πρώτα ιδεώδη βαθμού f. Τέλος ο δακτύλιος των ακεραίων $\mathcal{O}_m = \mathbb{Z}[m]$.

Θα δούμε τώρα την συμπεριφορά των άπειρων πρώτων στην επέκταση $K_m/\mathbb{Q}$. Το σώμα $\mathbb{Q}$ έχει ένα μοναδικό πρώτο στο άπειρο την συνηθισμένη απόλυτη τιμή. Στο σώμα K_m κάθε εμφύτευση στο σώμα των μιγαδικών αριθμών είναι μιγαδική αφού

οι μοναδικές ρίζες της μονάδας στο $\mathbb{R}$ είναι το ± 1. Ας θεωρήσουμε το σώμα $K_m^+ = \mathbb{Q}(\zeta_m + \zeta_m^{-1}) \subset \mathbb{R}$. Είναι ένα πραγματικό σώμα αριθμών και κάθε εμφύτευση του στο σώμα των μιγαδικών αριθμών είναι πραγματική. Επίσης $[K_m : \mathbb{Q}(\zeta_m + \zeta_m^{-1})] = 2$ αφού το ζ_m ικανοποιεί την σχέση $x^2 - (\zeta_m + \zeta_m^{-1})x + 1 = 0$. Συνεπώς ο πρώτος στο άπειρο του $\mathbb{Q}$ διασπάται σε $\phi(m)/2$ πραγματικούς πρώτους στο K^+ και κάθε ένας από αυτούς διακλαδίζεται σε ένα μιγαδικό πρώτο στο K_m. Αφού $\mathrm{Gal}(K_m/K_m^+) = \langle \sigma_{-1} \rangle$, το στοιχείο σ_{-1} μπορεί να θεωρηθεί να παράγει την ομάδα αδρανείας των πρώτων στο άπειρο του σώματος K_m.

Το θεώρημα των Kronecker-Weber και η θεωρία κλάσεων σωμάτων.

4.2 Drinfeld modules

Έχουμε ήδη δει από το πρώτο κεφάλαιο ότι ο δακτύλιος των προσθετικών πολυώνυμων πάνω από το σώμα k μπορεί να ταυτιστεί με τον δακτύλιο $k\{\tau\}$. Θα δώσουμε τώρα μια ερμηνεία του δακτυλίου αυτού στην γλώσσα των group schemes. Για μια γενική εισαγωγή στην θεωρία των group schemes παραπέμπουμε στο άρθρο του J. Tate [12].

Το group scheme $\mathbb{G}_a/k$ είναι ένας συναρτητής ο οποίος σε κάθε αντιμεταθετική k-άλγεβρα B αντιστοιχεί την προσθετική ομάδα $(B, +)$. Είναι σαφές ότι κάθε προσθετικό πολυώνυμο επάγει έναν ενδομορφισμό του $(B, +)$ με προφανή τρόπο. Δηλαδή αν $u \in B$ και $\sum a_i \tau^i \in k\{\tau\}$ τότε

$$\left(\sum a_i \tau^i\right)(u) = \sum a_i u^{q^i}.$$

Με βάση την παραπάνω παρατήρηση μπορεί να αποδειχθεί ότι

$$\mathrm{End}(\mathbb{G}_a/k) \cong k\{\tau\}.$$

Θεωρούμε τον δακτύλιο $\mathbf{A} = \mathbb{F}_q[T]$ και $k = \mathbb{F}_q(T)$. Στα παρακάτω η ενδιαφέρουσα k άλγεβρα B στην οποία θα επικεντρωθούμε είναι η αλγεβρική κλειστότητα $\bar{k}$.

Ορισμός 4.2.1. *Ένα Drinfeld module για το $\mathbb{A}$ ορισμένο επί του k είναι ένας μορφισμός από $\mathbb{F}_q$-άλγεβρες*

$$\begin{aligned} \rho : \mathbf{A} &\longrightarrow k\{\tau\} \\ a &\longmapsto \rho_a \end{aligned}$$

ώστε για κάθε $a \in \mathbf{A}$ ο σταθερός όρος του ρ_a να είναι a και επιπλέον για τουλάχιστον ένα $a \in \mathbf{A}$, $\rho_a \notin \mathbf{A}$.

Στην πραγματικότητα ο ορισμός των Drinfeld modules είναι πολύ γενικότερος αλλά ο παραπάνω ορισμός είναι αρκετός για τις ανάγκες μας. Παρατηρήστε ότι στην πραγματικότητα ορίζουμε μια παραμόρφωση (deformation) της αρχικής μας άλγεβρας $\mathbf{A}$.

Η ιδέα πίσω από τον ορισμό είναι ότι με βάση ένα Drinfeld module ρ κάθε αντιμεταθετική άλγεβρα B μπορεί να γίνει ένα $\mathbf{A}$-module με ένα εντελώς νέο τρόπο:

$$a \cdot u = \rho_a(u) \text{ για κάθε } a \in \mathbf{A} \text{ και } u \in B$$

Η συνθήκη $\rho_a \notin k$ εξασφαλίζει ότι η νέα δράση είναι πράγματι διαφορετική από τον πολλαπλασιασμό με $\mathbf{A}$.

Παρατηρούμε ότι αφού το $\mathbb{A}$ παράγεται με ελεύθερο τρόπο από το T, το να προσδιορίσουμε ένα Drinfeld module αρκεί να προσδιορίσουμε την εικόνα ρ_T του T ως ένα πολυώνυμο στο $k\{\tau\}$. Ο σταθερός όρος του πουλυωνύμου αυτού πρέπει να είναι T.

Η απλούστερη επιλογή για ένα Drinfeld module είναι αυτό του Carlitz όπου

$$C_T = T + \tau.$$

Αν ρ είναι ένα Drinfeld module και

$$\rho_T = T + c_1\tau + c_2\tau^2 + \cdots c_r\tau^r,$$

όπου τα $c_i \in k$ και $c_r \neq 0$. Αφού $\rho_{T^2} = \rho_T\rho_T$ ο σταθερός όρος του ρ_{T^2} θα είναι T^2 και η μεγαλύτερη δύναμη του τ η οποία εμφανίζεται είναι $2r$ ενώ ο κυρίαρχος συντελεστής θα είναι $c_r^{1+q^r}$. Συνεχίζοντας με τον ίδιο τρόπο βλέπουμε ότι ο σταθερός όρος του ρ_{T^n}, η μεγαλύτερη δύναμη που εμφανίζεται είναι nr ενώ ο κυρίαρχος συντελεστής είναι c_r υψωμένος στην $1 + q^r + q^{2r} + \cdots + q^{(n-1)r}$. Γενικά ο σταθερός όρος του γενικού ρ_a είναι a ενώ ο βαθμός του μεγαλύτερου τ είναι $r \cdot \deg(a)$. Θα λέμε λοιπόν ότι το Drinfeld module έχει rank r. Το Carlitz module έχει rank 1.

Αν θεωρήσουμε το $\bar{k}$ ως ένα $\mathbb{A}$-module μέσω του Drinfeld module ρ, μπορούμε να θεωρήσουμε το torsion module:

$$\Lambda_\rho := \{\lambda \in \bar{k} : \rho_a(\lambda) = 0\}.$$

Για κάθε $a \in \mathbf{A}$, $a \neq 0$ ορίζουμε το υπomodule $\Lambda_\rho[a] \subset \Lambda_\rho$ ως

$$\Lambda_\rho[a] := \{\lambda \in \bar{k} : \rho_a(\lambda) = 0\}.$$

Λήμμα 4.2.2. *Έστω $a \in \mathbf{A}$, $a \neq 0$. Ας θεωρήσουμε το $\mathbf{A}$-module M και ας υποθέσουμε ότι για κάθε $b \mid a$ το υπomodule $M[b] = \{m \in M : bm = 0\}$, έχει $q^{r\deg(b)}$ στοιχεία. Τότε*

$$M[a] \cong \mathbf{A}/a\mathbf{A} \oplus \cdots \oplus \mathbf{A}/a\mathbf{A}, \qquad r - \textit{προσθετέοι}.$$

Απόδειξη. Θεωρούμε την ανάλυση του a, σε πρώτους παράγοντες,

$$a = \alpha P_1^{e_1} P_2^{e_2} \cdots P_t^{e_t},$$

όπου $\alpha \in \mathbb{F}_q^*$ και τα P_i διατρέχουν τους μονικούς ανάγωγους διαιρέτες του a. Είναι σαφές από το κινέζικο θεώρημα ότι το $M[a]$ είναι ισόμορφο με το ευθύ άθροισμα των $M[P_i^{e_i}]$.

Θα περιοριστούμε λοιπόν στην περίπτωση $a = P^e$. Στην περίπτωση αυτή το $M[P]$ είναι ένας διανυσματικός χώρος υπέρ το $\mathbf{A}/P\mathbf{A}$ με $q^{\deg(P)}$ στοιχεία από την υπόθεση. Ας σημειωθεί ότι το $\mathbf{A}/P\mathbf{A}$ έχει $q^{\deg(P)}$ το πλήθος στοιχεία. Από το θεώρημα δομής των modules πάνω από περιοχές κυρίων ιδεωδών το $M[P^e]$ είναι άθροισμα r-κυκλικών υπomodules,

$$M[P^e] \cong \mathbf{A}/P^{f_1}\mathbf{A} \oplus \cdots \oplus \mathbf{A}/P^{f_r}\mathbf{A}.$$

Θα πρέπει να έχουμε $f_i \leq e$ για κάθε $1 \leq i \leq r$. Το πλήθος των στοιχείων στο δεξί μέρος της παραπάνω εξίσωσης είναι $q^{(f_1+\cdots+f_r)\deg(P)}$. Το πλήθος των στοιχείων του αριστερού μέρους είναι εξ υποθέσεως q υψωμένο στην $re\deg(P)$. Συνεπώς $f_i = e$ για όλα τα i. □

Πρόταση 4.2.3. *Έστω ρ ένα Drinfeld module rank r, δηλαδή για κάθε $a \in \mathbf{A}$, ο βαθμός του τ στο ρ_a είναι $r\deg(a)$. Τότε για κάθε $a \in \mathbf{A}$, $a \neq 0$ έχουμε*

$$\Lambda_\rho[a] \cong \mathbf{A}/a\mathbf{A} \oplus \cdots \oplus \mathbf{A}/a\mathbf{A}, \qquad r - \textit{φορες}.$$

Επίσης για το module Λ_ρ έχουμε

$$\Lambda_\rho \cong k/\mathbf{A} \oplus \cdots \oplus k/\mathbf{A}, \qquad r - \textit{φορες}.$$

Απόδειξη. Θα χρησιμοποιήσουμε το λήμμα 4.2.2 με $M = \bar{k}_\rho$. Θα πρέπει απλά να ελέγξουμε ότι για κάθε $a \neq 0$, $a \in \mathbf{A}$ το $\Lambda_\rho[a]$ έχει $q^{r \deg(a)}$ το πλήθος στοιχεία. Το $\rho_a(x)$ έχει την μορφή

$$\rho_a(x) = ax + b_1 x^q + b_2 x^{q^2} + \cdots + b_{r\deg(a)} x^{q^{r\deg(a)}},$$

όπου τα $b_i \in k$ και $b_{r\deg(a)} \neq 0$. Η παράγωγος του $\rho_a(x)$ ως προς x είναι $a \neq 0$ συνεπώς το πολυώνυμο έχει $q^{r\deg(a)}$ το πλήθος διαφορετικές ρίζες στο $\bar{k}$. Οι ρίζες αυτές είναι ακριβώς τα στοιχεία του $\Lambda_\rho[a]$, και το πρώτο μέρος της πρότασης έχει αποδειχθεί.

Το δεύτερο μέρος προκύπτει από το πρώτο, αρκεί να παρατηρήσει κανείς ότι το Λ_ρ είναι η ένωση των υπομodules $\Lambda_\rho[a]$ καθώς το a διατρέχει τα μη-μηδενικά στοιχεία του $\mathbf{A}$. Επιπλέον αφού $\mathbf{A}/a\mathbf{A} \cong a^{-1}\mathbf{A}/\mathbf{A}$ ο παραπάνω ισομορφισμός μπορεί να γραφεί ως

$$\Lambda_\rho[a] \cong a^{-1}\mathbf{A}/\mathbf{A} \oplus \cdots \oplus a^{-1}\mathbf{A}/\mathbf{A}, \qquad r - \text{φορες}.$$

Το ζητούμενο προκύπτει πέρνοντας το ευθύ όριο το οποίο στην περίπτωσή μας μπορεί να αντιμετατεθεί με τα αθροίσματα. □

Προσαρτούμε τώρα τα στοιχεία του $\Lambda_\rho[a]$ στο k για να σχηματίσουμε τα σώματα $K_{\rho,a} := k(\Lambda_r[a])$. Αφού τα $\rho_a(x)$ είναι όπως έχουμε δει διαχωρίσιμα πολυώνυμα η επέκταση $K_{\rho,a}/k$ είναι επέκταση του Galois. Αφού $\rho_a(x) \in k[x]$, έχουμε ότι $\rho_a(\lambda) = 0$ δίνει ότι $r_a(\sigma\lambda) = 0$ για κάθε $\sigma \in \mathrm{Gal}(K_{\rho,a}/k)$. Δηλαδή το σ επάγει ένα αυτομορφισμό του $\Lambda_r[a]$ και με αυτό τον τρόπο έχουμε ένα ομομορφισμό

$$\psi : \mathrm{Gal}(K_{\rho,a}/k) \longrightarrow \mathrm{Aut}_{\mathbf{A}/a\mathbf{A}}(\Lambda_r[a]).$$

Αφού το $\Lambda_\rho[a]$ παράγει το σώμα $K_{\rho,a}$, κάθε αυτομορφισμός σ που επάγει την ταυτότητα είναι τετριμμένος και ο ψ είναι μονομορφισμός. Επίσης έχουμε ότι

$$\mathrm{Aut}_{\mathbf{A}/a\mathbf{A}}(\Lambda_r[a]) \cong \mathrm{GL}_r(\mathbf{A}/a\mathbf{A}).$$

Καταλήγουμε λοιπόν στην πρόταση:

Πρόταση 4.2.4. *Το $K_{r,a}/k$ είναι μία επέκταση Galois και υπάρχει ένας μονομορφισμός*

$$\mathrm{Gal}(K_{\rho,a}/k) \to \mathrm{GL}_r(\mathbf{A}/a\mathbf{A}).$$

Πόρισμα 4.2.5. *Αν το ρ έχει rank 1 η επέκταση $K_{\rho,a}/k$ είναι αβελιανή.*

Απόδειξη. Πράγματι $\mathrm{GL}_1(\mathbf{A}/a\mathbf{A}) \cong (\mathbf{A}/a\mathbf{A})^*$. □

4.3 Το Carlitz module ως γενίκευση των κυκλοτομικών σωμάτων

Το Carlitz module είναι ένα Drinfeld Module rank 1 και συνεπώς δίνει με επισύναψη των σημείων του πεπερασμένης τάξης, αβελιανές επεκτάσεις του k. Θα συμβολίζουμε με Λ_a το $\Lambda_C[a]$ για τα σημεία a-ταξης του Carlitz module. Επίσης για να φέρουμε τον συμβολισμό κοντά στην θεωρία των κυκλοτομικών σωμάτων αντί $a \in \mathbf{A}$ θα θεωρούμε το στοιχείο $m \in \mathbf{A}$.

Τα σώματα $K_m = k(\Lambda_m)$ θα δούμε ότι είναι τα ανάλογα των κυκλοτομικών σωμάτων αριθμών και θα τα ονομάζουμε κυκλοτομικά σώματα συναρτήσεων.

Πρόταση 4.3.1. (i) *Έστω $\mathcal{O}_m$ η ακέραια κλειστότητα του $\mathbf{A}$ στο K_m. Τότε $\mathcal{O}_m = \mathbf{A}[\lambda_m]$.*

(ii) *Έστω $P \in \mathbf{A}$ ένα μονικό ανάγωγο πολυώνυμο και $e \in \mathbb{Z}$, $e > 0$. Τότε K_{P^e} είναι αδιακλάδιστο σε κάθε πρώτο ιδεώδες $Q\mathbf{A}$ με $Q\mathbf{A} \neq P\mathbf{A}$. Ο πρώτος $P\mathbf{A}$ διακλαδίζεται πλήρως με δείκτη διακλάδωσης $\Phi(P^e)$. Έχουμε*

$$[K_{P^e} : k] = \Phi(P^e) \text{ και } \mathrm{Gal}(K_{P^e}/k) = (\mathbf{A}/P^e\mathbf{A})^*.$$

Το πρώτο ιδεώδες υπέρ το $P\mathbf{A}$ είναι το $\lambda\mathcal{O}_{P^e}$, όπου λ είναι ένας γεννήτορας του Λ_{P^e}.

(iii) *Έστω $m = \alpha P_1^{e_1} \cdots P_t^{e_t}$ η ανάλυση σε πρώτα του m. Το σώμα K_m είναι η σύνθεση των σωμάτων $K_{P_i^{e_i}}$. Τα μοναδικά ιδεώδη του $\mathbf{A}$ τα οποία διακλαδίζονται στην επέκταση είναι τα $P_i\mathbf{A}$. Έχουμε $[K_m : k] = \Phi(m)$ και*

$$\mathrm{Gal}(K_m/k) \cong (\mathbf{A}/m\mathbf{A})^*.$$

(iv) *Έστω $m \in \mathbf{A}$ θετικού βαθμού και $P \in \mathbf{A}$ μονικό ανάγωγο πολυώνυμο που δεν διαιρεί το m. Τότε ο αυτομορφισμός του Artin του πρώτου ιδεώδους $P\mathbf{A}$ στην επέκταση K_m/k είναι ο αυτομορφισμός s_P ο οποίος στέλνει το λ_m στο $C_P(\lambda_m)$. Έστω f ο ελάχιστος θετικός ακέραιος ώστε*

$$P^f \equiv 1 \mod m.$$

Τότε το $P\mathcal{O}_m$ είναι το γινόμενο $\Phi(m)/f$ πρώτων ιδεωδών το καθένα από τα οποία έχει βαθμό f. Ειδικότερα το $P\mathbf{A}$ διασπάται πλήρως αν και μόνο αν $P \equiv 1 \mod m$.

Το επόμενο θεώρημα αναφέρεται στην συμπεριφορά των άπειρων πρώτων. Ο δακτύλιος $\mathbf{A}$ και τα πρώτα ιδεώδη του αντιστοιχούν στους «πεπερασμένους πρώτους» των σωμάτων αριθμών. Το σώμα συναρτήσεων $\mathbb{F}_q(T)$ από την άλλη αντιστοιχεί στην προβολική ευθεία. Αν και δεν υπάρχουν στα σώματα συναρτήσεων μη-αρχιμήδειες μετρικές μπορούμε να θεωρήσουμε τον άπειρο πρώτο $1/T$ και την πλήρωση k_∞ του σώματος $\mathbb{F}_q(1/T)$ ως προς αυτόν. Η επιλογή μεταβλητής $1/T$ γεωμετρικά αντανακλά την αλλαγή χάρτη που κάνουμε στην προβολική ευθεία προκειμένου να κάνουμε το ∞ να συμπεριφέρεται όπως το 0.

Το σώμα k_∞ μπορεί να γίνει και αυτό ένα $\mathbb{A}$-module με τον ίδιο ακριβώς τρόπο που έγινε $\mathbf{A}$-module το $\bar{k}$ δηλαδή

$$a \cdot u = C_a(u), \text{ για κάθε} a \in \mathbf{A} \text{ και } u \in k_\infty.$$

Το σώμα k_∞ θα παίζει τον ρόλο του $\mathbb{R}$ το οποίο στην περίπτωση των σωμάτων αριθμών αποτελεί την πλήρωση του $\mathbb{Q}$ ως προς τον άπειρο πρώτο, δηλαδή την συνηθισμένη απόλυτη τιμή $|\cdot|$. Στην περίπτωση των σωμάτων αριθμών ο δακτύλιος $\mathbb{Z}$ είχε μόνο μια μη τετριμμένη μονάδα η οποία στην ομάδα Galois αντιστοιχούσε στην μιγαδική συζυγία. Εδώ οι μονάδες του δακτυλίου $\mathbb{A}$ είναι πολλές, όλο το $\mathbb{F}_q^*$ οι οποίες δίνουν μια ομάδα μιγαδικών συζυγιών J.

Θεώρημα 4.3.2. *Έστω $J = \{\sigma_\alpha \in \mathrm{Gal}(K_m/k) : \alpha \in \mathrm{F}_q^*\}$. Θέτουμε $K_m^+ = K_m^J$. Τότε ο άπειρος πρώτος ∞ διασπάται πλήρως στο σώμα K_m^+ και κάθε πρώτος που επεκτείνει το ∞ στο K_m^+ διακλαδίζεται πλήρως και ήμερα στο K_m.*

Θα τελειώσουμε την σειρά των αναλογιών εκφράζοντας το αντίστοιχο του θεωρήματος των Kronecker-Weber στην περίπτωση των σωμάτων συναρτήσεων. Είναι σαφές ότι δεν είναι δυνατόν οι αβελιανές επεκτάσεις του k να περιγραφούν μόνο με τα κυκλοτομικά σώματα K_m. Για παράδειγμα οι αριθμητικές επεκτάσεις $\mathbb{F}_{q^h}(T)$ του $\mathbb{F}_q(T) = k$ δεν αποτελούν κυκλοτομικά σώματα αριθμών. Στην περίπτωση των σωμάτων αριθμών οι επισυνάψεις των ριζών της μονάδας είναι σύμφωνα με την θέαση του Iwasawa τα αντίστοιχα των επεκτάσεων των σταθερών και δεν υπάρχει καμία διαφοροποίηση.

Σταθεροποιούμε μία αλγεβρική κλειστότητα $\bar{k}$ του k. Συμβολίζουμε με $k(\Lambda)$ την ένωση όλων των κυκλοτομικών σωμάτων K_m. Θεωρούμε την μέγιστη επέκταση σταθερών του k την $\bar{\mathbb{F}}_q k$. Τα παραπάνω σώματα αποτελούν ξένες και αβελιανές επεκτάσεις του k. Όμως ούτε αυτές είναι αρκετές για να περιγράψουν την μέγιστη αβελιανή επέκταση αφού κάθε υπόσωμα αυτών διακλαδίζεται ήμερα στο ∞. Θεωρούμε το ιδεώδες $\langle 1/T \rangle$ στον δακτύλιο $\mathbb{F}_q[1/T]$ και πάλι μέσω της κατασκευής του Carlitz κατασκευάζουμε τα σώματα $k(\Lambda_{T^{-n-1}})$. Τα σώματα αυ΄τα είναι αβελιανές επεκτάσεις του k, πλήρως διακλαδισμένες στο ∞ και $[k(\Lambda_{T^{-n-1}}) : k] = q^n(q-1)$. Θεωρούμε το μοναδικό υπόσωμα σώμα L_n το όποιο έχει βαθμό επέκτασης $[L_n : k] = q^n$ και θέτουμε L_∞ την ένωση όλων των σωμάτων L_n. Τα τρία σώματα $k(\Lambda), \bar{\mathbb{F}}_q, L_\infty$ είναι ξένα και το ανάλογο του Kronecker Weber αναφέρει ότι κάθε αβελιανή επέκταση περιέχεται στην σύνθεση τους.

Καταλήγουμε τελικά στον παρακάτω πίνακα αναλογιών.

Σώματα Αριθμών	Σώματα Συναρτήσεων
$\mathbb{Z} \subset \mathbb{Q}$	$\mathbf{A} = \mathbb{F}_q[T] \subset k = \mathbb{F}_q(T)$
$\mathbb{R} \subset \mathbb{C}$	$k_\infty \subset C_\infty$
πρώτα ιδεώδη του $\mathbb{Z}$	Πρώτα ιδεώδη του $\mathbf{A}$
αρχίμηδειες και μη-αρχιμήδειες μετρικές	μόνο μη-αρχιμήδειες μετρικές
εκθετική συνάρτηση $e^x : \mathbb{C} \to \mathbb{C}$	$e_C(x) : C_\infty \to C_\infty$
$e^{nx} = (e^x)^n, n \in \mathbb{Z}$	$e_C(ax) = C_a(e_C(x)), a \in \mathbf{A}$
$S^1 = \mathbb{R}/\mathbb{Z}$	$k_\infty/\mathbf{A}$
n-στρέψη κύκλου $\mathbb{Z}/n\mathbb{Z}$	$\Lambda_m = \mathbf{A}/m\mathbf{A}$
$\mathbb{Q}(\zeta_m)$	K_m
$\mathrm{Gal}(\mathbb{Q}(\zeta_m)/Q) = (\mathbb{Z}/m\mathbb{Z})^*$	$\mathrm{Gal}(K_m/k) = (\mathbf{A}/m\mathbf{A})^*$
Μέγιστη αβελιανή επέκταση $\cup\mathbb{Q}(\zeta_n)$ του $\mathbb{Q}$	$k(\Lambda) \cdot \bar{\mathbb{F}}_q \cdot L_\infty$

Βιβλιογραφία

[1] Leonard Carlitz. The Arithmetic of Polynomials in a Galois Field. *Amer. J. Math.*, 54(1):39–50, 1932.

[2] V. G. Drinfel′ d. Elliptic modules. *Mat. Sb. (N.S.)*, 94(136):594–627, 656, 1974.

[3] L. D. Faddeev and O. A. Yakubovskiĭ. *Lectures on quantum mechanics for mathematics students*, volume 47 of *Student Mathematical Library*. American Mathematical Society, Providence, RI, 2009. Translated from the 1980 Russian original by Harold McFaden, With an appendix by Leon Takhtajan.

[4] David Goss. *Basic structures of function field arithmetic*, volume 35 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1996.

[5] Helmut Hasse. *Number theory*. Classics in Mathematics. Springer-Verlag, Berlin, german edition, 2002. Reprint of the 1980 English edition [Springer, Berlin; MR0562104 (81c:12001b)], Edited and with a preface by Horst Günter Zimmer.

[6] D. R. Hayes. Explicit class field theory for rational function fields. *Trans. Amer. Math. Soc.*, 189:77–91, 1974.

[7] David R. Hayes. Explicit class field theory in global function fields. In *Studies in algebra and number theory*, volume 6 of *Adv. in Math. Suppl. Stud.*, pages 173–217. Academic Press, New York-London, 1979.

[8] M Kapranov and A. Smirnov. Cohomology determinants and reciprocity laws:number field case. *Unpublished Article*.

[9] Dino Lorenzini. *An invitation to arithmetic geometry*, volume 9 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 1996.

[10] Michael Rosen. *Number theory in function fields*, volume 210 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 2002.

[11] Peter Stevenhagen. Hilbert's 12th problem, complex multiplication and Shimura reciprocity. In *Class field theory—its centenary and prospect (Tokyo, 1998)*, volume 30 of *Adv. Stud. Pure Math.*, pages 161–176. Math. Soc. Japan, Tokyo, 2001.

[12] John Tate. Finite flat group schemes. In *Modular forms and Fermat's last theorem (Boston, MA, 1995)*, pages 121–154. Springer, New York, 1997.

[13] Gabriel Daniel Villa Salvador. *Topics in the theory of algebraic function fields*. Mathematics: Theory & Applications. Birkhäuser Boston, Inc., Boston, MA, 2006.

[14] L. I. Wade. Certain quantities transcendental over $GF(p^n, x)$. II. *Duke Math. J.*, 10:587–594, 1943.

[15] Γ. Αντωνιάδης. *Αλγεβρική Θεωρία Αριθμών*. Διδακτικές σημειώσεις, Πανεπιστήμιο Κρήτης, 1986.

[16] Α. Κοντογεώργης Γ. Αντωνιάδης. Αριθμητική Γεωμετρία, Ιστορία, Επιτευγματα και μέλλον. *Τόμος της Ελληνικής Μαθηματικής Εταιρίας για τα 100 χρόνια από την ίδρυση της*, 2018.

[17] Γ. Τάτσης. Λ-δακτύλιοι και το σώμα με ένα στοιχείο. Master's thesis, Εθνικό και Καποδιστριακό Πανεπιστήμιο Αθηνών, 2017.