Πανεπιστημιο Κρητης Τμημα Μαθηματικων

Διδακτορικη Διατριβη

Drinfeld modules και εφαρμογες στο αντιστροφο προβλημα της θεωριας του Galois

Μαρινα Τριπολιτακη

Ηράκλειο 29 Μαΐου 2003

Η εργασία αυτή εκπονήθηκε στα πλαίσια των υποχρεώσεων της Μαρίνας Τριπολιτάκη για την απόκτηση διδακτορικού διπλώματος στα μαθηματικά στο τμήμα μαθηματικών του πανεπιστημίου κρήτης.

Η ΤΡΙΜΕΛΗΣ ΕΠΙΤΡΟΠΗ:

Γ. Αντωνιαδης
Δ. Δεριζιωτης
Α. Κουβιδακης

ΟΙ ΜΕΝ ΙΠΠΗΩΝ ΣΤΡΟΤΟΝ ΟΙ ΔΕ ΠΕΣΔΩΝ
ΟΙ ΔΕ ΝΑΩΝ ΦΑΙΣ ΕΠΙ ΓΑΝ ΜΕΛΑΙΝΑΝ
ΕΜΕΝΕ ΚΑΛΛΙΣΤΟΝ ΕΓΩ ΔΕ ΚΗΝ ΟΤΤΩ ΤΙΣ ΕΡΑΤΑΙ
ΣΑΠΦΑ

Περιεχόμενα

Εισαγωγή

Τα Drinfeld modules εμφανίστηκαν στη βιβλιογραφία για πρώτη φορά το 1974 κάτω από το όνομα elliptic modules. Σήμερα, προς τιμή του βραβευμένου με Fields δημιουργού τους, φέρουν το όνομα του. Από τότε μέχρι σήμερα έχουν κατακτήσει κεντρικό ρόλο στη θεωρία αριθμών της πεπερασμένης χαρακτηριστικής και ειδικότερα στη θεωρία των σωμάτων συναρτήσεων, στη θεωρία των ελλειπτικών καμπύλων και των αλγεβρών με διαίρεση. Άλλωστε ένα από τα τελευταία Fields Medals που δόθηκαν ανήκει στην περιοχή.

Με K θα συμβολίζουμε το σώμα συναρτήσεων μίας ανάγωγης και γεωμετρικά συνεκτικής καμπύλης $\mathcal{C}$ υπέρ το $\mathbf{F}_q$. Έστω ∞ μία θέση του K και A ο δακτύλιος των ακεραίων ως προς το άπειρο συναρτήσεων του K. Έστω $\mathbb{G}_a$ το προσθετικό group scheme πάνω από ένα $K-$scheme S και $\gamma\colon A \longrightarrow K$ ομομορφισμός δακτυλίων. Ένα $K-$Drinfeld module ταξεως $r \in \mathbb{N}$ είναι ένας μη τετριμμένος ενδομορφισμός

$$\varphi\colon A \longrightarrow \mathrm{End}_S(\mathbb{G}_a)\ ;\ a \longmapsto \phi_a$$

με $\frac{\partial}{\partial \tau}\varphi_a = \gamma(a)$ όπου το τ δηλώνει τον Frobenius ενδομορφισμό και r τον βαθμό του γεννοποιού στοιχείου της εικόνας.

Η έννοια των Drinfeld modules τάξεως ένα ήταν γνωστή στον Carlitz από τη δεκαετία του 30. Τα modules του τύπου αυτού παίζουν σημαντικό ρόλο στην θεωρία κλάσεων σωμάτων προσφέροντας μία κατασκευαστική προσέγγιση αυτής.

Η παρούσα εργασία χωρίζεται σε δύο ανεξάρτητα μέρη. Στο πρώτο μέρος υλοποιείται η ομάδα $\mathrm{PSL}(r, q^d)$ ως ομάδα του Galois regular καλύμματος του $\mathbf{P}^1_{\mathbf{F}_q}$, για $\gcd(r, q^d) = 2$ και έγινε σε συνεργασία με τον Gunther Cornelissen.[1] Στο δεύτερο μέρος υπολογίζονται οι modular αυτομορφισμοί των Drinfeld modular καμπύλων $X_1(\mathfrak{n})$.

Το κεντρικό θέμα του αντιστρόφου προβλήματος της θεωρίας του Galois είναι η εύρεση, για δοσμένο σώμα k και ομάδα G, ενός πεπερασμένου, γεωμετρικά συνεκτικού καλύμματος $\mathcal{C}$ της προβολικής ευθείας $\mathbb{P}^1_k$ με ομάδα Galois την G.

Για $k = \mathbb{C}$ αναλυτικές και τοπολογικές μέθοδοι (Riemman existence theorem) δίνουν κατασκευαστικές λύσεις. Για κάθε τοπικό σώμα k μέθοδοι από την rigid ή την formal γεωμετρία απαντούν θετικά στο πρόβλημα ([18]).

Αντιθέτως, για ολικά (global) σώματα πολύ λίγα πράγματα είναι γνωστά. Η αδυναμία αυτή οφείλεται κατά κύριο λόγο στην ελλιπή γνώση των ιδιοτήτων των αριθμητικών θεμελιωδών ομάδων (arithmetic fundamentral groups). Στην περίπτωση του σώματος των ρητών αριθμών έχει αναπτυχθεί μία ποικιλία μεθόδων (rigidity

[1] cornelissen@math.uu.nl

method, Hurwitz spaces), μέσω των οποίων υλοποιήθηκαν ειδικές κατηγορίες ομάδων (σποραδικές, επιλύσιμες κτλ., δες [25] και [16]).

Ακόμα λιγότερα είναι γνωστά στη περίπτωση της θετικής χαρακτηριστικής. Για πεπερασμένα σώματα και για ομάδες με τάξη πρώτη ως προς τη χαρακτηριστική, για τις οποίες συμβαίνει να γνωρίζουμε ότι υλοποιούνται υπέρ το $\mathbb{Q}$, η μέθοδος της αναγωγής στη θετική χαρακτηριστική χρησιμοποιείται για την λύση του προβλήματος — αρκεί βέβαια τα αριθμητικά μοντέλα να είναι αρκετά καλά ($Wewers, Beckmann$). Στην modular περίπτωση, στην περίπτωση δηλαδή που η χαρακτηριστική διαιρεί την τάξη της ομάδας, ο Abhyankar ανέπτυξε κατασκευαστικές μεθόδους για λιγοστές ομάδες, δυστυχώς όμως, τα αντίστοιχα καλύμματα δεν ορίζονται πάντα πάνω από πρώτα σώματα.

Στην παρούσα εργασία παρουσιάζεται μία απόδειξη του θεωρήματος

Έστω q μία δύναμη του πρώτου p. Για κάθε ζεύγος αριθμών (s, d) με s περιττό, υπάρχει μία $\mathbf{F}_q$-regular Galois επέκταση με ομάδα Galois την $\mathrm{PSL(2s, q^d)}$.

Λίγα λόγια πάνω στην προϊστορία του ζητήματος: Έστω $K = \mathbf{F}_q(T)$. Είναι γνωστό ότι η γενική γραμμική ομάδα $\mathrm{GL(m, q^n)}$ (και á fortiori η προβολική της εκδοχή) υλοποιείται ως ομάδα του Galois υπέρ το K, αφού είναι η εικόνα της Galois αναπαράστασης $\rho_{\mathfrak{p}}$ των $\mathfrak{p}$-torsion σημείων ενός generic Drinfeld module τάξεως r, με $\mathfrak{p}$ ανάγωγο βαθμού n στο $\mathbf{F}_q[T]$ ([7]). Ο Abhyankar και οι συνεργάτες του έδειξαν το ίδιο αποτέλεσμα με στοιχειώδη εργαλεία ([2],[1]). Από την άλλη μεριά, ο K.-Y. Shih έχει αποδείξει την υλοποίηση (υπό συνθήκες) των ομάδων $\mathrm{PSL}(2, p)$ ως ομάδων του Galois υπέρ το $\mathbb{Q}$ κάνοντας χρήση της θεωρίας των modular καμπύλων και αναπαριστώντας την απόλυτη ομάδα του Galois σε ομάδα μετασχηματισμών σημείων πεπερασμένης τάξεως κατάλληλης ελλειπτικής καμπύλης. (Το πρόβλημα, στη γενικότητά του, λύθηκε αργότερα από τους Malle και Matzat με χρήση rigid μεθόδων [25]).

Η προσέγγιση που εδώ ακολουθείται είναι ένας συνδυασμός των δύο παραπάνω τεχνικών. Μελετάται μία twisted εκδοχή του moduli space των Drinfeld modules τάξεως $2s$ με κατάλληλη level structure. Τα σημεία διαφοροποίησης από την θεωρία του Shih εντοπίζονται κυρίως στα ακόλουθα: (α) γίνεται χρήση πολυδιάστατων varieties και έτσι προβλήματα «ρητότητας» των moduli χώρων γίνονται δυσκολότερα και (β) δεν υπάρχει Weil pairing στη κατηγορία των Drinfeld modules.

Αρχικά μελετάται το moduli scheme των Drinfeld modules τάξεως $2s$ με μία full flag υποομάδων των T–ρητών σημείων. Δίνεται ακριβής περιγραφή αυτού του αντικειμένου. Έστω L το σώμα των σταθερών της $\det(\rho)_{\mathfrak{p}}$, όπου $\rho_{\mathfrak{p}}$ είναι η προαναφερόμενη αναπαράσταση. Ορίζουμε $\tilde{Y}^{2s}$ ως το πηλίκο της $Y_0^{2s}(T) \times_K L$ με την $\mathrm{Gal(L/K)} \times \langle \mathrm{w} \rangle$, όπου ο w είναι μία involution τύπου Atkin-Lehner. Η δράση της w στο Y^{2s} περιγράφεται λεπτομερώς. Στη συνέχεια δείχνεται ότι το σώμα συναρτήσεων του $\tilde{Y}^{2s}$ είναι ρητό, αποδεικνύοντας ότι μία naive συμπαγοποίηση του είναι Brauer-Severi. Στο δεύτερο μέρος, ορίζεται μία Galois αναπαράσταση για κάθε K–ρητό σημείο του $\tilde{Y}^{2s}$. Τελικά, για κάθε τέτοιο σημείο και για κατάλληλο $\mathfrak{p} \in \mathbf{F}_q[T]$ υπάρχει μία αναπαράσταση

$$\rho\colon \mathrm{Gal}(\bar{K}/K) \longrightarrow \mathrm{PSL}(2s, \mathbf{F}_q[T])/\mathfrak{p},$$

με την προϋπόθεση ότι ένας συγκεκριμένος χαρακτήρας είναι τετριμμένος. Υπολογίζουμε τον χαρακτήρα αυτόν χρησιμοποιώντας το wedge γινόμενο στην κατηγορία των t-motives.

Στο δεύτερο μέρος υπολογίζονται οι modular αυτομορφισμοί των Drinfeld modular καμπύλων $X_1(\mathfrak{n})$. Εδώ με $Y_1(\mathfrak{n})$ συμβολίζουμε τον rigid αναλυτικό χώρο που αντιστοιχεί στον (γεωμετρικό) χώρο ταξινόμησης (moduli space) των Drinfeld modules με $\Gamma_1(\mathfrak{n})$-level structure και με $X_1(\mathfrak{n})$ τόσο την αναλυτική συμπαγοποίησή του όσο και την προβολική καμπύλη που αντιστοιχεί σε αυτόν.

Οι καμπύλες $X_1(\mathfrak{n})$ έχουν κεντρικό ρόλο στη θεωρία κωδίκων, αφού

- η κατασκευή επίπεδων μοντέλων είναι σχετικά εύκολη και
- έχουν πολλά K_+-ρητά σημεία.

Έτσι το ερώτημα για το ποια είναι η ομάδα των modular αυτομορφισμών (δηλαδή των αυτομορφισμών της $Y_1(\mathfrak{n})$ που επεκτείνονται σε αυτομορφισμούς της προβολικής καμπύλης) είναι εύλογο και ουσιαστικό.

Η προσέγγιση στο πρόβλημα είναι ανάλογη της κλασικής, με την έννοια ότι γίνεται μία συστηματική ανάλυση πάνω στη δράση της προβολικής ομάδας στο «άνω Drinfeld ημιεπίπεδο» $\Omega = \mathrm{P}^1_{\mathbf{C}} \setminus \mathrm{P}^1_{K_\infty}$. Πιο συγκεκριμένα, αποδεικνύεται το θεώρημα:

Η ομάδα των modular αυτομορφισμών της $X_1(\mathfrak{n})$ είναι ισόμορφη προς:

1. *Την ομάδα $(\mathrm{A}/\mathfrak{n})^*/\mathbf{F}_q^* \rtimes (\mathbb{Z}/2\mathbb{Z})$, αν $q \geq 3$*

2. *Μία επέκταση της $(\mathrm{A}/\mathfrak{n})^*/\mathbf{F}_q^*$ με την $(\mathbb{Z}/2\mathbb{Z})^n$, αν $q = 2$ και $\varphi(\mathfrak{n}) \geq 2$, όπου το n συμβολίζει τον αριθμό των διαφορετικών πρώτων διαιρετών του $\mathfrak{n}$*

3 . *Την ομάδα $(\mathbb{Z}/2\mathbb{Z})^n$, αν $q = 2$ και $\varphi(\mathfrak{n}) = 1$, όπου το n συμβολίζει τον αριθμό των διαφορετικών πρώτων διαιρετών του $\mathfrak{n}$ και $n = 1$ ή 2.*

Έστω q δύναμη πρώτου, $A = \mathbf{F}_q[T]$ ο πολυωνυμικός δακτύλιος μίας μεταβλητής T και $K = \mathbf{F}_q(T)$ το αντίστοιχο σώμα κλασμάτων. Στο K ορίζεται η μετρική $|a/b| = q^{\deg a - \deg b}$. Η πλήρωση του K σε σχέση με την μετρική αυτή είναι το σώμα των σειρών Laurent $K_\infty = \mathbf{F}_q((1/T))$. Έστω $\mathbf{C}$ η πλήρωση της αλγεβρικής κλειστότητας του K_∞. Το $\mathbf{C}$ εφοδιασμένο με την $p-$αδική τοπολογία έχει διαφορετικές από το σώμα των (κλασικών) μιγαδικών αριθμών $\mathbb{C}$ ιδιότητες. Για παράδειγμα οι Cauchy μη μηδενικές ακολουθίες είναι τελικά σταθερές, το $\mathbf{C}$ ως τοπολογικός χώρος είναι πουθενά συμπαγής, η επέκταση σωμάτων $\mathbf{C}/K_\infty$ είναι άπειρη σε αντιδιαστολή με την επέκταση $\mathbb{C}/\mathbb{R}$ η οποία είναι πεπερασμένη και μάλιστα δείκτη δύο, οι ακέραια ολόμορφες συναρτήσεις (entire functions) στο $\mathbf{C}$ δεν είναι κατ'ανάγκη σταθερές. Μάλιστα το σύνολο των ριζών των ή είναι κενό ή σχηματίζει ένα $A-$lattice Λ — τέτοιες συναρτήσεις είναι $\mathbf{F}_q$-γραμμικές και Λ-περιοδικές και απαντώνται στη σχετική βιβλιογραφία ως εκθετικές.

Στην κλασική περίπτωση έχει γίνει αρκετή δουλειά αναφορικά με το πρόβλημα υπολογισμού του κανονικοποιητή congruence υποομάδων της $\mathrm{SL}(2,\mathbb{Z})$ στην $\mathrm{PSL}(2,\mathbb{R})$. Ως παράδειγμα αναφέρουμε την εργασία [3] στην οποία υπολογίζεται ο κανονικοποιτής της κλασικής $\Gamma_0(N)$ και την [24] όπου υπολογίζεται ο κανονικοποιητής της $\Gamma_1(N)$. Σε ότι αφορά τις Drinfeld modular καμπύλες, ο A. Schweizer στο [29] υπολογίζει την ομάδα των modular αυτομορφισμών της modular $X_0(\mathfrak{n})$ για κάθε $\mathfrak{n}$.

Το πρόβλημα εύρεσης μεθόδου ικανής να δουλέψει για κάθε congruence υποομάδα παραμένει — τόσο στην κλασική όσο και στην Drinfeld modular περίπτωση — μέχρι στιγμής αναπάντητο.

Θα ήθελα να ευχαριστήσω τον επιβλέποντα καθηγητή κ. Γιάννη Αντωνιαδη για την βοήθεια που μου πρόσφερε σε όλη την διάρκεια των μεταπτυχιακών σπουδών μου. Επίσης θα ήθελα να ευχαριστήσω τον συνεργάτη μου κ. Gunther Cornelissen για την πολύτιμη βοήθεια του στην ολοκλήρωση της μελέτης σχετικά με την υλοποίηση των ομάδων PSL πάνω απο το $\mathbf{F}_p$. Ευχαριστώ επίσης το Ίδρυμα Κρατικών Υποτροφιών του οποίου υπήρξα υπότροφος.

Ευχαριστώ ιδιαίτερα τους γονείς μου Γιάννη και Ελένη και τις αδελφές μου Χαρά, Αθηνά και Γεωργία για την ηθική και οικονομική τους συμπαράσταση κατά την διάρκεια των σπουδών μου. Τέλος θα ήθελα να ευχαριστήσω τους φίλους μου Αριστείδη και Δημήτρη για την ηθική τους συμπαράσταση.

Ρέθυμνο 15 Ιανουαρίου 2003

Μαρίνα Τριπολιτάκη

Ελλειπτικες καμπυλες

Κρίνεται σκόπιμο να παρατεθούν ορισμοί και θεωρήματα από τη θεωρία των ελλειπτικών καμπύλων ώστε να γίνει σαφής η σχέση αντιστοιχίας μεταξύ της θεωρίας αυτής και της θεωρίας των Drinfeld modules. Στις μέρες μας έχει γίνει φανερό ότι τα εργαλεία που προσφέρει η θεωρία των Drinfeld modules είναι τα «φυσικά» εργαλεία της θετικής χαρακτηριστικής. Θεωρίες που ο Drinfeld ανέπτυξε εφαρμόστηκαν στην συνέχεια στις ελλειπτικές καμπύλες —όπως για παράδειγμα η θεμελίωση της έννοιας της level structure που νωρίτερα παρουσίαζε προβλήματα στις ίνες που την «τέμνουν». Πιο συγγεκριμένα, αν με $Y(N)$ συμβολίσουμε το moduli scheme των ελλειπτικών καμπύλων πάνω από το $\mathbb{Q}$ με $N-$level structure, τότε αυτό ορίζει ένα moduli scheme πάνω από το $\mathbb{Z}[1/N]$, αλλά μόνο μετά τον Drinfeld το scheme μπόρεσε να οριστεί και πάνω από το $\mathbb{Z}$ (τουλάχιστο για «μεγάλο N»).

1.1 Ορισμοί

Έστω ω_1, ω_2 δύο μη-μηδενικοί μιγαδικοί αριθμοί με $\tau = \omega_1/\omega_2$ μη πραγματικό. Χωρίς βλάβη της γενικότητας υποθέτουμε ότι τ ανήκει στο πάνω ημιεπίπεδο H. Το δικτυωτό (lattice)

$$\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$$

είναι $\mathbb{Z}$-ελεύθερο τάξεως 2 και το πηλίκο $\mathbb{C}/\Lambda$ δέχεται τη δομή επιφάνειας Riemann γένους 1, η οποία μέσω του θεωρήματος ύπαρξης του Riemman (Riemman existence theorem, ή αλλιώς αναλυτική gaga)([16], §11.3) αντιστοιχεί σε μία μη ιδιόμορφη, ανάγωγη προβολική καμπύλη γένους 1 (nonsingular, irreducible curve of genus 1), δηλαδή σε μία ελλειπτική καμπύλη. [1]

Ορισμος 1.1.1. *Έστω k σώμα. Μία ελλειπτική καμπύλη υπέρ το k είναι μία γεωμετρικά συνεκτική, μη ιδιόμορφη προβολική καμπύλη γένους 1, μαζί με ένα k-ρητό σημείο.*

Αξίζει να σημειωθεί ότι οι μη-ιδιόμορφες, γεωμετρικά συνεκτικές καμύλες γένους ένα υπέρ το k είναι ελλειπτικές πάνω από μια πεπερασμένη επέκτασή του.

Κάθε ελλειπτική καμπύλη E_k δέχεται τη δομή αβελιανής ομάδας. Έστω L σώμα με $L \supset k$. Με $E(L)$ θα συμβολίζουμε το σύνολο των L-ρητών σημείων της E, δηλαδή το σύνολο των μορφισμών $\mathrm{Spec}(L) \longrightarrow E$. Έστω N φυσικός αριθμός. Η ομάδα Galois $\mathrm{Gal}(L^{alg}/L)$ δρα στα N-σημεία πεπερασμένης τάξης της E και ορίζει μία αναπαράσταση $\mathrm{Gal}(L^{alg}/L) \longrightarrow E(L)$, όπου L^{alg} η αλγεβρική θήκη του L.

Ορισμος 1.1.2. *Έστω A δακτύλιος. Θεωρούμε το σύνολο των πρώτων ιδεωδών του A — συμβολικά $\mathrm{Spec}(A)$. Στο $\mathrm{Spec}(A)$ βάζουμε μία δομή συναρτήσεων: για κάθε $P \in \mathrm{Spec}(A)$ ορίζουμε το φύτρο (stalk) των συναρτήσεων του P ως το δακτύλιο A_P. Μία βάση κλειστών συνόλων του $\mathrm{Spec}(A)$ αποτελούν τα σύνολα $V(I) := \{Q \colon Q \in \mathrm{Spec}(A), Q \supset I\}$ με I ιδεώδες του A. Σε κάθε ανοιχτό $U \subset \mathrm{Spec}(A)$ αντιστοιχούμε το «σύνολο συναρτήσεων»*

$$\mathcal{O}_{\mathrm{Spec}(A)}(U) := \mathrm{invlim}_{P \in U} A_P.$$

Για παράδειγμα, αν ο A είναι ακέραια περιοχή, τότε $\mathcal{O}_{\mathrm{Spec}(A)}(U) := \cap_{P \in U} A_P$. Το σύνολο $\mathrm{Spec}(A)$, μαζί με τη δομή συναρτήσεων, ονομάζεται αφινικό scheme.

Για ένα πιο γενικό ορισμό της έννοιας του scheme, καθώς και διάφορων εννοιών που απαιτούνται σε αυτόν (π.χ separable pre-scheme) δες [20] κεφ. 2.

[1] Ως τοπολογικός χώρος (χωρίς αναλυτική δομή) το $\mathbb{C}/\Lambda$ είναι ισόμορφο προς το $(\mathbb{R}/\mathbb{Z})^2$.

Θυμίζουμε ότι ένας συναρτητής (functor) από μία κατηγορία A σε μία κατηγορία B είναι κάθε απεικόνιση από την A στην B που σέβεται τις δομές, δηλαδή κάθε απεικόνιση που σε κάθε αντικείμενο (object) (σε κάθε μορφισμό αντικειμένων της A) αντιστοιχεί ένα αντικείμενο της B (μορφισμό αντιμειμένων της B), έτσι ώστε, ο ταυτοτικός μορφισμός να απεικονίζεται στον ταυτοτικό και η σύνθεση δύο (οποιωνδήποτε) μορφισμών της A να απεικονίζεται στην σύνθεση των εικόνων των μορφισμών.

Ορισμος 1.1.3. *Έστω A, B δακτύλιοι θετικής χαρακτηριστικής και $\gamma\colon A \longrightarrow B$ ομομορφισμός. Ένα scheme M μαζί με ένα φυσικό μετασχηματισμό Ψ_M από ένα συναρτητή (functor) F στον συναρτητή των σημείων Mor_M του M θα λέγεται* coarse moduli scheme *για τον functor* F *αν*

- *η απεικόνιση $\Psi_{\mathrm{Spec}(K)}\colon \mathrm{F}(\mathrm{Spec}(K)) \longrightarrow M(K) = \mathrm{Mor}(\mathrm{Spec}(K), M)$ είναι συνολοθεωτητικός ισομορφισμός*
- *για κάθε άλλο scheme M' και φυσικό μετασχηματισμό $\Psi_{M'}\colon \mathrm{F} \longrightarrow \mathrm{Mor}_{M'}$, υπάρχει μοναδικός μορφισμός $\pi\colon M \longrightarrow M'$ έτσι ώστε ο επαγόμενος φυσικός μετασχηματισμός $\Pi\colon \mathrm{Mor}_M \longrightarrow \mathrm{Mor}_{M'}$ να ικανοποεί τη σχέση $\Psi_{M'} = \Pi \circ \Psi_M$.*

Λέμε ότι ο functor F είναι αναπαραστάσιμος (representable) από το M, αν ισχύουν τα παραπάνω και επιπλέον ο Ψ είναι ισομορφισμός μεταξύ *του F και του functor των σημείων του M.*

Τυπικό παράδειγμα μη αναπαραστάσιμου moduli scheme είναι το moduli scheme $\mathcal{M}_g$ των καμπύλων γένους $g > 2$ (υπάρχουν καμπύλες με μη τετριμμένους αυτομορφισμούς). Στα παρακάτω θα συναντήσουμε παραδείγματα αναπαραστάσιμων και μη moduli schemes. Ο αναγνώστης θα βρει το βιβλίο [19] πολύ κατατοπιστικό.

1.2 Modular καμπύλες

1.2.1 Η καμπύλη $Y_0(N)$

Έστω N φυσικός αριθμός και E_k, E'_k ελλειπτικές καμπύλες. Έστω L σώμα με $L \supset k$ και $C \leq E_k(L), C' \leq E'_k(L)$ κυκλικές υποομάδες τάξης N. Ένας ισομορφισμός από το (E, C) στο (E', C') είναι ένας ισομορφισμός ελλειπτικών καμπύλων $E \longrightarrow E'$ που απεικονίζει την C στην C'.

Οι ορισμοί αυτοί μπορούν να επεκταθούν με φυσικό τρόπο στην κατηγορία των ελλειπτικών καμπύλων πάνω από varieties ή schemes.

Ορισμος 1.2.1. *Έστω S ένα $k-$ scheme. Ορίζουμε $\mathcal{E}_{0,N}(S)$ ως το σύνολο των κλάσεων ισομορφίας των ζευγών (E, C), όπου E είναι μία ελλειπτική καμπύλη υπέρ το S και C μία κυκλική υποομάδα της E τάξεως N. Ο contravariant functor*

$$\mathcal{Y}_0(N)\colon \left\{ \begin{array}{c} k-\mathrm{schemes} \\ S \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \text{κλάσεις ισομορφίας ζευγών} \\ (E, C) \ \textit{υπέρ το } S \end{array} \right\}$$

ορίζει ένα coarse moduli πρόβλημα. Με $Y_0(N)$ θα συμβολίζουμε το coarse moduli scheme που αντιστοιχεί στον $\mathcal{Y}_0(N)$.

Στο [23] περιγράφονται τα moduli schemes των ελλειπτικών καμπύλων με κάθε δυνατή λεπτομέρεια.

1.2.2 Η καμπύλη $Y(N)$

Έστω N θετικός ακέραιος, $\zeta_N \in \mathbb{C}$ μία πρωταρχική $N-$ ρίζα της μονάδος και k τέλειο σώμα χαρακτηριστικής $p \geq 0$, με $p \not| N$ και $E \longrightarrow \mathrm{Spec}(k)$ ελλειπτική καμπύλη. Πάνω από την αλγεβρική κλειστότητα k^{alg} του k, το σύνολο των N-torsion σημείων της ελλειπτικής καμπύλης $E(k^{alg})_N$, σχηματίζει μία ομάδα τάξεως N^2 ισόμορφη προς την $\mathbb{Z}/N \times \mathbb{Z}/N$.

Έστω K σώμα με $K \supset k$. Μία $N-$level structure ορισμένη πάνω από το K για την ελλειπτική καμπύλη E αποτελείται από

- μία $\mathbb{Z}/N$-βάση N-torsion σημείων $E(K)_N \subset K$ της E,

- ένα $\mathbb{Z}$ module ισομορφισμό
$$i_N : E(K)_N \longrightarrow (\mathbb{Z}/N)^2$$
- και ένα ισομορφισμό (γνωστό ως Weil pairing)
$$e_N : \wedge^2 E(K)_N \longrightarrow \langle \zeta_N \rangle$$

με ζ_N μία πρωταρχική N-ρίζα της μονάδας.

Δύο ζεύγη $(E_i, i_N), i = 1, 2$ είναι ισόμορφα, αν υπάρχει ισομορφισμός ελλειπτικών καμπύλων $\pi : E_1 \longrightarrow E_2$ ώστε το ακόλουθο διάγραμμα να είναι αντιμεταθετικό

$$\begin{tikzcd} E_1(k)_N \arrow[rr, "\pi"] \arrow[dr, "i_{1N}"'] & \arrow[d, phantom, "="] & E_2(k)_N \arrow[dl, "i_{2N}"] \\ & (\mathbb{Z}/N)^2 & \end{tikzcd}$$

Για κάθε $k-$ scheme S, με $\mathcal{E}_N(S)$ θα συμβολίζουμε το σύνολο των κλάσεων ισομορφίας των ζευγαριών (E, i_N), όπου E είναι μία ελλειπτική καμπύλη υπέρ το S και i_N μία $N-$level stucture της E. Ο contravariant functor
$$\mathcal{Y}(N) \colon \left\{ \begin{array}{c} k-\text{schemes} \\ S \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \text{κλάσεις ισομορφίας ζευγών} \\ (E, i_N) \text{ υπέρ το } S \end{array} \right\}$$
ορίζει ένα moduli πρόβλημα το οποίο είναι αναπαραστάσιμο (representable) από ένα $k-$ scheme $Y(N)$ (για $N > 3$).

Drinfeld modules

Το κεφάλαιο αυτό αποτελεί μία μικρή εισαγωγή στις βασικές έννοιες που θα συναντήσουμε παρακάτω. Κύριες πηγές της αναφοράς αυτής είναι το βιβλίο του Gekeler «Drinfeld Modular Curves» [12], το βιβλίο του Goss «The Arithmetic of Function Fields» [13], οι διαλέξεις του συνεδρίου «Drinfeld modules, Drinfeld modular schemes and applications» [11] καθώς επίσης και το ερευνητικό άρθρο του Gekeler [10]. Τέλος μία ικανοποιητική εισαγωγή στη σύγχρονη γλώσσα της Αλγεβρικής Γεωμετρίας αποτελεί το κλασικό βιβλίο του Hartshorne «Algebraic Geometry» [20].

2.1 Ορισμοί

Προσθετικά (additive) group schemes

Έστω B αντιμεταθετικός δακτύλιος πεπερασμένης χαρακτηριστικής p. Το προσθετικό (additive) group scheme υπέρ το B, το οποίο σημειώνεται με $\mathbb{G}_{a,B}$ ή $\mathbb{G}_a$ για συντομία, είναι εξ ορισμού το αφινικό scheme $\mathrm{Spec}(B[T])$ μαζί με ένα «νόμο πολλαπλασιασμού»

$$\mathbb{G}_a \times \mathbb{G}_a \longrightarrow \mathbb{G}_a$$

ο οποίος επάγεται από τον $B-$ ομομορφισμό

$$B[T] \longrightarrow B[T] \otimes_B B[T], \qquad T \longmapsto T \otimes 1 + 1 \otimes T.$$

Το ουδέτερο στοιχείο του $\mathbb{G}_a$ και η αντιστροφή στο $\mathbb{G}_a$ επάγονται αντίστοιχα από τους ενδομορφισμούς

$$f_e : B[T] \longrightarrow B[T], \qquad T \longmapsto eT \text{ για } e = 0 \text{ και } e = -1.$$

Κάθε μορφισμός $\beta : \mathbb{G}_{a,B} \longrightarrow \mathbb{G}_{a,B}$ επάγεται από ένα ενδομορφισμό $b : B[T] \longrightarrow B[T]$, ο οποίος με τη σειρά του καθορίζεται από την εικόνα $b(T)$ του T. Ο μορφισμός b είναι ένας group-scheme ενδομορφισμός, αν και μόνο αν

$$b(T \otimes 1 + 1 \otimes T) = b(T \otimes 1) + b(1 \otimes T).$$

Σημείωση 1. Για B άπειρο δακτύλιο End $\mathbb{G}_a = \{\sum_{i=0}^{n} b_i \tau^i : n \in \mathbb{N}, b_i \in B\}$. Ο δακτύλιος των ενδομορφισμών $\mathrm{End}_B(\mathbb{G}_a)$, είναι μη-αντιμεταθετικός ($\forall a \in L, \tau \circ a = a^p \circ \tau$) και παράγεται από τον Frobenious ενδομορφισμό

$$\tau : B \longrightarrow B \ \ ; \ \ x \longmapsto x^p.$$

Γενικότερα με τ^i θα συμβολίζουμε τον ομομορφισμό $x \longmapsto x^{p^i}$. Δίνοντας έμφαση στον γεννοποιό δακτύλιο B γράφουμε $\mathrm{End}_B(\mathbb{G}_a) = B\{\tau\}$.

Αν $B = L$ σώμα τότε σε κάθε ενδομορφισμό $f = f(\tau) \in L\{\tau\}$ αντιστοιχεί ένα πολυώνυμο στην μεταβλητή X (συμβολικά το $f(X)$) το οποίο προκύπτει από το $f(\tau)$ με αντικατάσταση του τ^i με X^{p^i} για κάθε i.

Ορισμος 2.1.1. *Έστω A, B δακτύλιοι θετικής χαρακτηριστικής και $\gamma \colon A \longrightarrow B$ ομομορφισμός. Η A-χαρακτηριστική του B είναι εξ ορισμού ο πυρήνας του γ. Λέμε ότι ο B είναι γενικής χαρακτηριστικής ή ότι η χαρακτηριστική του είναι ∞, αν ο γ είναι μονομορφισμός.*

Drinfeld modules και ισογένιες

Ορισμος 2.1.2. *Ένα Drinfeld module υπέρ το B τάξεως $r \in \mathbb{N}$ είναι ένας μονομορφισμός δακτυλίων*

$$\phi : A \longrightarrow \mathrm{End}_B(\mathbb{G}_a) \ ; \ \ \mathfrak{n} \longmapsto \phi_{\mathfrak{n}}$$

τέτοιος ώστε, για κάθε $\mathfrak{n} \in A$

1. $\deg \phi_{\mathfrak{n}} = r \cdot \deg \mathfrak{n}$, *και*
2. $\frac{\partial}{\partial \tau}(\phi_{\mathfrak{n}}) = \gamma(\mathfrak{n})$ *όπου $\frac{\partial}{\partial \tau}$ συμβολίζει τη διαφόριση ως προς τ.*

Μέσω του ϕ το προσθετικό group scheme $\mathbb{G}_{a,B}$ γίνεται scheme από A modules.

Ορισμος 2.1.3. *Έστω ϕ και ψ Drinfeld modules υπέρ το L. Ένας* μορφισμός *$u : \phi \longrightarrow \psi$ είναι ένα $u \in \mathrm{End_B}(\mathbb{G}_\mathrm{a})$ τέτοιο ώστε για όλα τα $\mathfrak{n} \in A$ το ακόλουθο διάγραμμα είναι αντιμεταθετικό:*

$$\begin{tikzcd}
\mathbb{G}_a \arrow[r, "u"] \arrow[d, "\phi_{\mathfrak{n}}"'] \arrow[dr, phantom, "="] & \mathbb{G}_a \arrow[d, "\psi_{\mathfrak{n}}"] \\
\mathbb{G}_a \arrow[r, "u"] & \mathbb{G}_a .
\end{tikzcd}$$

Μη τετριμμένοι μορφισμοί υπάρχουν μόνο μεταξύ Drinfeld modules ίδιας τάξεως και ονομάζονται ισογένιες.

Ορισμος 2.1.4. *Έστω X μία λεία, γεωμετρικά συνεκτική, προβολική καμπύλη υπέρ το $\mathbf{F}_q$. Επιλέγουμε ένα κλειστό (αλλά όχι απαραίτητα $\mathbf{F}_q$—ρητό) σημείο της X —το οποίο και θα συμβολίζουμε με ∞. Ο δακτύλιος $A := \Gamma(X \setminus \{\infty\}, \mathcal{O}_X) = \cap_{P \in X \setminus \infty} \mathcal{O}_P$ ονομάζεται δακτύλιος του Drinfeld (εδώ το $\mathcal{O}_P$ δεν είναι παρά το φύτρο συναρτήσεων —stack— του P).*

Παράδειγμα 2.1.1. Αν $X = \mathbb{P}^1_{\mathbf{F}_q}$ — ο προβολικός χώρος υπέρ το $\mathbf{F}_q$ και ∞ το (σύνηθες) επάπειρο σημείο τότε $A = \mathbf{F}_q[T]$.

Συμβολισμός 1. Με $\mathcal{Y}^r(1)(L)$ συμβολίζουμε το σύνολο των κλάσεων ισομορφίας των Drinfeld modules τάξεως r υπέρ το L.

Παράδειγμα 2.1.2. Έστω $A = \mathbf{F}_q[T]$ όπως στο παράδειγμα 2.1.1, και έστω $K = \mathbf{F}_q(T)$ το σώμα κλασμάτων. Το να ορίσει κανείς ένα Drinfeld module ϕ υπέρ το K ή πάνω από μία επέκταση L του K, είναι ισοδύναμο με το να ορίσει το προσθετικό πολυώνυμο $\phi_T = T + c_1\tau + \cdots + c_r\tau^r \in L\{\tau\}$ όπου $c_r \neq 0$ και $r = \mathrm{rank}(\phi)$. Ένα Carlitz module είναι ένα Drinfeld module τάξεως ένα, δηλαδή της μορφής $\phi_T = T + \alpha\tau, \alpha \in K$. Δύο Drinfeld modules ϕ και ϕ' είναι ισόμορφα πάνω από την αλγεβρική κλειστότητα L^{alg} του L αν και μόνο αν υπάρχει $u \in L^{\mathrm{alg}} \setminus 0$ τέτοιο ώστε $y'_i = u^{q^i-1}y_i$ για όλα τα $i \geq 1$. Άρα το $\mathcal{Y}^r(1)(L^{\mathrm{alg}})$ μπορεί να περιγραφεί (για $r \geq 1$) ως ένα ανοιχτό, πυκνό subscheme του $(r-1)$—διάστατου προβολικού χώρου με βάρη (weighted) υπέρ το L^{alg}.

2.2 Σημεία πεπερασμένης τάξης

Ένα finite flat group scheme G πάνω από ένα scheme S είναι ένας μορφισμός $\pi : G \longrightarrow S$ μαζί με τους με τους μορφισμούς πράξεως, ώστε η π να είναι finite, flat, και μάλιστα, τοπικά, πάνω από κάθε ανοιχτό αφινικό $\mathrm{Spec}(A) \subset S$ το $\pi^{-1}(\mathrm{Spec}(A)) \cong \prod_{i=i}^r \mathrm{Spec}(B)$, με $\mathrm{Spec}(B) \longrightarrow \mathrm{Spec}(A)$ finite και flat, για $r \in \mathbb{N}$.

Ορισμος 2.2.1. *Έστω $a \in A$ και ϕ ένα Drinfeld module υπέρ το L. Με $\phi[a]$ συμβολίζουμε το subscheme των a—torsion σημείων του $\mathbb{G}_{a,L}$ εφοδιασμένο με την επαγόμενη A—module δομή. Έτσι για κάθε L—άλγεβρα M*

$$\phi(M)[a] = \{x \in M : \phi_a(x) = 0\}.$$

Πιο γενικά, για $\mathfrak{a} \lhd A$ ιδεώδες, θέτουμε

$$\phi_{\mathfrak{a}} = \bigcap_{a \in \mathfrak{a}} \phi_a$$

για οποιοδήποτε (και όχι απαραίτητα κύριο) ιδεώδες $\mathfrak{a}$ του A. Το $\phi_{\mathfrak{a}}$ είναι ένα finite flat group scheme βαθμού $\mathrm{rank}(\phi) \cdot \deg(\mathfrak{a})$. *Η δομή του $\phi[\mathfrak{a}]$ θα περιγραφεί αναλυτικότερα στα παρακάτω.*

Θεωρία Κλάσεων Σωμάτων — Μία κατασκευαστική προσέγγιση

Τα σημεία πεπερασμένης τάξης των Drinfeld modules τάξεως ένα στην θετική χαρακτηριστική έχουν ιδιότητες ανάλογες με τις ρίζες της μονάδος. Οι n—οστές ρίζες της μονάδος ($p \nmid n$) ικανοποιούν την εξίσωση $x^n - 1 = 0$ και σχηματίζουν ένα $\mathbb{Z}$—module, έστω το M. Η δράση του $\mathbb{Z}$ στο M ορίζεται ως εξής: $\zeta \in M, n \in \mathbb{Z}$, $n * \zeta := \zeta^n$. Αν με $K(n)$ συμβολίσουμε το σώμα διάσπασης (splitting field) του πολυωνύμου $x^n - 1 = 0$, η επέκταση $K(n)/K$ είναι Galois με ομάδα Galois ισόμορφη προς την $(\mathbb{Z}/n)^*$. Η αντιστοιχία είναι σχεδόν πλήρης:

ΘΕΩΡΗΜΑ 2.2.1 ([7],[5]). *Έστω ϕ ένα Drinfeld module υπέρ το L τάξεως $r \geq 1$.*

1. *Αν* $\mathrm{char}_A(L) = \infty$ *τότε*

   (α΄) το $\phi_{\mathfrak{a}}$ είναι reduced (δηλ. χωρίς μηδενοδύναμα στοιχεία) για κάθε ιδεώδες $\mathfrak{a}$ του A,

   (β΄) $\phi[\mathfrak{a}](L^{\mathrm{sep}}) = \phi[\mathfrak{a}](L^{\mathrm{alg}})$ και

   (γ΄) $\phi[\mathfrak{a}](L^{\mathrm{alg}}) =: \phi[\mathfrak{a}] \sim (A/\mathfrak{a})^r$ ως A-modules.

2. *Αν $\mathfrak{p} = \mathrm{char}_A(L)$ είναι maximal ιδεώδες με $\gcd(\mathfrak{a}, \mathfrak{p},)$ τότε $\phi[\mathfrak{a}](L^{\mathrm{alg}}) \simeq (A/\mathfrak{a})^r$.*

Η απόλυτη ομάδα Galois $\mathrm{G_L}$ του L δρα στο $\phi[\mathfrak{a}](L^{\mathrm{sep}})$ μέσω A—γραμμικών αυτομορφισμών. Συνεπώς κάθε Drinfeld module επάγει μία Galois αναπαράσταση στα torsion σημεία του.

Τα παραπάνω συνοψίζονται στα θεωρήματα των Carlitz και Hayes ([21]):

ΘΕΩΡΗΜΑ 2.2.2. *Έστω A ο πολυωνυμικός δακτύλιος $\mathbf{F}_q[T]$ με σώμα κλασμάτων το K. Έστω $\rho\colon A \longrightarrow K\{\tau\}$ το Carlitz module $\rho_T = T + \tau$. Για κάθε μη τετριμμένο ιδεώδες $\mathfrak{a} \lhd A$ έστω $K(\mathfrak{a}) := K(\rho[\mathfrak{a}](K^{alg}))$ η επέκταση του K που γεννιέται από τα $\mathfrak{a}$-torsion σημεία του.*

1. *η $K(\mathfrak{a})/K$ είναι αβελιανή επέκταση του Galois με ομάδα Galois ισόμορφη προς την $(A/\mathfrak{a})^*$. Έστω $\sigma_{\mathfrak{b}}$ ο αυτομορφισμός που αντιστοιχεί στην κλάση του $\mathfrak{b} \bmod \mathfrak{a}$. Τότε $\forall x \in \rho[\mathfrak{a}](K^{\mathrm{alg}})$, $\sigma_{\mathfrak{b}}(x) = \rho_{\mathfrak{b}}(x)$.*

2. *Αν το $\mathfrak{a} = \mathfrak{p}^n$ είναι primary με $\mathfrak{p}$ πρώτο ιδεώδες τότε η επέκταση $K(\mathfrak{a})/K$ είναι πλήρως διακλαδιζόμενη στο $\mathfrak{p}$ και αδιακλάδιστη σε όλες τις άλλες πεπερασμένες θέσεις.*

3. *Αν το $\mathfrak{a} = \prod_{i=1}^{s} \mathfrak{a}_i$ είναι γινόμενο πρώτων ανά δύο ιδεωδών $\mathfrak{a}_i$ του A, τα σώματα $K(\mathfrak{a}_i)$ είναι γραμμικά διαφορετικά (linearly disjoint) και $K = \bigotimes_{i=1}^{s} K(\mathfrak{a}_i)$.*

4. *Έστω $K_+(\mathfrak{a})$ το σώμα των σταθερών στοιχείων της ${\mathbf{F}_q}^* \leq (A/\mathfrak{a})^*$. Τότε το ∞ αναλύεται πλήρως στην επέκταση $K_+(\mathfrak{a})/K$ και διακλαδίζεται πλήρως στην $K(\mathfrak{a})/K_+(\mathfrak{a})$.*

5. *Έστω $\mathfrak{p} = \langle \pi \rangle$ πρώτο ιδεώδες και πρώτο ως προς το $\mathfrak{a}$. Κάτω από την ταύτιση $\mathrm{Gal}(K(\mathfrak{a})/K) = (A/\mathfrak{a})^*$ το Frobenius στοιχείο $\mathrm{Frob}_{\mathfrak{p}}$ είναι ίσο με την residue class του $\pi \bmod \mathfrak{a}$.*

Τα ιδεώδη του A (σε σχέση με την διαιρετότητα) σχηματίζουν ένα αντίστροφο σύστημα (inverse system). Με $K(\infty)$ συμβολίζουμε το σώμα που παράγεται πάνω από το K από τα σημεία πεπερασμένης τάξης του $\rho = T + \tau$. Η επέκταση $K(\infty)/K$ είναι Galois με ομάδα την $\mathrm{Gal}(K(\infty)/K) = \mathrm{invlim}_{\mathfrak{a}}\,(\mathrm{A}/\mathfrak{a})^*$, η οποία ταυτίζεται σχεδόν παντού με την πεπερασμένη κλάση των idele του K. Το $K(\infty)$ είναι η maximal αβελιανή επέκταση του K η οποία μάλιστα διακλαδίζεται ήμερα στο ∞. Το παραπάνω θεώρημα είναι το ανάλογο του κλασικού θεωρήματος των Kronecker-Weber στην χαρακτηριστική p. Η θεωρία των Drinfeld modules προσφέρει μία κατασκευαστική προσέγγιση στη θεωρία κλάσεων σωμάτων, όπου τα σημεία πεπερασμένης τάξης του Carlitz module παίζουν ρόλο ανάλογο με τις μιγαδικές ρίζες της μονάδας.

2.2.1 Η θεωρία του Weierstraß

Στα παρακάτω θα περιοριστούμε σε Dedekind δακτυλίους του Drinfeld της μορφής $\mathbf{F}_q[T]$.

Εισάγουμε τους συμβολισμούς:

$\mathbf{F}_q$	$=$	$\mathbf{F}_{p^m}$	Το σώμα χαρακτηριστικής p με q στοιχεία
$\mathbf{A}$	$=$	$\mathbf{F}_q[T]$	Ο δακτύλιος των πολυωνύμων υπέρ το $\mathbf{F}_q$
K	$=$	$\mathbf{F}_q(T)$	Το σώμα πηλίκων του A. Το $\infty = \frac{1}{T}$ ορίζει την p-αδική εκτίμηση v_∞ με $v_\infty(\frac{1}{T}) = 1$
K_∞	$=$	$\mathbf{F}_q((\frac{1}{T}))$	Η πλήρωση του K σε σχέση με την v_∞. Έστω $\mathcal{O}_\infty = \{x \in K_\infty \vert w_\infty(q) \geq 0\}$, w_∞ επέκταση του v_∞, δηλαδή $K_\infty = \{\sum_{i=m}^{\infty} \alpha_i \cdot (\frac{1}{T})^i \vert \alpha_i \in \mathbf{F}_q$, $i \in \mathbb{Z}$ και $i \geq m\}$ ενώ το $\mathcal{O}_\infty = \{\sum_{i=0}^{\infty} \alpha_i \cdot (\frac{1}{T})^i \vert \alpha_i \in \mathbf{F}_q, i \geq 0\}$
$\mathbf{C}$	$=$	$\hat{\bar{K}}_\infty$	Η πλήρωση της αλγεβρικής κλειστότητας του K_∞. Το $\mathbf{C}$ είναι επίσης αλγεβρικά κλειστό, και ο βαθμός επέκτασης $[C : K] = \infty$.
$\mathbf{\Omega}$	$=$	$\mathbf{C} \setminus K_\infty$	Το Drinfeld άνω ημιεπίπεδο.

Ορισμος 2.2.2. *Ένα lattice Λ τάξεως r του $\mathbf{C}$ (ή για συντομία ένα r-lattice) είναι ένα πεπερασμένα παραγόμενο (και άρα προβολικό, γιατί τα πεπερασμένα παραγόμενα modules πάνω από Dedekind δακτυλίους είναι προβολικά), διακριτό (κάθε μη κενή σφαίρα του $\mathbf{C}$ έχει πεπερασμένη τομή με το Λ — στην κλασική περίπτωση η ιδιότητα αυτή πηγάζει από τον ορισμό· εδώ απαιτείται) A-submodule Λ του $\mathbf{C}$ προβολικής τάξεως r. Αφού το Λ είναι πεπερασμένα παραγόμενο και προβολικό, για κάθε πρώτο ιδεώδες $\mathfrak{p}$ του A το $\Lambda_\mathfrak{p}$ πάνω από τον $A_\mathfrak{p}$, είναι ελεύθερο. Λόγω «συνεκτικότητας» του δακτυλίου A, η rank του ${}_{A_\mathfrak{p}}\Lambda_\mathfrak{p}$ είναι ανεξάρτητη από το $\mathfrak{p}$ — ο αριθμός αυτός ονομάζεται «προβολική τάξη του Λ».*

Η εκθετική συνάρτηση του Λ

Σε κάθε lattice Λ αντιστοιχούμε μία ολόμορφη συνάρτηση με ρίζες στα σημεία του Λ

$$e_\Lambda : \mathbf{C} \to \mathbf{C},$$

η οποία ορίζεται ως το γινόμενο

$$e_\Lambda(z) = z \prod_{0 \neq \lambda \in \Lambda} (1 - \frac{z}{\lambda}).$$

Είναι ακέραια, $\Lambda-$περιοδική και $\mathbf{F}_q-$γραμμική. Για κάθε μη μηδενική ρίζα $a \in A$ θεωρούμε το διάγραμμα

$$\begin{tikzcd} 0 \arrow[r] & \Lambda \arrow[r] \arrow[d, "a"] & \mathbf{C} \arrow[r, "e_\Lambda"] \arrow[d, "a"] & \mathbf{C} \arrow[r] \arrow[d, dotted, "\exists \phi_a^\Lambda"] & 0 \\ 0 \arrow[r] & \Lambda \arrow[r] & \mathbf{C} \arrow[r, "e_\Lambda"] & \mathbf{C} \arrow[r] & 0 \end{tikzcd}$$

Οι γραμμές είναι ακριβείς. Το αριστερό και το κάθετο μεσαίο βέλος δηλώνουν πολλαπλασιασμό με a. Αποδεικνύεται η ύπαρξη ενός προσθετικού πολυωνύμου ϕ_a^Λ —που εξαρτάται από τα a και Λ— ώστε το παραπάνω διάγραμμα να είναι αντιμεταθετικό. Μάλιστα, για κάθε $a, b \in \mathbf{A}, \phi_a^\Lambda \circ \phi_b^\Lambda = \phi_b^\Lambda \circ \phi_a^\Lambda = \phi_{ab}^\Lambda$. Συνοψίζοντας

1. $\phi_a^\Lambda \in \mathbf{C}\{\tau\}$,

2. $\deg_\tau(\phi_a^\Lambda) = r \cdot \deg(a)$,
3. η αντιστοιχία $a \mapsto \phi_a^\Lambda$ ορίζει ένα ομομορφισμό δακτυλίων, ο οποίος με τη σειρά του ορίζει ένα Drinfeld module τάξεως r.
4. Όλα τα Drinfeld modules υπέρ το $\mathbf{C}$ προκύπτουν με αυτόν τον τρόπο (δηλαδή αντιστοιχούν σε lattices).

Το παραπάνω συνοψίζονται στην πρόταση 3.1 του πρώτου άρθρου του Drinfeld ([7]).

ΘΕΩΡΗΜΑ 2.2.3. • *Κάθε Drinfeld module τάξεως r υπέρ το $\mathbf{C}$ προκύπτει από κάποιο r-lattice Λ του $\mathbf{C}$.*

• *Δύο Drinfeld modules ϕ^Λ, $\phi^{\Lambda'}$ είναι ισόμορφα, αν και μόνο αν, υπάρχει $0 \neq c \in \mathbf{C}$ τέτοιο ώστε $\Lambda' = c \cdot \Lambda$.*

Σημείωση 1. Ας γυρίσουμε στο παράδειγμα με τις ρίζες της μονάδας. Η κλασική εκθετική συνάρτηση exp : $\mathbb{C} \longrightarrow \mathbb{C}^* : z \longmapsto e^z$ είναι επιμορφισμός ομάδων με πυρήνα το $\Lambda := 2\pi i\mathbb{Z}$ — ένα $\mathbb{Z}-$lattice τάξεως ένα — τα μη μηδενικά στοιχεία του οποίου αντιστοιχούν στις ρίζες όλων των εξισώσεων της μορφής $x^n - 1 = 0$.

Σημείωση 2. (Ελλειπτικές καμπύλες). Κάθε ελλειπτική καμπύλη πάνω από τους μιγαδικούς αντιστοιχεί (κατά προσέγγιση ισομορφισμού) σε ένα $\mathbb{Z}$-lattice Λ τάξεως 2. Έστω $\wp_\Lambda$ η συνάρτηση Weierstraß του Λ. Η $\wp_\Lambda$ είναι ολόμορφη στο $\mathbb{C}$, Λ-περιοδική και μηδενική πάνω στο Λ.

2.2.2 Το Drinfeld άνω ημιεπίπεδο

Μπορούμε να περιγράψουμε το χώρο των $\mathbf{C}$-ρητών σημείων $\mathcal{Y}^r(1)(\mathbf{C})$ του $\mathcal{Y}^r(1)$ ως τον χώρο των κατά προσέγγιση ισομορφίας r-lattices, δηλαδή ως ένα γενικευμένο άνω ημιεπίπεδο modulo τη δράση μιας αριθμητικής ομάδας.

Η γενική περίπτωση

Έστω $r \geq 1$ και έστω $\mathbb{P}^{(r-1)}(\mathbf{C})$ το σύνολο των $\mathbf{C}$-ρητών σημείων του προβολικού $(r-1)$-χώρου $\mathbb{P}_{\mathbf{C}}^{(r-1)}$ και

$$\Omega^r := \mathbb{P}^{(r-1)}(\mathbf{C}) \setminus \bigcup \mathrm{H}(\mathbf{C})$$

όπου το H διατρέχει τα K_∞-ρητά υπερεπίπεδα του $\mathbb{P}_{\mathbf{C}}^{(r-1)}$. Ένα σημείο $\underline{\omega} = (\omega_1 : \ldots : \omega_r)$ ανήκει στο Drinfeld άνω ημιεπίπεδο Ω^r αν και μόνο αν δεν υπάρχει μη-τετριμμένη σχέση $\sum a_i\omega_i = 0$ με συντελεστές $a_i \in K_\infty$.

Τα $\mathbb{P}^{(r-1)}(\mathbf{C})$ και Ω^r δέχονται τη δομή rigid αναλυτικών χώρων. Μπορούμε έτσι να μιλούμε για ολόμορφες συναρτήσεις στο Ω^r.

Έστω A περιοχή κυρίων ιδεωδών και δακτύλιος του Drinfeld. Τότε κάθε lattice Λ τάξεως r του $\mathbf{C}$ είναι ελεύθερο $A-$module ελεύθερα παραγόμενο από r στοιχεία, $\Lambda = \langle \omega_1, \ldots, \omega_r \rangle$. Είναι εύκολο να διαπιστώσει κανείς ότι το Λ είναι διακριτό αν και μόνο αν $\boldsymbol{\omega} := (\omega_1 : \cdots : \omega_r) \in \Omega^r$.

Δράση αριθμητικών ομάδων στο άνω ημιεπίπεδο

Θεωρούμε την προφανή δράση της αριθμητικής ομάδας $\Gamma(1) := \mathrm{GL(r, A)}$ στο Ω^r. Δύο σημεία $\boldsymbol{\omega}$ και $\boldsymbol{\omega'}$ του Ω^r ορίζουν όμοια lattices (και ως εκ τούτου ισόμορφα Drinfeld modules) αν είναι συζυγή κάτω από τη δράση της $\Gamma(1)$. Συνεπώς, παίρνουμε μία κανονική ισομορφία

$$\Gamma(1) \setminus \Omega^r \sim \mathcal{Y}^r(1)(\mathbf{C})$$

από τον πηλικοχώρο $\Gamma(1) \setminus \Omega^r$ στο σύνολο των κλάσεων ισομορφίας $\mathcal{Y}^r(1)(\mathbf{C})$.

Η περίπτωση $r = 2$

Για $r = 2$ θα συμβολίζουμε με Ω το Drinfeld άνω ημιεπίπεδο Ω^2 το οποίο είναι το $\mathbb{P}^1(\mathbf{C}) \setminus \mathbb{P}^1(K) = \mathbf{C} \setminus K$. [1] Η ομάδα $\Gamma(1) := \mathrm{GL(2, A)}$ δρα στο Ω μέσω γραμμικών μετασχηματισμών

$$\begin{pmatrix} a\, b \\ c\, d \end{pmatrix}(z) = \frac{az+b}{cz+d}.$$

[1]Το Drinfeld άνω ημιεπίπεδο αντιστοιχεί στο κλασικό άνω και κάτω μιγαδικό ημιεπίπεδο: $\mathbb{C} - \mathbb{R} = H^+ \bigcup H^-$ και όχι στο H^+, όπως θα περίμενε κανείς.

Modular μορφές στο Ω

Μία modular μορφή βάρους k για την Γ είναι μία ολόμορφη συνάρτηση $f\colon \Omega \to \mathbf{C}$ η οποία ικανοποιεί τις συνθήκες

- $f\left(\frac{az+b}{cz+d}\right) = (cz+d)^k f(z)$ και $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma$ και
- $f(z)$ φράσσεται σε ένα υπόχωρο $\{z \in \Omega : \inf_{x \in K_\infty} |z-x| > 1\}$ του Ω.

Έστω M_k ο $\mathbf{C}$-διανυσματικός χώρο των modular forms για τη Γ βάρους k. Για $k \geq 1$ το άθροισμα

$$E_k(z) := \sum_{(0,0) \neq (a,b) \in A \times A} \frac{1}{(az+b)^k}$$

συγκλίνει και μάλιστα ορίζει μία σειρά, την σειρά του Eisenstein βάρους k. Για $k \equiv 0 \mod (q-1)$ η σειρά του Eisenstein είναι μία modular μορφή. Ανά δύο οι διανυσματικοί χώροι M_k είναι γραμμικά ανεξάρτητοι (δηλ. $M_k \cap M_l = \{0\}, \forall k \neq l$). Θέτουμε

$$M(\Gamma) := \bigoplus_{k \geq 0} M_k.$$

Αποδεικνύεται ότι ο $M(\Gamma)$ παράγεται από τις αλγεβρικά ανεξάρτητες Eisenstein σειρές E_{q-1} και E_{q^2-1}. Είναι επομένως ένας πολυωνυμικός δακτύλιος σε δύο μεταβλητές υπέρ το $\mathbf{C}$.

2.3 Drinfeld modules πάνω από schemes

Για να οριστεί το moduli schemes των Drinfeld modules πάνω από σώματα (δηλαδή ο χώρος ταξινόμησης τους) είναι αναγκαία η θεώρηση Drinfeld modules πάνω από schemes. Ένα invertible sheaf $\mathcal{F}$ πάνω από ένα scheme S είναι ένα sheaf συναρτήσεων, ώστε για κάθε αφινικό ανοιχτό $U = \mathrm{Spec}(B) \subset S$, το module $\mathcal{F}(U)$ πάνω από το B να είναι ισόμορφο προς το $B-$module B. Δίνουμε τον ορισμό:

Ορισμος 2.3.1. *Έστω $A = \mathbf{F}_q[T]$, $K = \mathbf{F}_q(T)$. Έστω S ένα $K-$ scheme και $\mathcal{L}$ ένα invertible sheaf πάνω από το S. Ο functor*

$$E : \{\text{Schemes/S}\} \longrightarrow \text{Abelian Groups}$$

ο οριζόμενος από την $E(S') = \Gamma(S', \mathcal{O}_{S'} \otimes_{\mathcal{O}_{S'}} \mathcal{L})$ ορίζει ένα αντιμεταθετικό group scheme υπέρ το S', τέτοιο ώστε, για κάθε αφινικό ανοιχτό $U \subset S$ το E_U (αναφορικά με την Zariski τοπολογία) είναι ισόμορφο προς το $\mathbb{G}_a$.

Με $\gamma : A \longrightarrow \Gamma(S')$ συμβολίζουμε τον φυσικό ομομορφισμό.

Ορισμος 2.3.2. *Ένα Drinfeld module τάξεως r υπέρ το S αποτελείται από*

1. *ένα invertible sheaf $\mathcal{L}$ του $\mathcal{O}_S-$ μαζί με ένα functor $E := E_{\mathcal{L}}$ όπως παραπάνω,*
2. *ένα ενδομορφισμό δακτύλιων*

$$\begin{aligned} \phi : A &\longrightarrow \mathrm{End}_{S-\text{groups}}(E) \\ \mathfrak{a} &\longmapsto \phi_{\mathfrak{a}} := \sum_{i=0}^{m} \alpha_i(\mathfrak{a}) \tau^i \end{aligned}$$

όπου $\tau^i : \mathcal{L} \longrightarrow \mathcal{L}^{\otimes p^i}$, $\alpha_i(\mathfrak{a}) \in \mathcal{L}^{\otimes(1-p^i)}, \alpha_0(\mathfrak{a}) = \gamma(\mathfrak{a})$ και $\alpha_m(\mathfrak{a})$ είναι μία generating section του $\mathcal{L}$ (δηλαδή μία πουθενά μηδενιζόμενη global section) και $m = r \cdot \deg(\mathfrak{a})$.

2.3.1 Level structure

Ο Drinfeld στο [7] εισήγαγε την έννοια της level structure σε Drinfeld $A-$ modules. Έστω ϕ ένα Drinfeld module και $\mathfrak{n} \in A$ ένα μη τετριμμένο ιδεώδες του ϕ. Το $\phi[\mathfrak{n}]$ είναι A submodule scheme $\ker \phi_{\mathfrak{n}} \subset \mathbb{G}_a$— το subscheme των $\mathfrak{n}$ *σημείων πεπερασμένης τάξης* του ϕ.

Προταση 2.3.1. *Έστω r η τάξη ενός Drinfeld module ϕ υπέρ το L. Τότε:*

1. *$\phi[\mathfrak{n}]$ είναι ένα πεπερασμένο group scheme τάξεως $\#(A/\mathfrak{n}A)^r$ υπέρ το L και*

2. *αν το $\mathfrak{n}$ είναι πρώτο ως προς τη χαρακτηριστική του L τότε το $\phi[\mathfrak{n}]$ είναι ένα ελεύθερο $A/\mathfrak{n}A$ module τάξεως r.*

Ορισμος 2.3.3. *Μία* $\mathfrak{n}$-level structure *σε ένα Drinfeld module ϕ* υπέρ *το L είναι ένας μορφισμός*

$$l : (A/\mathfrak{n})^r \longrightarrow \mathbb{G}_a(\mathrm{Spec}(L)) := \mathrm{Mor}(\mathrm{Spec}(L), \mathbb{G}_a)$$

από A-module schemes τέτοιος ώστε στο $\mathbb{G}_a$

$$\sum l(\mathfrak{n})_{\mathfrak{n}} \in (A/\mathfrak{n}A)^r = \phi[\mathfrak{a}]$$

(περνώντας στους αντίστοιχους διαιρέτες) να ικανοποιείται η παραπάνω ισότητα.

Πιο συγκεκριμένα, έστω ϕ ένα Drinfeld module γενικής χαρακτηριστικής τάξεως r. Μία $\mathfrak{n}$-*level structure* υπέρ το L σημαίνει ότι

- το ϕ ορίζεται υπέρ το L
- οι ρίζες του $\phi_{\mathfrak{n}}(X)$ σχηματίζουν ένα $A-$module *και* είναι στοιχεία του L
- υπάρχει ένας $A-$module ισομορφισμός $(A/\mathfrak{n}A)^r \longrightarrow \phi[\mathfrak{n}]$.

Σημείωση 3. Έστω (ϕ, i) και (ψ, j) δύο Drinfeld modules υπέρ το L με $\mathfrak{n}$-level structure δοσμένη από τα i και j. Αν (ϕ, i), και (ψ, j) είναι ισόμορφα, τότε υπάρχει $u \in L$ τέτοιο ώστε $\psi = u\phi u^{-1}$ και το ακόλουθο διάγραμμα να είναι αντιμεταθετικό.

$$\begin{tikzcd}
 & (\frac{A}{\mathfrak{n}})^r \arrow[dl, "i"'] \arrow[dr, "j"] \arrow[d, phantom, "="] & \\
\phi_{\mathfrak{n}} \arrow[rr, "u^{-1}"'] & {} & \psi_{\mathfrak{n}}
\end{tikzcd}$$

2.4 Moduli schemes

2.4.1 Το Moduli scheme $Y^r(1)$

Θεωρούμε τον functor:

$$\mathcal{Y}^r(1)\colon \left\{ \begin{array}{c} K-\text{schemes} \\ S \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \text{κλάσσεις ισομορφίας} \\ \text{Drinfeld modules τάξεως } r \text{ υπέρ το } S \end{array} \right\}.$$

Ο functor δεν είναι αναπαραστάσιμος (representable) από κάποιο S-scheme $M^r(1)$ (υπάρχουν μη τετριμμένοι αυτομορφισμοί Drinfeld modules πάνω από αλγεβρικά κλειστά $A-$σώματα). Ο $\mathcal{Y}^r(1)$ ορίζει ένα coarse moduli πρόβλημα. Το (αφινικό) scheme που αντιστοιχεί σε αυτό συμβολίζεται με $Y^r(1)$.

2.4.2 Το moduli scheme $Y^r(\mathfrak{n})$

Έστω $\mathfrak{n}$ μη τετριμμένο πολυώνυμο και $\mathcal{Y}^r(\mathfrak{n})$ ο functor

$$\mathcal{Y}^r(\mathfrak{n})\colon \left\{ \begin{array}{c} K-\text{schemes} \\ S \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \text{κλάσεις ισομορφίας από} \\ \text{Drinfeld modules τάξεως } r \text{ υπέρ το } S \\ \text{εφοδιασμένα με μία } \mathfrak{n}\text{-level structure} \end{array} \right\}.$$

Θεωρημα 2.4.1 (Drinfeld [7]). *Υποθέτουμε ότι το $\mathfrak{n}$ διαιρείται από τουλάχιστον δύο διαφορετικούς πρώτους. Τότε ο $\mathcal{Y}^r(\mathfrak{n})$ είναι αναπαραστάσιμος από ένα λείο αφινικό A-scheme $Y^r(\mathfrak{n})$, σχετικής διάστασης $(r-1)$.*

Σημείωση 4. Τα πολυώνυμα που ικανοποιούν την παραπάνω απαίτηση χαρακτηρίζονται στην σχετική βιβλιογραφία ως admissible. Το παραπάνω θεώρημα γενικεύεται και για μη admissible (και μη τετριμμένα) πολυώνυμα. Και σε αυτήν την περίπτωση υπάρχει ένα $A[\frac{1}{\mathfrak{n}}]$-scheme $Y^r(\mathfrak{n})$ που αναπαριστά τον functor. Στην παρούσα εργασία θα περιοριστούμε σε Drinfeld modules που ορίζονται πάνω από K-άλγεβρες. Έτσι, το αντίστοιχο scheme «ορίζεται» πάνω από το K και κατά συνέπεια προβλήματα σχετικά με την level structure δεν εμφανίζονται.

Κρίνουμε σκόπιμο να παραθέσουμε μία απόδειξη στο παραπάνω θεώρημα. Η απόδειξη που παρουσιάζουμε οφείλεται εν μέρη στον Marius Van Der Put και βρίσκεται στο [31].

Στα παρακάτω όλοι οι δακτύλιοι που θεωρούμε υποθέτουμε ότι είναι δακτύλιοι της Noether. Σε αφινικά schemes πάνω από τέτοιους δακτύλιους οι ένοιες των invertible sheaf, trivial line bundle και group scheme ταυτίζονται, με την ένοια ότι το κάθε ένα από αυτά αντιστοιχεί με μοναδικό τρόπο στα υπόλοιπα. Πιο συγκεκριμένα, το τετριμμένο line bundle $\mathrm{Spec}(R[X])$ αντιστοιχεί στο structure sheaf $\mathcal{O}_{\mathrm{Spec}(R)}$ που με τη σειρά του αντιστοιχεί στο additive group scheme $\mathbb{G}_{a,R} = \mathrm{Spec}(R[X])$.

Έστω $c_1, \dots, c_r$ αλγεβρικά ανεξάρτητες μεταβλητές υπέρ το $\mathbf{F}_p$ και

$$\mathfrak{n} = \sum_{i=0}^{d} a_i T^i$$

ένα μη τετριμμένο πολυώνυμο του $A = \mathbf{F}_q[T]$. Θεωρούμε τον δακτύλιο

$$\mathcal{B} := K[c_1, \dots, c_r, c_r^{-1}, \{x_\alpha\}]_{\alpha \in (A/\mathfrak{n})^r}$$

ο οποίος γεννιέται υπέρ τον A από τα $c_1, \dots, c_r, c_r^{-1}$ ($c_r c_r^{-1} = 1$) και τα x_α, $\alpha \in (A/\mathfrak{n})^r$. Οι σχέσεις μεταξύ των γενητόρων θα προσδιοριστούν παρακάτω. Ορίζουμε ένα Drinfeld module τάξεως r υπέρ το $\mathcal{B}$ ως εξής:

$$\tilde{\phi}\colon A \longrightarrow \mathcal{B}\colon T \longmapsto T + c_1\tau + \dots + c_r\tau^r.$$

Οι σχέσεις μεταξύ των γεννητόρων είναι οι εξής:

1. $x_\alpha + x_{\alpha'} = x_{\alpha+\alpha'}$ και $x_{\lambda\alpha} = \lambda x_\alpha$ για κάθε $\alpha, \alpha' \in (A/\mathfrak{n})^r$. και $\lambda \in \mathbf{F}_p^*$, και $x_0 = 0$
2. $x_{T\alpha} = \tilde{\phi}_T(x_\alpha) = Tx_\alpha + c_1 x_\alpha^p + \dots + c_r x_\alpha^{p^r}$ για κάθε μη μηδενικό στοιχείο $\alpha \in (A/\mathfrak{n})^r$
3. Το πολυώνυμο $\tilde{\phi}_{\mathfrak{n}}(X) := \sum_{i=0}^{rd} a_j X^{p^j}$ ισούται με το $a_{rd} \prod\limits_{\alpha \in A/\mathfrak{n}} (X - x_\alpha)$.
4. Διαλέγουμε ένα στοιχείο $\alpha_0 \in (A/\mathfrak{n})^r$ με $\alpha_0 \neq 0$ και $\mathfrak{n} \cdot \alpha_0 = 0$ και θέτουμε $x_{\alpha_0} = 1$.

Τα παραπάνω ορίζουν ένα Drinfeld module $(\tilde{\phi}, \tilde{i})$ υπέρ το $\mathrm{Spec}(\mathcal{B})$ τάξεως r, με $\mathfrak{n}$-level structure δοσμένη από το μονομορφισμό $\tilde{i}\colon (A/\mathfrak{n}A)^r \longrightarrow \mathcal{B}\colon \alpha \longmapsto x_\alpha$ και line bundle το structure sheaf του $\mathrm{Spec}(\mathcal{B})$.

Θα δείξουμε ότι το $\tilde{\phi}$ εφοδιασμένο με την παραπάνω δομή αντιπροσωπεύει τον functor $\mathcal{Y}^r(\mathfrak{n})$. Έστω R τυχόν δακτύλιος με $K \subset R$ εφοδιασμένος με

α′. ένα τετριμμένο line bundle $\mathcal{L}$ υπέρ το $\mathrm{Spec}(R)$

β′. ένα Drinfeld module $\phi\colon A \longrightarrow \mathrm{End}(\mathcal{L})$ τάξεως r

γ′. ένα ομομορφισμό από A-modules $i\colon A \longrightarrow \mathcal{L}(\mathrm{Spec}(R))$ ώστε ο πυρήνας του ϕ να ταυτίζεται με τον Cartier divisor του $\sum_{\alpha \in (A/\mathfrak{n})^r} i(\mathrm{div}(\alpha))$.

Η section $i(\alpha)$ ικανοποιεί την σχέση $\tilde{\phi}(\mathfrak{n})i(\alpha) = 0$. Από το μέρος γ′ και επειδή το πολυώνυμο $\phi(\mathfrak{n})(X) \equiv \phi_{\mathfrak{n}}(X)$ είναι διαχωρίσιμο (η διακρίνουσά του είναι δύναμη του $\mathfrak{n}$), η section $i(\alpha)$ δεν έχει ρίζες. Χωρίς βλάβη της γενικότητας, μπορούμε να υποθέσουμε ότι $i(\alpha) = 1$. Συνεπώς, μπορούμε με μοναδικό τρόπο να ταυτίσουμε το line bundle $\mathcal{L}$ με το structure sheaf R ώστε $i(\alpha) = 1$. Επομένως ο ομομορφισμός $\phi\colon A \longrightarrow \mathrm{End}(\mathcal{L})$ δίνεται από ένα ομομορφισμό της μορφής $\phi\colon A \longrightarrow R\{\tau\}\colon \phi_T \longmapsto T + d_1\tau + \dots + d_r\tau^r$, με $d_i \in R$.

Αφού όλα τα $i(\alpha)$ είναι στοιχεία του δακτυλίου R, η συνθήκη γ μπορεί να μετασχηματιστεί στην συνθήκη: τα πολυώνυμα $\phi_{\mathfrak{n}}(X)$ και $d\prod_\alpha (X - i(\alpha))$, για κάποια κατάλληλη αντιστρέψιμη σταθερά $d \in R$ ταυτίζονται.

Ορίζουμε τον K-ομομορφισμό $h\colon \mathcal{B} \longrightarrow R$ όπου $h(x_\alpha) = i(\alpha)$ και $h(c_i) = d_i$ για κάθε $\alpha \in (A/\mathfrak{n})^r$ και $i = 1, \ldots, r$. Ο h είναι καλά ορισμένος, λόγω των 1-4 και α΄-γ΄ παραπάνω. Είναι σαφές ότι μέσω του h μεταφέρεται η level structure δομή του «universal» αντικειμένου $\widetilde{\phi}$ στο ϕ και μάλιστα, ο h προσδιορίζεται μοναδικά από την παραπάνω ιδιότητα.

Συνεπώς, το Spec($\mathcal{B}$) αναπαριστά τον functor $\mathcal{Y}^r(\mathfrak{n})$ υπέρ το K. Δείξαμε δηλαδή το παρακάτω θεώρημα:

Θεωρημα 2.4.2 ([7], [28],[31]). *Έστω $\mathfrak{n}$ ένα μη μηδενικό ιδεώδες του A. Τότε, ο functor $\mathcal{M}^r(\mathfrak{n})$ αντιπροσωπεύεται από ένα αφινικό $K-$ scheme $Y^r(\mathfrak{n})$.*

Η δράση της $\mathrm{GL(r, A/\mathfrak{n})}$

Η πεπερασμένη ομάδα $G(\mathfrak{n}) := \mathrm{GL(r, A/\mathfrak{n})}$ δρα στο $\mathcal{Y}^r(\mathfrak{n})$ μεταθέτοντας τις level structures. Μέσω του functor, η δράση αυτή περνάει και στο scheme $Y^r(\mathfrak{n})$. Το $Y^r(1)$ είναι το πηλίκο του $Y^r(\mathfrak{n})$ με την $\mathrm{G}(\mathfrak{n})$ (το οποίο δεν εξαρτάται από την επιλογή του $\mathfrak{n}$). Έχει μάλιστα την ιδιότητα, ότι τουλάχιστο τα L-ρητά σημεία, για αλγεβρικά κλειστά A-σώματα L αντιστοιχούν με τρόπο ένα προς ένα, επί και συναρτησιακά (functorially) στο $\mathcal{Y}^r(1)(L)$.

Τα Drinfeld modules τάξεως 2 ταξινομούνται από την αφινική ευθεία $Y^2(1) = \mathbb{A}^1$. Πράγματι έστω $A = \mathbf{F}_q[T]$, K το σώμα πηλίκων του A και $\gamma : A \longrightarrow K$ δοσμένος ομομορφισμός. Έστω $\phi : A \longrightarrow K\{\tau\}$ ένα Drinfeld module τάξεως 2 υπέρ το K. Ο ομομορφισμός ϕ καθορίζεται από την τιμή ϕ_T του T :

$$\phi_T = \gamma(T) + c_1\tau + c_2\tau^2$$

όπου $c_i \in K$ και $c_r \in K^*$. Αντίστροφα, κάθε επιλογή $\{c_1, c_2\}$, με $c_2 \in K^*$, ορίζει ένα Drinfeld module τάξεως 2. Δύο Drinfeld module ϕ και ϕ' είναι ισόμορφα αν και μόνο αν υπάρχει ένα στοιχείο $a \in K^*$ ώστε

$$\forall i = 1, 2, \qquad c_i a^{p^i - 1} = c_i'.$$

Μέρος I

Η ομάδα PSL

Ο Weil μορφισμος

3.1 Η ορίζουσα ενός Drinfeld module

Το κεφάλαιο αυτό δεν αποτελεί προτότυπη εργασία. Το Weil pairing στην κατηγορία των Drinfeld modules είχε αναφερθεί από τον ίδιο τον Drinfeld σε ένα ιδιωτικό του γράμμα προς τον Gross· αναφέρεται δε και στο βιβλίο «The arithmetic of function fields» [14] επιγραμματικά, και αυτή η αναφορά μιας γραμμής ήταν η μοναδική αναφορά γνωστή σε εμάς. Ωστόσο, για μας, η κατασκευή του είχε ιδιαίτερη σημασία, αφού ενδιαφερόμασταν για την Galois δράση σε Drinfeld modules τάξεως r και πως αυτή περνάει σε Drinfeld modules τάξεως 1. Αναγκαστήκαμε λοιπόν να ξαναααποδείξουμε την ύπαρξη του. Στην κούρσα των δημοσιεύσεων ωστόσο, προηγήθηκε ο Gert-Jan van der Heiden, ο οποίος δουλεύοντας ανεξάρτητα από εμάς, παρουσίασε την εργασία του «Weil Pairing for Drinfeld Modules» (preprint) [15]. Στην παρούσα εργασία κρίνεται σκόπιμο να παρατεθεί η δικιά μας προσσέγγιση.

Έστω $\mathfrak{n}$ ένα, μη-τετριμμένο, ιδεώδες του A και C το Carlitz module $C_T = T + \tau$ υπέρ το L. Θα συμβολίζουμε με $L(\mathfrak{n})$ το σώμα που γεννιέται υπέρ το L από τις ρίζες του πολυωνύμου $C_{\mathfrak{n}}(X)$, δηλαδή του πολυωνύμου που αντιστοιχεί στο Carlitz module. Θα συμβολίζουμε με $K^+ \subset L(\mathfrak{n})$ την maximal αβελιανή επέκταση του K στην οποία το ∞ αναλύεται πλήρως και με $L_+(\mathfrak{n}) \subset L(\mathfrak{n})$ την maximal αβελιανή επέκταση του L στην οποία το ∞ αναλύεται πλήρως.

Θεωρημα 3.1.1. [21] *Το moduli scheme των Drinfeld modules τάξεως 1 —των οριζόμενων πάνω από K-σώματα— είναι το*

$$Y^1(\mathfrak{n}) = \mathrm{Spec}(K_+(\mathfrak{n})).$$

Θέλουμε να ορίσουμε έναν dominant μορφισμό $\mathcal{W}_{\mathfrak{n}} : Y^r(\mathfrak{n}) \longrightarrow Y^1(\mathfrak{n})$ ο οποίος θα στέλνει Drinfeld modules τάξεως r με $\mathfrak{n}$-level structure σε Drinfeld modules τάξεως 1 με $\mathfrak{n}$-level structure. Στην κατηγορία των Drinfeld modules ο μορφισμός $\mathcal{W}_{\mathfrak{n}}$ θα παίζει ρόλο ανάλογο με εκείνο της «Weil Pairing» στην κατηγορία των ελλειπτικών καμπύλων με level structure. Το τι εννοούμε θα γίνει αντιληπτό στις επόμενες παραγράφους. Μία ενδιαφέρουσα εφαρμογή είναι ο προσδιορισμός του σώματος ορισμού του moduli scheme $Y^r(\mathfrak{n})$.

3.1.1 $T-$motives

Στην παράγραφο αυτή χρησιμοποιούμε τα σύμβολα και τους ορισμούς του κεφ. 5 του [13]. Έστω $A = \mathbf{F}_p[T], \phi \colon A \longrightarrow L\{\tau\}$ ένα Drinfeld module τάξεως r και $\phi_T = a_r\tau^r + \cdots + a_1\tau + T\tau^0$. Η μη αντιμεταθετική L-άλγεβρα $M := L\{\tau\}$ γίνεται μία $A-$άλγεβρα μέσω $am := m \circ \phi_a$ για $a \in A$ και $m \in M$. Μπορούμε να δούμε το M ως μια $B = L \otimes_{\mathbf{F}_p} A-$άλγεβρα μέσω του ομομορφισμού δακτυλίων

$$B \xrightarrow{1\otimes\phi} M \ .$$

Πιο συγκεκριμένα, το M γίνεται μία $B-$άλγεβρα μέσω του $(\kappa\otimes a)\cdot m = \kappa\cdot(m\circ\phi_a)$ και $m(\kappa\otimes a) = \kappa^p\cdot(m\circ\phi_a)$, για κάθε $m \in M,\ a \in A$ και $\kappa \in L$. Σημειώνουμε ότι ο B είναι πολυωνυμικός δακτύλιος μίας μεταβλητής υπέρ το L, $B = L[Y]$ όπου $Y = 1 \otimes T$. Είναι γνωστό ότι το M είναι ένα *ελεύθερο* module τάξεως r υπέρ το B με βάση $\{1, \tau, \tau^2, \ldots, \tau^{r-1}\}$. Συνεπώς, η «full exterior power» του ${}_BM$, συμβ. ${}_B\bigwedge^r, M$ είναι ένα ελεύθερο module τάξεως ένα με βάση $\{1 \wedge \tau \wedge \cdots \wedge \tau^{r-1}\}$.

Συμβολισμός 2. Θέτουμε $\mu^m := \tau^m \wedge \cdots \wedge \tau^{m+r-1},\ m \geq 0$ και $N :=_B \bigwedge^r M$.

Ορίζουμε δράση του τ στο N ως ακολούθως

$$\tau \cdot (m_1 \wedge \cdots \wedge m_r) := \tau(m_1) \wedge \cdots \wedge \tau(m_r).$$

Η δράση αυτή είναι A-γραμμική αλλά όχι και B-γραμμική.

3.1.2 Η κατασκευή της ορίζουσας ενός Drinfeld module.

Ο σκοπός της παραγράφου αυτής είναι η κατασκευή της ορίζουσας ή αλλιώς της *full exterior power* ενός Drinfeld Module τάξεως r. Η ορίζουσα θα είναι ένα Drinfeld module τάξεως 1. Για να την κατασκευάσουμε, θα πρέπει να δούμε το N ως μια skew[1] $L-$άλγεβρα παραγόμενη από ένα Frobenius ενδομορφισμό (δες το λήμμα ;; παρακάτω).

Λημμα 3.1.1. *Στο B ο $r-$ Frobenius ενδομορφισμός τ^r ισούται με $\sigma_0\tau^0 + \sigma_1\tau + \cdots + \sigma_{r-1}\tau^{r-1}$, όπου $\sigma_0 = a_r^{-1} \otimes T - a_r^{-1}T \otimes 1$ και $\sigma_i = -a_r^{-1}a_i \otimes 1$ για $i = 1, \ldots, r-1$.*

Απόδειξη. $(1\otimes)T \cdot \tau^0 = \tau^0\phi_T = \phi_T = T \otimes 1\tau^0 + a_1 \otimes 1 \cdot \tau + \cdots + a_r \otimes 1 \cdot \tau^r$. ❑

Λημμα 3.1.2. $\mu = (-1)^{r-1}\sigma_0 \cdot \mu^0$.

Απόδειξη. $\mu = \tau\wedge\cdots\wedge\tau^r = \tau\wedge\cdots\wedge\sum_{i=0}^{r-1}\sigma_i\tau^i = \tau\wedge\cdots\wedge\sigma_0\tau^0 = (-1)^{r-1}\sigma_0\cdot\tau^0\wedge\cdots\wedge\tau^{r-1} = (-1)^{r-1}\sigma_0\cdot\mu^0$. ❑

Λημμα 3.1.3. $(1 \otimes T) \cdot \mu^m = T^{p^m} \otimes 1 \cdot \mu^0 + (-1)^{r-1}a_r^{p^m} \otimes 1 \cdot \mu^{m+1}$

Απόδειξη.

$$\begin{aligned}
(1 \otimes T) \cdot \mu^m &= \tau^m\phi_T \wedge \cdots \wedge \tau^{m+r-1} \\
&= (T^{p^m}\tau^m + a_1^{p^m}\tau^{m+1} + \cdots + a_r^{p^m}\tau^{r+m}) \wedge \tau^{m+1} \wedge \cdots \wedge \tau^{m+r-1} \\
&= T^{p^m} \otimes 1 \cdot \mu^0 + (-1)^{r-1}a_r^{p^m} \otimes 1 \cdot \mu^{m+1}.
\end{aligned}$$

❑

Λημμα 3.1.4. *Αν $a \in A$ τότε το $(1 \otimes a) \cdot \mu^0$ είναι γραμμικός συνδυασμός των $\mu^0, \ldots, \mu^{d+1}$ υπέρ το L όπου $d = \deg(a)$.*

Απόδειξη. Αρκεί να αποδείξουμε το λήμμα για $1 \otimes T^m \cdot \mu^0, \forall m$. Για $m = 1$,

$$\begin{aligned}
(1 \otimes T) \cdot \mu^0 &= \phi_T \wedge \cdots \wedge \tau^{r-1} \\
&= T \otimes 1 \cdot \mu^0 + (-1)^{r-1}a_r \otimes 1 \cdot \mu.
\end{aligned}$$

Για $m = 2$,

$$\begin{aligned}
(1 \otimes T^2) \cdot \mu^0 &= (1 \otimes T) \cdot (1 \otimes T \cdot \mu^0) \\
&= (1 \otimes T)(T \otimes 1 \cdot \mu^0 + (-1)^{r-1}a_r \otimes 1 \cdot \mu) \\
&= T^2 \cdot \mu^0 + (-1)^{r-1}Ta_r\mu + (-1)^{r-1}a_r((-1)^{r-1}a_r^p\mu^2 + T^p\mu) \\
&= T^2\mu^0 + (-1)^{r-1}a_r(T + T^p)\mu + a_r^{1+p}\mu^2.
\end{aligned}$$

Υποθέτουμε ότι $(1 \otimes T^m) \cdot \mu^0 = A_0\mu^0 + A_1\mu + \cdots + A_m\mu^m$ 'οπου $A_i \in L$. Τότε,

$$\begin{aligned}
(1 \otimes T^{m+1}) \cdot \mu^0 &= (1 \otimes T)(1 \otimes T^m \cdot \mu^0) \\
&= (1 \otimes T) \cdot (A_0\mu^0 + A_1\mu + \cdots + A_m\mu^m) \\
&= A_0(1 \otimes T \cdot \mu^0) + A_1(1 \otimes T \cdot \mu) + \cdots + A_m(1 \otimes T \cdot \mu^m)
\end{aligned}$$

❑

[1] μη-αντιμεταθετική

Σημείωση 5. Είναι τώρα προφανές ότι μπορούμε να γράψουμε κάθε στοιχείο του N σαν πολυώνυμο του μ υπέρ το L.

Μένει να ορίσουμε μία αριστερή $\mu-$δράση στο N.

Ορισμος 3.1.1. *Το $L\{\mu\}$ είναι μία L-άλγεβρα παραγόμενη υπέρ το L από τα $\{\mu^m, m = 0, 1, \ldots\}$ με πολλαπλασιασμό ορισμένο ως:*

- $\mu^i\mu^j = \mu^{i+j}$ *και*
- $\mu\kappa = \kappa^p\mu$

Είμαστε τώρα έτοιμοι να αποδείξουμε το

Λημμα 3.1.5. *Το N είναι μία skew $L-$άλγεβρα παραγόμενη από το μ.*

Απόδειξη. Κάθε στοιχείο του N μπορεί να γραφτεί στη μορφή $\beta \cdot \mu^0$ όπου $\beta = \sum_i \kappa_i \otimes a_i \in B$.

$$\beta \cdot \mu^0 = \sum_i \kappa_i \otimes a_i \cdot \mu^0 = \sum_i \kappa_i \otimes 1 \cdot (1 \otimes a_i \cdot \mu^0).$$

Από το λήμμα (3.1.4), $\forall i$ το $(1 \otimes a_1) \cdot \mu^0$ είναι πολυώνυμο ως προς τα $\mu^0, \ldots, \mu^{\deg(a_i)}$, υπέρ το L. Αυτό αποδεικνύει το γεγονός ό,τι κάθε στοιχείο του N μπορεί να θεωρηθεί ως ένα πολυώνυμο ως προς μ υπέρ το L. Τέλος, σημειώνουμε ότι $\mu \cdot (\kappa \otimes 1) = (\kappa^p \otimes 1) \cdot \mu$. ❏

Είμαστε τώρα σε θέση να δώσουμε τον ορισμό της ορίζουσας ενός Drinfeld Module:

Ορισμος 3.1.2. *Έστω ϕ και μ όπως παραπάνω. Η ορίζουσα $\wedge^r\phi$ του ϕ είναι ένα Drinfeld module τάξεως ένα*

$$\wedge^r\phi : A \longrightarrow L\{\mu\}$$

δοσμένο από

$$\begin{array}{ccccc} A & \longrightarrow & L \otimes_{\mathbf{F}_p} A & \longrightarrow & \bigwedge^r L\{\tau\} \xrightarrow{\sim} L\{\mu\} \\ a & \longmapsto & 1 \otimes a & \longmapsto & 1 \otimes a \cdot \mu^0 \end{array}$$

Ακριβέστερα,

$$T \longmapsto T \cdot \mu^0 + c_r(-1)^{r-1}\mu.$$

Υπενθυμίζουμε ότι με $Y^r(1)$ συμβολίζουμε το moduli scheme των Drinfeld modules τάξεως ένα, τα οποία ορίζονται πάνω από σώματα L με $L \supset K$. Κλείνουμε την παράγραφο αποδεικνύοντας την ύπαρξη ενός μορφισμού $\mathcal{W} : Y^r(1) \longrightarrow Y^r(1)$ οποίος μεταφέρει Drinfeld modules τάξεως r στις ορίζουσες τους. Ας σημειωθεί ότι η έννοια της level structure δεν έχει ακόμα χρησιμοποιηθεί. Αυτό θα γίνει στην επόμενη παράγραφο. Έχουμε ήδη αποδείξει την ακόλουθη

Προταση 3.1.1. *Υπάρχει ένας μορφισμός*

$$\mathcal{W} : Y^r(1) \longrightarrow Y^1(1) \;\; ; \;\; \phi \longmapsto \wedge^r\phi. \tag{3.1}$$

3.2 Σημεία πεπερασμένης τάξης και t-motives.

Οι ορισμοί —καθώς και οι συμβολισμοί— της παραγράφου αυτής περιέχονται στο [13], §5.6, σελ. 151-156. Προκειμένου να αποδείξουμε την ύπαρξη ενός dominant μορφισμού

$$\mathcal{W}_n : Y^r(\mathfrak{n}) \longrightarrow Y^1(\mathfrak{n})$$

θα πρέπει να εισάγουμε στο μορφισμό (3.1) τη level structure. Έστω (ϕ, i) ένα $L-$ρητό σημείο του $Y^r(\mathfrak{n})$ όπου $i : (A/\mathfrak{n}A)^r \longrightarrow \phi[\mathfrak{n}]$ είναι ένας $A/\mathfrak{n}A$ ισομορφισμός (δηλ. είναι μία $\mathfrak{n}$-level structure). Το module ϕ θα πρέπει να απεικονίζεται μέσω του $\mathcal{W}_\mathfrak{n}$ στο $\wedge^r\phi$. Ο μορφισμός $\mathcal{W}_\mathfrak{n}$ θα πρέπει να μεταφέρει την $\mathfrak{n}-$level structure —από την κατηγορία των Drinfeld modules τάξεως r— σε μία $\mathfrak{n}-$level structure στην κατηγορία των Drinfeld modules τάξεως ένα. Αρκεί επομένως να δειχθεί ότι ο επαγώμενος ομομορφισμός $\wedge^r : \wedge^r((A/\mathfrak{n}A)^r) \longrightarrow \wedge^r(\phi[\mathfrak{n}])$ είναι φυσικός, δηλαδή να δειχτεί ότι τα $\wedge^r(\phi[\mathfrak{n}])$ και $(\wedge^r\phi)[\mathfrak{n}]$ είναι, με κανονικό τρόπο, ισόμορφα.

Έστω M, N, τ, μ και ϕ όπως παραπάνω. Απο εδώ και στο εξής θα υποθέτουμε ότι το σώμα L είναι τέλειο· στη συνέχεια θα άρουμε τον περιορισμό αυτό. Η προσέγγιση αυτή γίνεται για τεχνικούς λόγους. Υπενθυμίζουμε ότι με $\phi[\mathfrak{n}]$ σημειώνουμε το σύνολο των $\mathfrak{n}$ σημείων πεπερασμένης τάξης του ϕ, δηλαδή τις ρίζες του προσθετικού πολυωνύμου $\phi_{\mathfrak{n}}(X)$. Θέτουμε

$$(M/\mathfrak{n}M)^\tau := \{m \in M/\mathfrak{n}M \mid \tau m - m \in \mathfrak{n}M\}.$$

Το θεώρημα του Lang για την $\mathrm{GL}(r)$ μας λέει ότι

$$(M/\mathfrak{n}M)^\tau \otimes_{\mathbf{F}_p} L \cong M/\mathfrak{n}M$$

ως διανυσματικοί χώροι και B modules (δες [13, πόρισμα 5.6.4,σελ. 152]). (Όμοιοι ορισμοί και συμπεράσματα ισχύουν και για το $(N/\mathfrak{n}N)^\mu$ και το $N/\mathfrak{n}N$.)

Θεωρημα 3.2.1. *Ως $A-$module το $\phi[\mathfrak{n}]$ είναι κανονικά ισόμορφο προς το*

$$\mathrm{Hom_A}((\mathrm{M}/\mathfrak{n}\mathrm{M})^\tau, \mathrm{Hom}_{\mathbf{F}_p}(\mathrm{A}/\mathfrak{n}\mathrm{A}, \mathbf{F}_\mathrm{p}))\,.$$

Απόδειξη. Είναι συνδυασμός του θεωρήματος 5.6.6 και της πρότασης 5.6.3 (και της σημείωσης κάτω από αυτήν) του [13]. ❑

Λημμα 3.2.1. *Ως $B-$modules τα $\bigwedge^r \frac{M}{\mathfrak{n}M}$ και $\frac{N}{\mathfrak{n}N}$ είναι ισόμορφα.*

Απόδειξη. Θεωρούμε την ακριβή ακολουθία των B modules:

$$0 \longrightarrow \mathfrak{n}M \longrightarrow M \longrightarrow \frac{M}{\mathfrak{n}M} \longrightarrow 0.$$

Αφού το $_BM$ είναι flat, η ακολουθία

$$0 \longrightarrow (\mathfrak{n}M) \otimes_B M^{\otimes r-1} \longrightarrow M^{\otimes r} \longrightarrow \frac{M}{\mathfrak{n}M} \otimes_B M^{\otimes r-1} \longrightarrow 0$$

είναι ακριβής και ως εκ τούτου, αφού $(\mathfrak{n}M) \otimes_B M^{\otimes r-1} \cong \mathfrak{n}(M^{\otimes r})$, [2] έχουμε

$$\frac{M}{\mathfrak{n}M} \otimes_B M^{\otimes r-1} \cong \frac{M^{\otimes r}}{\mathfrak{n}M^{\otimes r}}.$$

Από την άλλη μεριά $\frac{M}{\mathfrak{n}M} = \frac{B}{\mathfrak{n}B} \otimes_B M$ και $\frac{M^{\otimes r}}{\mathfrak{n}M^{\otimes r}} = \frac{B}{\mathfrak{n}B} \otimes_B M^{\otimes r}$. Αυτό αποδεικνύει την ισότητα

$$(\frac{M}{\mathfrak{n}M})^{\otimes r} = \frac{M^{\otimes r}}{\mathfrak{n}(M^{\otimes r})}. \tag{3.2}$$

Έστω $\mathcal{T}$ το submodule του $M^{\otimes r}$ που παράγεται από τα στοιχεία της μορφής

$$\cdots \otimes m \otimes \cdots \otimes m \otimes \cdots$$

και έστω $\mathcal{T}'$ το B submodule του $(\frac{M}{\mathfrak{n}M})^{\otimes r}$ που παράγεται από στοιχεία της μορφής

$$\cdots \otimes (m + \mathfrak{n}M) \otimes \cdots \otimes (m + \mathfrak{n}M) \otimes \cdots\,.$$

Τα $\mathcal{T}'$ και $(\mathcal{T} + \mathfrak{n}(M^{\otimes r}))/\mathfrak{n}M^{\otimes r}$ αντιστοιχούν το ένα στο άλλο μέσω της (3.2). Έτσι, αφού $N = M^{\otimes r}/\mathcal{T}$, έχουμε ότι

$$\begin{aligned}\frac{N}{\mathfrak{n}N} &= \frac{M^{\otimes r}/\mathcal{T}}{\mathfrak{n}(M^{\otimes r}/\mathcal{T})} = \frac{M^{\otimes r}/\mathcal{T}}{(\mathfrak{n}M^{\otimes r} + \mathcal{T})/\mathcal{T}} = \frac{M^{\otimes r}}{\mathfrak{n}M^{\otimes r} + \mathcal{T}} \\ &= \frac{M^{\otimes r}/\mathfrak{n}(M^{\otimes r})}{(\mathfrak{n}(M^{\otimes r}) + \mathcal{T})/\mathfrak{n}(M^{\otimes r})} = \frac{(\frac{M}{\mathfrak{n}M})^r}{\mathcal{T}'} = \bigwedge^r (\frac{M}{\mathfrak{n}M})^r\end{aligned}$$

❑

[2] Για $_BX$ με $\mathfrak{n}X = 0$ είναι $B/\mathfrak{n}B \otimes_B X = X$

ΛΗΜΜΑ 3.2.2. *Έστω X, Y δύο A modules με $\mathfrak{n}X = \mathfrak{n}Y = 0$. Ισχύουν τα ακόλουθα:*

1. *X και Y είναι A ισόμορφα αν και μόνο αν είναι $A/\mathfrak{n}A$ ισόμορφα.*

2. *$\mathrm{Hom_A(X,Y)}$ και $\mathrm{Hom_{A/\mathfrak{n}A}(X,Y)}$ είναι ισόμορφα $A/\mathfrak{n}A$ modules.*

Απόδειξη. Σημειώνουμε απλά ότι $X \otimes_A A/\mathfrak{n}A = \frac{X}{\mathfrak{n}X} = X$. ❑

ΠΡΟΤΑΣΗ 3.2.1. *Ισχύει ότι τα $(\wedge\phi)[\mathfrak{n}] \cong \wedge(\phi[\mathfrak{n}])$ είναι ισόμορφα ως $A/\mathfrak{n}A$-modules.*

Απόδειξη. Θέτουμε $X = (M/\mathfrak{n}M)^r$ και $Y = \mathrm{Hom_{\mathbf{F}_p}(A/\mathfrak{n}A, \mathbf{F}_p)}$. Το $\mathbf{F}_p$− module Y μπορεί να θεωρηθεί ως ένα A module μέσω $(a \cdot f)(x) := f(a \cdot x)$ για κάθε $a \in A,\ f \in Y$ και $x \in A/\mathfrak{n}A$. [3] Σημειώνουμε ότι τα X, Y μηδενίζονται από το $\mathfrak{n}$. Ως εκ τούτου, εφαρμόζοντας το λήμμα 3.2.2, από το Πόρ. 5.6.4 του [13] σελ.152, X και $(A/\mathfrak{n}A)^r$ είναι A ισόμορφα —ας σημειώσουμε με $\kappa : (A/\mathfrak{n}A)^r \longrightarrow X$ αυτόν τον ισομορφισμό. Σημειώνουμε με κ^* τον επαγόμενο ισομορφισμό:

$$\kappa^* : \mathrm{Hom_A(X,Y)} \longrightarrow \mathrm{Hom_A((A/\mathfrak{n}A)^r, Y)}, \quad f \longmapsto \kappa \circ f.$$

Τα ακόλουθα είναι $A/\mathfrak{n}A$ ισομορφισμοί από $A/\mathfrak{n}A$ modules:

$$\mathrm{Hom_A((A/\mathfrak{n}A)^r, Y)} = \mathrm{Hom_{A/\mathfrak{n}A}((A/\mathfrak{n}A)^r, Y)} = \bigoplus_{i=1}^{r} \mathrm{Hom_{A/\mathfrak{n}A}(A/\mathfrak{n}A, Y)} = Y^r$$

Τώρα, περνώντας στις full exterior powers παίρνουμε ένα ισομορφισμό ο οποίος εξαρτάται μονάχα από το κ :

$$i : \bigwedge^{r} \mathrm{Hom_{A/\mathfrak{n}A}(X,Y)} \longrightarrow \bigwedge^{r} Y^r.$$

Με ν συμβολίζουμε τον φυσικό $A/\mathfrak{n}A$-ισομορφισμό $\nu : \bigwedge^r Y^r \longrightarrow Y$ και με

$$\nu^* : \mathrm{Hom_{A/\mathfrak{n}A}(A/\mathfrak{n}A, \bigwedge^{r} Y^r)},$$

Έτσι

$$\wedge(\phi[\mathfrak{n}]) = \bigwedge^{r} \mathrm{Hom}_{A/\mathfrak{n}A}(X,Y) \xrightarrow{i} \bigwedge^{r} Y^r \xrightarrow{\nu} \mathrm{Hom}_{A/\mathfrak{n}A}(A/\mathfrak{n}A, Y) \longrightarrow \mathrm{Hom}_A(A/\mathfrak{n}A, Y) \longrightarrow \mathrm{Hom}_A(N/\mathfrak{n}N, Y) = (\wedge\phi)[\mathfrak{n}]$$

❑

Συμβολισμός 3. Έστω $\lambda : \phi \longrightarrow \psi$ ισογένεια υπέρ το L. Έστω M_ϕ (αντ. M_ψ) το B−module $L\{\tau\}$. Η ισογένεια λ επάγει ένα B−ομομορφισμό

$$\lambda : M_\psi \longrightarrow M_\phi, m \mapsto m \circ \lambda.$$

---

[3] Έστω $\mathcal{E} = \{x_1, \ldots, x_d\}$ μία $\mathbf{F}_p$ βάση του $A/\mathfrak{n}A$. Έστω $\mathcal{E}^* = \{x_1{}^*, \ldots, x_d{}^*\}$ η δυϊκή $\mathrm{Hom_{\mathbf{F}_p}(A/\mathfrak{n}A, \mathbf{F}_p)}$. Συμβολίζουμε με κ τον ισομορφισμό $x_i \longmapsto x_i^*$. Με x θα συμβολίζουμε τα στοιχεία του $A/\mathfrak{n}A$ και με x^* τα αντίστοιχα στοιχεία του δυϊκού χώρου (μέσω της αντιστοίχισης που ορίζεται από το κ). Το σύνολο $\mathrm{Hom_{\mathbf{F}_p}(A/\mathfrak{n}A, \mathbf{F}_p)}$ γίνεται ένα A module μέσω

$$(a \cdot x^*)(y) = x^*(a \cdot x), \forall y \in A/\mathfrak{n}A.$$

Κάθε στοιχείο $a \in A$ ορίζει ένα $\mathbf{F}_p$ ενδομορφισμό του $A/\mathfrak{n}A$. Σημειώνουμε με $g_a = (a_{ij})$ τον πίνακα που αντιστοιχεί στο a (σε σχέση πάντα με το $\mathcal{E}$). Ορίζουμε μά (νέα) A−δράση $(\star)$ στο $A/\mathfrak{n}A$:

$$a \star x = \kappa^{-1}(a \cdot x^*).$$

Σημειώνουμε ότι $\forall a, b \in A,\ g_a g_b = g_b g_a$. Έστω $x \in A/\mathfrak{n}A,\ x = \sum_i \lambda_i x_i$. Τότε, $x^* = \sum_i \lambda_i x_i^*$ και $(a \star x) = \kappa^{-1}(a \cdot x^*)$. Αλλά $a \cdot x^* = a \cdot \sum_i \lambda_i x_i^* = \sum \lambda_i a \cdot x_i^*$ και ως εκ τούτου, για κάθε j, $a \cdot x^*(x_j) = \sum_i \lambda_i x_i^*(a x_j) = \sum_i \lambda_i x_i^*(g_a x_j) = \sum_i \lambda_i a_{ij}$. Αυτό αποδεικνύει ότι $a \star x = g_a^t \cdot x$, όπου τα g_a^t συμβολίζουν τον ανάστροφο πίνακα του g_a. Ως εκ τούτου, θεωρούμενα ως A modules, τα $\mathrm{Hom_{\mathbf{F}_p}(A/\mathfrak{n}A, \mathbf{F}_p)}$ και $(A/\mathfrak{n}A, \star)$ είναι ισόμορφα.

Περνόντας στις r exterior powers, παίρνουμε $B-$ομομορφισμούς

$$\wedge\lambda : \bigwedge^r M_\psi \longrightarrow \bigwedge^r M_\phi,$$

και μία ισογένεια

$$\wedge\lambda : \wedge\phi \longrightarrow \wedge\psi.$$

Θεωρημα 3.2.2. *Υπάρχει ένας μορφισμός*

$$\mathcal{W}_\mathfrak{n} : Y^r(\mathfrak{n}) \longrightarrow Y^1(\mathfrak{n})$$

Απόδειξη. Έστω ϕ ένα Drinfeld module τάξεως r ορισμένο πάνω από ένα σώμα $L \supseteq K$, με μία $\mathfrak{n}-$level structure δοσμένη από το

$$\alpha : (A/\mathfrak{n}A)^r \longrightarrow \phi[\mathfrak{n}].$$

Έστω $\wedge\phi$ η ορίζουσα του ϕ. Είναι προφανές ότι ο ισομορφισμός είναι $\mathrm{Gal}(K^{\mathrm{sep}}/K)-$αναλλοίωτος. Από την πρόταση 3.2.1 έχουμε ότι $(\wedge\phi)[\mathfrak{n}] \sim \wedge(\phi[\mathfrak{n}])$. Περνόντας στις exterior powers, παίρνουμε τον επιθυμητό μορφισμό (την level structure)

$$\wedge\alpha\colon A/\mathfrak{n} \cong \bigwedge(A/\mathfrak{n}A)^r \longrightarrow \wedge^r(\phi[\mathfrak{n}]) \cong (\wedge\phi)[\mathfrak{n}].$$

❏

3.2.1 Το σώμα ορισμού των Moduli schemes

Για ένα πρώτο $\mathfrak{p}$ έστω $K(\mathfrak{p})$ το σώμα που περιέχει το K και τα $\mathfrak{p}$ σημεία πεπερασμένης τάξης του Carlitz module $C_T = T + \tau$. Θα σημειώνουμε με $K_+(\mathfrak{p})$ τη maximal αβελιανή επέκταση του K, την περιεχόμενη στο $K(\mathfrak{p})$, στην οποία το ∞ αναλύεται πλήρως. Έστω K_+ η maximal αβελιανή επέκταση του K στην οποία το ∞ αναλύεται πλήρως. Το moduli scheme των Drinfeld modules τάξεως ένα με $\mathfrak{p}$ level structure η οποία ορίζεται πάνω από $K-$σώματα είναι το K_+ (δες Goss [13] και Hayes [21]).

Από το θεώρημα 3.2.2, για $\mathfrak{p}$ πρώτο του A υπάρχει ένας dominant μορφισμός, ο Weil μορφισμός, ώστε για κάθε πρώτο ιδεώδες $\mathfrak{p}$ του $A = \mathbf{F}_p[T]$ να έχουμε

$$\mathcal{W}_\mathfrak{p} : Y^r(\mathfrak{p}) \longrightarrow Y^1(\mathfrak{p}).$$

Παίρνοντας την δυϊκή του $\mathcal{W}_\mathfrak{p}$ (δηλ. περνόντας στις global sections) έχουμε ένα μονομορφισμό δακτυλίων

$$\Gamma(Y^1(\mathfrak{p}), \mathcal{O}_{Y^1(\mathfrak{p})}) \longrightarrow \Gamma(Y^r(\mathfrak{p}), \mathcal{O}_{Y^r(\mathfrak{p})}).$$

Επειδή $\Gamma(Y^1(\mathfrak{p}), \mathcal{O}_{Y^1(\mathfrak{p})}) = K_+(\mathfrak{p})$ (δες 3.1.1), παίρνουμε το ακόλουθο

Θεωρημα 3.2.3. *Το σώμα ορισμού της $Y^r(\mathfrak{p})$ περιέχει το σώμα $K_+(\mathfrak{p})$.*

3.2.2 Δράση οριζουσών

Έστω $\mathcal{M}^m(\mathfrak{a})$ ο contravariant functor από την κατηγορία των $K-$ σωμάτων στην κατηγορία των συνόλων $\mathcal{M}^m(\mathfrak{a}) : (K-\text{σώματα}) \longrightarrow (\text{σύνολα})$, $L \longmapsto \mathcal{M}^m(\mathfrak{a})(L)$ όπου $\mathcal{M}^r(\mathfrak{a})(L)$ σημειώνει το σύνολο των κλάσεων ισομορφίας των Drinfeld modules τάξεως m των οριζόμενων υπέρ το L με $\mathfrak{a}-$level structure.

Η ομάδα $\mathrm{GL}(r, A/\mathfrak{n})/\mathbf{F}_p^*$ δρα στο $\mathcal{M}^r(\mathfrak{n})$ και η ομάδα $\mathrm{GL}(1, \mathfrak{n})/\mathbf{F}_p^*$ δρα στο $\mathcal{M}^1(\mathfrak{n})$. Έστω $g \in \mathrm{GL}(r, A/\mathfrak{n})/\mathbf{F}_p^*$. Θεωρούμε το ακόλουθο διάγραμμα

$$\begin{tikzcd}
\mathcal{M}^r(\mathfrak{n}) \arrow[r, "g"] \arrow[d, "\mathcal{W}_\mathfrak{n}"'] & \mathcal{M}^r(\mathfrak{n}) \arrow[d, "\mathcal{W}_\mathfrak{n}"] \\
\mathcal{M}^1(\mathfrak{n}) \arrow[r, "\det g"] & \mathcal{M}^1(\mathfrak{n})
\end{tikzcd}
\qquad\qquad
\begin{tikzcd}
(\phi, i) \arrow[r, mapsto, "g"] \arrow[d, mapsto, "\mathcal{W}_\mathfrak{n}"'] & (\phi, i_g) \arrow[d, "\mathcal{W}_\mathfrak{n}"] \\
(\wedge\phi, \wedge i) \arrow[r, mapsto, "\det g"] & (\phi, \wedge i \det g)
\end{tikzcd}$$

Το παραπάνω διάγραμμα είναι αντιμεταθετικό. Έτσι έχουμε το ακόλουθο

Θεωρημα 3.2.4. *Η ομάδα* $\mathrm{GL}(r, A/\mathfrak{n})/\mathbf{F}_p^*$ *δρα στο* $K_+(\mathfrak{n})$ *όπως η ορίζουσα.*

Η υλοποιηση της PSL

Έστω $\mathfrak{p}$ πρώτος του A και $r = 2s$ άρτιος με $\gcd(s, q^d - 1) = 1$. Έστω $Y^r(\mathfrak{p})$ το moduli scheme των Drinfeld modules τάξεως r, με $\mathfrak{p}$-level structure. Η ομάδα $\mathrm{GL}(r, A/\mathfrak{p})/\mathbf{F}_p^*$ δρα στον $Y^r(\mathfrak{p})$. Το πηλίκο της δράσης είναι το $Y^r(1)$ —το moduli scheme των Drinfeld modules τάξεως r. Το σώμα ορισμού της $Y^r(\mathfrak{p})$ περιέχει το $K_+(\mathfrak{p})$. Η ομάδα $\mathrm{GL}(r, A/\mathfrak{p})/\mathbf{F}_p^*$ δρα στο $K_+(\mathfrak{p})$ όπως η ορίζουσα. Ως εκ τούτου, η υποομάδα των πινάκων της $\mathrm{GL}(r, A/\mathfrak{p})/\mathbf{F}_p^*$ με ορίζουσα στο $\mathbf{F}_p^*$ δρα στον $Y^r(1) \times \mathrm{Spec}(K_+(\mathfrak{p}))$ τετριμμένα.

4.1 Το moduli scheme $Y_0^r(\mathfrak{n})$

4.1.1 Η κατασκευή του $Y_0^r(\mathfrak{n})$

Έστω L σώμα που περιέχει το K, ϕ ένα Drinfeld module γενικής χαρακτηριστικής τάξεως r που ορίζεται πάνω από το L και $\mathfrak{n}$ ένα μη τετριμμένο πολυώνυμο του A. Συμβολίζουμε με L' το σώμα διάσπασης του διαχωρισίμου πολυωνύμου $\phi_{\mathfrak{n}}(X)$.

Ορισμος 4.1.1.

α'. *Η Borel υποομάδα* $\mathrm{B}(\mathfrak{n})$ *του* $\mathrm{GL}(2, n)$ *είναι η υποομάδα των άνω τριγωνικών πινάκων.*

β'. *Δύο $A-$ισομορφισμοί $i, i' : (A/\mathfrak{n})^r \longrightarrow \phi[\mathfrak{n}]$ ονομάζονται* Borel ισοδύναμοι *αν υπάρχει ένα στοιχείο $g \in \mathrm{B}(\mathfrak{n})$ με $i = gi'$.*

γ'. *Μία* full flag *υποομάδων του $\phi[\mathfrak{n}]$ είναι μία ακολουθία υποομάδων του $\phi[\mathfrak{n}]$,*

$$C_1 \leq C_2 \leq \cdots \leq C_r = \phi[\mathfrak{n}]$$

τέτοια, ώστε η C_1 και οι C_{i+1}/C_i για $i = 1, \cdots, r-1$ να είναι ισόμορφες με το $A/\mathfrak{n}A$.

δ'. *Μία* Borel flag *υποομάδων $\phi[\mathfrak{n}]$ είναι μία flag υποομάδων του $\phi[\mathfrak{n}]$ μαζί με μία Borel ισοδυναμία $i : (A/\mathfrak{n}A)^r \longrightarrow \phi[\mathfrak{n}]$*

ε'. *Ένα $L-$*ρητό σημείο *$(\phi, \{C_1 \leq C_2 \leq \cdots \leq C_r = \phi[\mathfrak{n}]\})$ αποτελείται από*

  (α') ένα Drinfeld module τάξεως r οριζόμενο υπέρ το L,

  (β') μία Borel flag υποομάδων $C_1 \leq C_2 \leq \cdots \leq C_r$ του $\phi[\mathfrak{n}]$ υπέρ L', με $C_s \leq L$ και $C_i^g = C_i, \forall i$ και $g \in \mathrm{Gal}(K^{\mathrm{sep}}/L)$.

Σημείωση 6. Μέσω της β', μπορούμε να ταυτίσουμε την ομάδα Galois της L'/L με μία υποομάδα της $\mathrm{B}(\mathfrak{n})$.

Θεωρούμε τον contravariant functor $\mathcal{M}_0^r(\mathfrak{n})$ από την κατηγορία των επεκτάσεων του K στην κατηγορία των συνόλων

$$\mathcal{M}_0^r(\mathfrak{n}) : (L\colon L \supset K) \longrightarrow (\text{Σύνολα}), \quad L \longmapsto \mathcal{M}_0^r(\mathfrak{n})(\mathrm{Spec}(L))$$

ο οποίος σε ένα σώμα L με $L \supset K$ αντιστοιχεί τις κλάσεις ισομορφίας των δυάδων (ϕ, flag).

Έστω $\mathcal{B}$ ο δακτύλιος για τον οποίο το scheme $\mathrm{Spec}(\mathcal{B})$ αναπαριστά τον functor $\mathcal{Y}^r(\mathfrak{n})$. Η ομάδα $\mathrm{GL}(r, A/\mathfrak{n})/\mathbf{F}_q^*$ δρα στον $\mathcal{B}$. Έστω $\mathcal{D}$ ο δακτύλιος των αναλλοιώτων του $\mathcal{B}$ κάτω από τη δράση της ομάδας αυτής. Στην παρακάτω πρόταση δείχνουμε ότι functor $\mathcal{Y}_0^r(\mathfrak{n})$ αναπαρίσταται ασθενώς (coarsly) από το scheme $\mathrm{Spec}(\mathcal{D})$.

ΠΡΟΤΑΣΗ 4.1.1. *Το* $Y_0(\mathfrak{n}) := \mathrm{Spec}(\mathcal{C})$ *είναι το coarse moduli scheme του* $\mathcal{M}_0^r(\mathfrak{n})$.

Απόδειξη. Έστω $(\phi, flag)$ δυάδα υπέρ το L, και έστω L' το σώμα διάσπασης του πολυωνύμου $\phi_{\mathfrak{n}}(X)$. Έστω $\mu : \mathrm{Spec}(L') \longrightarrow \mathrm{Spec}(L)$ ο κανονικός μορφισμός. Επεκτείνοντας τις σταθερές το ϕ γίνεται Drinfeld module υπέρ το L'. Έστω

$$i : (A/\mathfrak{n}A)^r \xrightarrow{\sim} \phi[\mathfrak{n}]$$

ένας $A-$ισομορφισμός υπέρ το L'. Ο αυτομορφισμός αυτός αντιστοιχεί σε μία $\mathfrak{n}$-level structure του ϕ υπέρ το L'— έστω (ϕ, i) η αντίστοιχη δυάδα. Αφού το moduli scheme $Y^r(\mathfrak{n})$ είναι fine, το παραπάνω ζεύγος αντιστοιχεί με μοναδικό τρόπο σε ένα μορφισμό $\xi' : \mathrm{Spec}(L') \longrightarrow Y^r(\mathfrak{n})$. Η εικόνα του ξ' αντιστοιχεί σε ένα maximal ιδεώδες του $\mathcal{B}$ έστω το $\mathfrak{M}$. Αφού η επέκταση δακτυλίων $\mathcal{B}/\mathcal{C}$ είναι ακέραια, η προβολή του $\mathfrak{M}$ στον $\mathcal{C}$, έστω $\mathfrak{P}$, θα είναι ένα maximal ιδεώδες. Ορίζουμε ως ξ: $\mathrm{Spec}(\mathcal{B}/\mathfrak{P}) \longrightarrow \mathrm{Spec}(\mathcal{B})$ το φυσικό μορφισμό. Είναι προφανής η ύπαρξη των μορφισμών $\mathrm{Spec}(L') \longrightarrow \mathrm{Spec}(\mathcal{B}/\mathfrak{P})$ και $\mathrm{Spec}(L) \longrightarrow \mathrm{Spec}(\mathcal{C}/\mathfrak{P})$ και $\mathrm{Spec}(L') \longrightarrow \mathrm{Spec}(\mathcal{C}/\mathfrak{P})$. Υποστηρίζουμε ότι υπάρχει ένας μορφισμός $\mathrm{Spec}(L) \longrightarrow Y_0^r(\mathfrak{n})$ ο οποίος κάνει το ακόλουθο διάγραμμα αντιμεταθετικό:

$$\begin{tikzcd}
\mathrm{Spec}(L') \arrow[r] \arrow[d] \arrow[rr, bend left, "\xi'"] & \mathrm{Spec}(\mathcal{B}/\mathfrak{P}) \arrow[r, "\xi"'] \arrow[d, "\mu"] & Y^r(\mathfrak{n}) \arrow[d, "\pi"'] \\
\mathrm{Spec}(L) \arrow[r, dotted, "\exists"] & \mathrm{Spec}(\mathcal{C}/\mathfrak{P}) \arrow[r] & Y_0^r(\mathfrak{n})
\end{tikzcd}$$

Η ομάδα αυτομορφισμών G της L'/Lεμφυτεύεται στην Borel ομάδα $\mathrm{B}(\mathfrak{n})$: έστω $g \in G$, τότε ο μορφισμός $\mathrm{Spec}(L)' \xrightarrow{g} \mathrm{Spec}(L)' \xrightarrow{\xi'} Y^r(\mathfrak{n})$ αντιστειχεί σε ένα maximal ιδεώδες $\mathfrak{M}'$ του $\mathcal{B}$. Συμβολίζουμε με g τον (μοναδικό) αυτομορφισμό του $\mathcal{B}$ που στέλνει το $\mathfrak{M}$ στο $\mathfrak{M}'$. Ο μορφισμός ξ' παραγοντοποιείται μέσω του ξ και του μ: $\mathrm{Spec}(\mathcal{B}/\mathfrak{P}) \longrightarrow \mathrm{Spec}(\mathfrak{M})$, όπου $\mathfrak{P}$ είναι η εικόνα του $\mathfrak{M}$ μέσω του π. Το σώμα $\mathcal{C}/\mathfrak{P}$ είναι υπόσωμα του $\mathcal{B}/\mathfrak{M}$ και μάλιστα σταθεροποιείται από τον αυτομορφισμό g, για κάθε $g \in G$. Έτσι το σώμα $\mathcal{C}/\mathfrak{P}$ είναι υπόσωμα του L, από όπου και ο μορφισμός $\mathrm{Spec}(L) \longrightarrow \mathrm{Spec}(\mathcal{C}/\mathfrak{P}) \longrightarrow Y^r(\mathfrak{n})$. Συμβολίζουμε με ν τον μορφισμό $\mathrm{Spec}(L) \longrightarrow Y^r(\mathfrak{n})$.

Υποστηρίζουμε ότι ο ν είναι ανεξάρτητος από την επιλογή του i. Πράγματι, έστω i' μία άλλη $\mathfrak{n}$–level structure η οποία σέβεται την Borel structure του $\phi[\mathfrak{n}]$ δηλ. $i' = gi$ για ένα $g \in \mathrm{B}(\mathfrak{n})$. Έστω χ': $\mathrm{Spec}(L') \longrightarrow Y^r(\mathfrak{n})$ και ν': $\mathrm{Spec}(L) \longrightarrow Y_0^r(\mathfrak{n})$ οι αντίστοιχοι μορφισμοί. Είναι φανερό ότι $\xi' \circ g = \xi'$ και άρα $\nu' = \nu$.

Για δυάδες $(\phi, flag)$ πάνω από αλγεβρικά κλειστά σώματα $k \supset K$ ο functor $\mathcal{M}_0^r(\mathfrak{n})$ είναι ένας ισομορφισμός: αρκεί να δειχθεί ότι για κάθε αλγεβρικά κλειστό σώμα $k \supset K$ τα k ρητά σημεία του $Y_0^r(\mathfrak{n})$ (με άλλα λόγια τα $Y_0^r(\mathfrak{n})(k)$) αντιστοιχούν με τρόπο μοναδικό σε Drinfeld modules που ορίζονται πάνω από το k —μαζί με μία (δοσμένη) Borel flag structure.

Έστω $\nu : \mathrm{Spec}(k) \longrightarrow Y_0^r(\mathfrak{n})$ μορφισμός. Θα δείξουμε ότι υπάρχει μία δυάδα (ϕ, flag) που αντιπροσωπεύει το ν. Αφού το k είναι σώμα, η εικόνα του μέγιστου ιδεώδους είναι ένα γεωμετρικό σημείο $x \in Y_0^r(\mathfrak{n})$ με $\mathrm{quot}(x) = k$. Κάθε σημείο της ίνας του x (σε σχέση με το μορφισμό π) είναι επίσης γεωμετρικό k-ρητό σημείο του $Y^r(\mathfrak{n})$. Έστω $y \in Y_0^r(\mathfrak{n})$ ένα από αυτά. Ο ομομορφισμός

$$\mathcal{O}_{Y_0^r(\mathfrak{n}),x} \longrightarrow \mathcal{O}_{Y^r(\mathfrak{n}),y}$$

επάγει τον ομομορφισμό

$$\mathcal{O}_{Y_0^r(\mathfrak{n}),x}/P_x \longrightarrow \mathcal{O}_{Y^r(\mathfrak{n}),y}/P_y$$

ο οποίος με τη σειρά του επάγει τον μορφισμό (δες την άσκηση 2.7 στη σελ. 80 του [20])

$$\alpha\colon k \longrightarrow Y^r(\mathfrak{n})$$

(εδώ το $\mathcal{O}$ συμβολίζει το structure sheaf ενώ το P_x συμβολίζει το maximal ιδεώδες του $\mathcal{O}_x$ που αντιστοιχεί σε αυτό). Έστω $(\phi, i_{\mathfrak{n}})$ ένα Drinfeld module που αντιστοιχεί στον α. Κάθε άλλο σημείο z στην ίνα του x

είναι $\mathrm{B}(\mathfrak{n})$-συζυγές του y, δηλ. υπάρχει ένα $g \in \mathrm{B}(\mathfrak{n})$ με $g(y) = z$. Έστω $(\psi, i'_{\mathfrak{n}})$ η δυάδα που αντιστοιχεί στο z. Η $\mathrm{B}(\mathfrak{n})$ δρα στο $Y^r(\mathfrak{n})$ μεταθέτοντας απλώς την level structure (αφού και η $\mathrm{GL}(r, A/\mathfrak{n})/\mathbf{F}_p^*$ δρα έτσι και $\mathrm{B}(\mathfrak{n}) \leq \mathrm{GL}(r, A/\mathfrak{n})/\mathbf{F}_p^*$). Έτσι, $\phi = \psi$ και $i_{\mathfrak{n}} = g i'_{\mathfrak{n}}$. Είναι φανερό ότι η flag η οριζόμενη από την ν επάγεται από την level structure $i_{\mathfrak{n}}$ «modulo» $\mathrm{B}(\mathfrak{n})$ ❑

4.1.2 Βασικές ιδιότητες

Έστω L σώμα που περιέχει το K. Έστω $\mathfrak{n}$ και $\mathfrak{m}$ πρώτα μεταξύ τους ιδεώδη του A με $d = \deg(\mathfrak{m})$ και $r = 2s$ άρτιους.

Λημμα 4.1.1.

α΄. $Y^r(\mathfrak{nm}) = Y^r(\mathfrak{n}) \times Y^r(\mathfrak{m})$

β΄. $Y^r(\mathfrak{n}) \times Y^r(\mathfrak{m}) \longrightarrow Y^r(1)$ *είναι ένας normal μορφισμός (με την έννοια της θεωρίας του Galois).*

Απόδειξη. 1. Έστω $f \colon Y^r(\mathfrak{nm}) \longrightarrow Y^r(\mathfrak{n}) \times Y^r(\mathfrak{m})$ ο μορφισμός ο οριζόμενος μέσω του fiber product των απεικονίσεων: $Y^r(\mathfrak{nm}) \longrightarrow Y^r(\mathfrak{n})$ και $Y^r(\mathfrak{nm}) \longrightarrow Y^r(\mathfrak{m})$. Ορίζουμε μία απεικόνιση $g \colon Y^r(\mathfrak{n}) \times Y^r(\mathfrak{m}) \longrightarrow Y^r(\mathfrak{nm})$ ως εξής: Ένα στοιχείο $a \in Y^r(\mathfrak{n}) \times Y^r(\mathfrak{m})$ αντιστοιχεί σε ένα μοναδικό Drinfeld module ϕ με την έννοια του ακόλουθου αντιμεταθετικού διαγράμματος:

$$\begin{tikzcd}
& Y^r(\mathfrak{n}) \times Y^r(\mathfrak{m}) \arrow[dl, "\pi_{\mathfrak{n}}"'] \arrow[dr, "\pi_m"] & \\
Y^r(\mathfrak{n}) \arrow[dr] \arrow[rr, phantom, "="] & & Y^r(\mathfrak{m}) \arrow[dl] \\
& Y^r(1) &
\end{tikzcd}$$

Έτσι, η εικόνα του a μέσω της $\pi_{\mathfrak{n}}$ είναι $(\phi, i_{\mathfrak{n}})$ και μέσω της $\pi_{\mathfrak{m}}$ είναι $(\phi, i_{\mathfrak{m}})$, για κατάλληλες $\mathfrak{n}$ και $\mathfrak{m}$ level structures. Αφού τα $\mathfrak{n}, \mathfrak{m}$ είναι πρώτα μεταξύ τους, οι $i_{\mathfrak{n}}$ και $i_{\mathfrak{m}}$ ορίζουν μέσω της

$$I_{\mathfrak{nm}} : (A/\mathfrak{nm})^r \longrightarrow (A/\mathfrak{n}A)^r \times (A/\mathfrak{m}A)^r$$

ένα A-ισομορφισμό $i_{\mathfrak{nm}} : (A/\mathfrak{nm}A)^r \longrightarrow \phi[\mathfrak{nm}]$.

Είναι τώρα σαφές, ότι $n \circ m = \mathbf{1}$ και $m \circ n = \mathbf{1}$.

2. Προφανώς, αφού τόσο ο μορφισμός $Y_0^r(\mathfrak{n}) \longrightarrow Y^r(1)$ όσο και ο $Y^r(\mathfrak{m}) \longrightarrow Y^r(1)$ είναι normal (δες [6, κεφ. 3]).

❑

4.1.3 Το moduli scheme $Y_0^r(T)$.

Έστω x ένα L-ρητό σημείο του $Y_0^r(T)$. Έστω $(\phi, \{C_1 \leq \cdots \leq C_r = \phi[\mathfrak{n}]\})$ η αντίστοιχη δυάδα που αντιστοιχεί στο x. Θυμίζουμε ότι το $C_s \leq L$ και το $C_i^g = C_i$ για όλα τα i και $g \in \mathrm{Gal}(K^{sep}/L)$. Επειδή οι συντελεστές του ϕ_T ανήκουν L και επειδή οι πεπερασμένες ομάδας C_i είναι Galois-αναλλοίωτες και ο δακτύλιος $L\{\tau\}$ είναι περιοχή κυρίων ιδεωδών ως προς τα δεξιά του ιδεώδη, υπάρχουν $\forall i, \exists a_i, b_i \in L$ με

$$\phi_T = (a_1\tau + b_1) \cdots (a_r\tau + b_r),$$

και μάλιστα οι ρίζες του $(a_i\tau + b_i) \cdots (a_r\tau + b_r)$ σχηματίζουν ένα A module ισόμορφο προς το C_i.

Προταση 4.1.2. *Το $Y_0^r(T)$ είναι ένα ρητό scheme.*

Απόδειξη. Έστω ϕ ένα Drinfeld module οριζόμενο υπέρ το L με μία full flag υποομάδων του $\phi[T]$. Μπορούμε να γράψουμε το ϕ_T ως ένα γινόμενο

$$\phi_T = (a_1\tau + b_1)\cdots(a_{r-1}\tau + b_{r-1})(a_r\tau + b_r),$$

όπου $a_i, b_i \in L^*$. Αφού οι ρίζες του $a_r X^p + b_r X$ ανήκουν στο L, υπάρχει ένα στοιχείο $d_\phi \in L$ με $d_\phi^{p-1} = \frac{a_r}{b_r}$. Θέτουμε

$$\begin{array}{llll} u_r = \frac{b_r}{d_\phi} & \text{και} & u_{i-1} = b_{i-1}u_i & \text{για } i = 2, \dots, r \\ X_r = 1 & \text{και} & X_{i-1} = \frac{a_{i-1}}{b_{i-1}}u_{i+1}^{p-1} & \text{για } i = 2, \dots, r. \end{array}$$

Σημειώνουμε ότι $u_1 = Td^{-1}$. Τότε,

$$\begin{aligned}
&(a_1\tau + b_1)\cdots(a_{r-1}\tau + b_{r-1})(a_r\tau + b_r) = \\
&(a_1\tau + b_1)\cdots(a_{r-1}\tau + b_{r-1})\boldsymbol{b_r}(a_r\boldsymbol{b_r^{-1}}\tau + \mathbf{1}) = \\
&(a_1\tau + b_1)\cdots(a_{r-1}\tau + b_{r-1})\boldsymbol{b_r d_\phi^{-1}}(\boldsymbol{d_\phi^p}\tau + \boldsymbol{d_\phi}) = \\
&(a_1\tau + b_1)\cdots(a_{r-1}\tau + b_{r-1})\boldsymbol{u_r}(\tau + 1)\boldsymbol{d_\phi} = \\
&(a_1\tau + b_1)\cdots(a_{r-1}\boldsymbol{u_r^p}\tau + b_{r-1}\boldsymbol{u_r})(\tau + 1)d_\phi = \\
&(a_1\tau + b_1)\cdots(a_{r-1}u_r^p\tau + \boldsymbol{u_{r-1}})(\tau + 1)d_\phi = \\
&(a_1\tau + b_1)\cdots\boldsymbol{u_{r-1}}(\boldsymbol{\tfrac{a_{r-1}}{b_{r-1}}u_r^{p-1}}\tau + 1)(\tau + 1)d_\phi = \\
&(a_1\tau + b_1)\cdots(a_{r-2}\boldsymbol{u_{r-1}^p}\tau + b_{r-2}\boldsymbol{u_{r-1}})(X_{r-1}\tau + 1)(\tau + 1)d_\phi = \\
&(a_1\tau + b_1)\cdots(a_{r-2}\boldsymbol{u_{r-1}^p}\tau + \boldsymbol{u_{r-2}})(X_{r-1}\tau + 1)(\tau + 1)d_\phi = \\
&\vdots \qquad\qquad\qquad\qquad \vdots \qquad\qquad\qquad\qquad \vdots \\
&(a_1\tau + b_1)\boldsymbol{u_1}(X_2\tau + 1)\cdots(X_{r-2} + 1)(X_{r-1}\tau + 1)(\tau + 1)d_\phi = \\
&(a_1T^p d_\phi^{-p}\tau + Td^{-1})(X_2\tau + 1)\cdots(X_{r-1}\tau + 1)(\tau + 1)d_\phi \sim \\
&\boldsymbol{d_\phi}(a_1T^p d_\phi^{-p}\tau + Td^{-1})(X_2\tau + 1)\cdots(X_{r-1}\tau + 1)(\tau + 1)d_\phi\boldsymbol{d_\phi^{-1}} \sim \\
&(\boldsymbol{a_1T^p d_\phi^{1-p}}\tau + T)(X_2\tau + 1)\cdots(X_{r-1}\tau + 1)(\tau + 1) = \\
&(\boldsymbol{X_1}\tau + T)\cdots(X_{r-1}\tau + 1)(\tau + 1).
\end{aligned}$$

Έστω τώρα $(\psi, \{C_1' \le \cdots \le C_r' = \psi[T]\})$ μία δυάδα ισόμορφη προς την $(\phi, \{C_1 \le \cdots \le C_r = \phi[T]\})$. Τότε υπάρχει $u \in L^*$ με

- $u : \psi \longrightarrow \phi$ είναι ένας ισομορφισμός στην κατηγορία των Drinfeld modules
- $\phi[T] \xrightarrow{\sim} \psi[T]$ και $uC_i = C_i'$.

Τότε

$$\begin{aligned}
\phi_T = u^{-1}\phi_T u = &u^{-1}(a_1\tau + b_1)\cdots(a_r\tau + b_r)u = \\
&u^{-1}(a_1\tau + b_1)uu^{-1}(a_2\tau + b_2)u^{-1}u\cdots uu^{-1}(a_r\tau + b_r)u = \\
&(a_1u^{p-1}\tau + b_1)\cdots(a_ru^{p-1}\tau + b_r).
\end{aligned}$$

Θέτουμε $d_\psi = d_\phi u$, δηλαδή, $d_\psi^{p-1} = \frac{u^{p-1}a_r}{b_r}$ και

$$\begin{array}{llll} v_r = \frac{b_r}{d_\psi} & \text{και} & v_{i-1} = b_{i-1}v_i & \text{για όλα τα } i = 2, \dots, r \\ Y_r = 1 & \text{και} & Y_{i-1} = \frac{u^{p-1}a_{i-1}}{b_{i-1}}v_{i+1}^{p-1} & \text{για όλα τα } i = 2, \dots, r. \end{array}$$

Τότε, $uv_i = u_i$ και $X_i = Y_i$ για όλα $i = 1, \dots, r$. ❑

4.2 Ο Fricke αυτομορφισμός

Έστω $\langle \mathfrak{p} \rangle$ ένας πρώτο ιδεώδες του A με $d := \deg \mathfrak{p}$ άρτιο και $r = 2s \in \mathbf{N}$ φυσικό αριθμό. Έστω $x := (\phi, \{C_1 \le \cdots \le C_s \le C_{s+1} \le \cdots \le C_r = \phi[T]\})$ ένα L–ρητό σημείο του $Y_0^r(T)$ και λ πολυώνυμο με ρίζες τα στοιχεία της C_s. Είναι εύκολο να δειχτεί ότι υπάρχει ένα Drinfeld module ψ ισογενές ως προς το ϕ με πυρήνα τις ρίζες του λ, δηλαδή

$$\lambda \colon \phi \longrightarrow \psi,$$

ισογένεια με πυρήνα το C_s.

Ορισμος 4.2.1. *Το ψ αναφέρεται ως «πηλίκο» του ϕ με την C_s.*

Ορισμος 4.2.2. *Ορίζουμε μία involution w στο $Y_0^r(T)$ ως ακολούθως: Έστω $x \in Y_0^r(T)(L)$ ένα $L-$ρητό σημείο το οποίο αντιπροσωπεύεται από τη δυάδα $(\phi, \{C_1 \leq \cdots \leq C_r = \phi[T]\})$. Με $w(x)$ θα συμβολίζουμε το σημείο που αντιπροσωπεύεται από τη δυάδα*

$$(\psi, \{C_1' \leq \cdots \leq C_r' = \psi[T]\})$$

όπου

1. *το ψ είναι ένα Drinfeld module-πηλίκο του ϕ με την C_s*
2. *$C_1' = \lambda(C_{s+1}), \ldots, C_s' = \lambda(C_r)$ και*
3. *$C_{s+1}' = \hat{\lambda}^{-1}(C_1), \ldots, C_r' = \hat{\lambda}^{-1}(C_s)$*

και $\hat{\lambda}$ δυική ισογένεια λ. Η involution αυτή θα ονομάζεται Fricke involution.

4.2.1 Το twisted scheme Y

Συμβολισμός 4. Έστω $K_* = K(\sqrt{\mathfrak{p}})$ και σ ο μη τετριμμένος αυτομορφισμός της K_*/K. Συμβολίζουμε με Z το πηλίκο του $Y_0^r(T)$ κάτω από τη δράση της Fricke involution w, δηλαδή $Z = Y_0^r(T)/w$.

Ορισμος 4.2.3. *Το scheme Y είναι το twist του $Y_0^r(\mathfrak{n})$ σε σχέση με το K_*, με άλλα λόγια το Y είναι το πηλίκο του $Y_0^r(T) \times K_*$ με την $\langle \sigma w \rangle$.*

$$\begin{tikzcd}
 & Y_0^r(T) \times K_* \arrow[dl, "\sigma"'] \arrow[d, dashed, "\sigma w"] \arrow[dr] & \\
Y_0^r(T) \arrow[dr, "w"'] & Y \arrow[d, dashed] & Z \times K_* \arrow[dl] \\
 & Z &
\end{tikzcd}$$

Προταση 4.2.1. *Η Fricke involution w δρα στο $Y_0^r(T)$ ως ένας ρητός μετασχηματισμός ο οποίος ορίζεται υπέρ το K.*

Απόδειξη. Η Fricke involution δρα στο $Y_0^r(T)$ με τον ακόλουθο τρόπο:

$$(X_1\tau + T)\cdots(X_s\tau + 1)(X_{s+1} + 1)\cdots(\tau + 1) \longmapsto$$
$$(X_{s+1}\tau + 1)\cdots(\tau + 1)(X_1\tau + T)\cdots(X_s\tau + 1)$$

Θέτουμε $d_s^{p-1} = X_s, d_s \in K^{\text{sep}}$. (Τα τονισμένα σύμβολα, τονίζουν την εξέλιξη της διαδικασίας.) Υπέρ το K^{sep} η w διασπάται στα σκόλουθα βήματα:

$$\begin{aligned}
&(X_{s+1}\tau + 1)\cdots(X_{r-1}\tau + 1)(\tau + 1)(X_1\tau + T)\cdots(X_s\tau + 1) = \\
&(X_{s+1}\tau + 1)\cdots(X_{r-1}\tau + 1)(\tau + 1)(X_1\tau + T)\cdots(\boldsymbol{d_s^{p-1}}\tau + 1) = \\
&(X_{s+1}\tau + 1)\cdots(\tau + 1)(X_1\tau + T)\cdots(X_{s-1}\tau + 1)\boldsymbol{d_s^{-1}}(\boldsymbol{d_s^p}\tau + \boldsymbol{d_s}) \sim \\
&(X_{s+1}\tau + 1)\cdots(X_{r-1}\tau + 1)(\tau + 1)(X_1\tau + T)\cdots(X_{s-1}\boldsymbol{d_s^{-p}}\tau + \boldsymbol{d_s^{-1}}\boldsymbol{)}(d_s^p\tau + d_s) = \\
&(X_{s+1}\tau + 1)\cdots(X_{r-1}\tau + 1)(\tau + 1)(X_1\tau + T)\cdots\boldsymbol{d_s^{-1}}(X_{s-1}d_s^{1-p}\tau + 1)(d_s^p\tau + d_s) = \\
&(X_{s+1}\tau + 1)\cdots(X_{r-1}\tau + 1)(\tau + 1)(X_1\boldsymbol{d_s^{-p}}\tau + T\boldsymbol{d_s^{-1}}\boldsymbol{)\cdots}(X_{s-1}d_s^{1-p}\tau + 1)(d_s^p\tau + d_s) \sim \\
&(X_{s+1}\tau + 1)\cdots(X_{r-1}\tau + 1)(\tau + 1)\boldsymbol{T d_s^{-1}}(X_1 d_s^{-p+1}T^{-1}\tau + 1)\cdots(X_{s-1}d_s^{-p+1}\tau + 1)(d_s^p\tau + d_s) = \\
&(X_{s+1}\tau + 1)\cdots(\boldsymbol{d_s^{-p}T^p}\tau + \boldsymbol{d_s^{-1}T})(X_1 d_s^{-p+1}T^{-1}\tau + 1)\cdots(X_{s-1}d_s^{-p+1}\tau + 1)(d_s^p\tau + d_s) = \\
&\boldsymbol{(d_s T^{-p}}X_{s+1}\tau + 1\boldsymbol{d_s^{-1}T)\cdots(d_s^{-p}T^p d_s T^{-1}}\tau + 1)\cdots(X_{s-1}d_s^{-p+1}\tau + 1)(d_s^p\tau + d_s) \sim \\
&\boldsymbol{d_s}(d_s T^{-p}X_{s+1}\tau + 1d_s^{-1}T)\cdots(d_s^{-p}T^p d_s T^{-1}\tau + 1)\cdots(X_{s-1}d_s^{-p+1}\tau + 1)(d_s^p\tau + d_s)\boldsymbol{d_s^{-1}} = \\
&(\boldsymbol{d_s^{1-p}}T^p X_{s+1}\tau + T)\cdots(d_s^{-p+1}T^{p-1}\tau + 1)(X_1 d_s^{-p+1}T^{-1}\tau + 1)\cdots(X_{s-1}d_s^{-p+1}\tau + 1)(\tau + 1) = \\
&(\boldsymbol{X_s^{-1}}T^p X_{s+1}\tau + T)\cdots(X_s^{-1}T^{p-1}\tau + 1)(X_s^{-1}X_1 T^{-1}\tau + 1)\cdots(X_s^{-1}X_{s-1}\tau + 1)(\tau + 1)
\end{aligned}$$

Ως εκ τούτου η w δρα στο σώμα πηλίκο $K(X_1,\ldots,X_{r-1})$ του $Y_0^r(T)$ με τον ακόλουθο τρόπο

$$(X_1,\cdots,X_s,X_{s+1},\cdots,X_{r-1}) \longmapsto (\frac{T^pX_{s+1}}{X_s},\cdots,\frac{T^{p-1}}{X_s},\frac{T^{-1}X_1}{X_s},\frac{X_2}{X_s},\cdots,\frac{X_{s-1}}{X_s}).$$

❏

Το $Y_0^r(T)$ ταυτίζεται με ένα ανοιχτό αφινικό subscheme του $\mathrm{Spec}(K)[X_1,..,X_{r-1}]$. Εισάγουμε μία ακόμα μεταβλητή X_r και θεωρούμε την εμφύτευση

$$Y_0^r(T)\hookrightarrow \mathbf{P}_K^{r-1},\quad (X_1,\ldots,X_{r-1})\mapsto[X_1;\cdots;X_{r-1};1].$$

Λημμα 4.2.1. *Η Fricke involution επεκτείνεται σε όλο το χώρο $\mathbf{P}_K^{r-1}$.*

Απόδειξη. Θεωρούμε την απεικόνιση

$$[X_1;X_2;\cdots;X_s;X_{s+1};X_{s+2}\cdots;X_r] \mapsto [T^pX_{s+1},\cdots,T^{p-1}X_r,\frac{X_1}{T},X_2,\cdots,X_{s-1},X_s].$$

Η απεοκόνιση αυτή είναι πράγματι μία involution:

$$\begin{aligned}&[X_1;X_2;\cdots;X_s;X_{s+1};X_{s+2},\cdots;X_r]\mapsto\\ &\qquad[T^pX_{s+1},\cdots,T^{p-1}X_r,T^{-1}X_1,X_2,\cdots,X_{s-1},X_s]\mapsto\\ &[T^pT^{-1}X_1,\cdots,T^{p-1}X_s,T^{-1}T^pX_{s+1},T^{p-1}X_{s+2},\cdots,T^{p-1}X_{r-1},T^{p-1}X_r]=\\ &\qquad\qquad[X_1;X_2;\cdots;X_s;X_{s+1};X_{s+2},\cdots;X_r].\end{aligned}$$

❏

Ορισμος 4.2.4. *Ένα scheme X υπέρ το K διάστασης m ονομάζεται Brauer-Severi αν είναι προβολικό, γεωμετικά συνεκτικό και αν υπάρχει πεπερασμένη επέκταση F του K ώστε το scheme $X\times_K L$ να είναι ισόμορφο προς το $\mathbf{P}_L^m$. Το σώμα L ονομάζεται σώμα διάσπασης του X.*

Λημμα 4.2.2. *Το scheme Y (δες ορισμό 4.2.3) είναι unirational, δηλαδή το $\mathrm{quot}(Y)$ είναι ρητό.*

Απόδειξη. Έστω $P=\mathbf{P}_K^{r-1}$ και $X=P^w$ το πηλίκο του P κάτω από τη δράση της w. Έστω $L=K(\sqrt{\mathfrak{p}})$ και σ ο μη τετριμμένος αυτομορφισμός L/K. Το scheme $P\times_K L$ είναι ισόμορφο προς το $\mathbf{P}_L^{r-1}$. Ο αυτομορφισμός σ επεκτείνεται σε ένα αυτομορφισμό του $P\times_K L$. Διατηρούμε και για την επέκταση τον ίδιο συμβολισμό. Το scheme $(P\times_K L)^{\sigma w}$ είναι Brauer-Severi με σώμα διάσπασης το L. Έστω $\bar Y:=\langle\sigma w\rangle\backslash(P\times_K L)$.

Θα δείξουμε ότι το scheme $\bar Y$ είναι γεωμετρικά συνεκτικό (δηλ. $\mathrm{quot}(\bar Y)\cap K^{\mathrm{sep}}=K$). Πράγματι, $\mathrm{quot}(\bar Y)\cap K^{\mathrm{sep}}\subset\mathrm{quot}(\bar Y)\times_K L)\cap K^{\mathrm{sep}}=L$. Ως εκ τούτου

$$\mathrm{quot}(\bar Y)\cap K^{\mathrm{sep}}=\mathrm{quot}(\bar Y)\cap L=L(X_1,\cdots X_{r-1})^{\sigma w}\cap L=K.$$

Ένα $(r-1)$-διάστατο Brauer-Severi $K-$-scheme με ένα τουλάχιστο K-ρητό σημείο είναι ισόμορφο με τον προβολικό χώρο $\mathbf{P}_K^{r-1}$ (δες [22, πρόταση 4.8,σελ. 26]). Θα είναι λοιπόν το scheme $\bar Y$ ρητό αν έχει ένα K-ρητό (και άρα γεωμετρικό) σημείο. Θα δείξουμε αρχικά την ύπαρξη ενός $K-$ρητού σημείου του P με μη τετριμμένη ομάδα διακλάδωσης (για τη θεωρία διακλαδώσεων σε γενικούς δακτυλίους δες [4]). Έστω

$$B:=K[X_1,\cdots,X_{r-1},\frac{1}{X_s}],$$

$(r=2s)$ και $A=B^w$. Το maximal ιδεώδες

$$\mathfrak{M}=(X_1,\cdots,X_{s-1},X_{s+1},\cdots,X_{r-1},X_s-1)$$

είναι αναλλοίωτο κάτω από τη δράση της w. Έστω $\mathfrak{m}$ ο περιορισμός του $\mathfrak{M}$ στο A. Ως εκ τούτου η ομάδα ανάλυσης $G_Z(\mathfrak{M}/\mathfrak{m})=\langle w\rangle$. Από [4], η επέκταση επέκταση σωμάτων $(B/\mathfrak{M})/(A/\mathfrak{m})$ είναι κανονική και

$G_Z/G_T \cong \mathrm{Aut}(\mathrm{B}/\mathfrak{M}/\mathrm{A}/\mathfrak{M})$. $\mathfrak{M}$ είναι α $K-$ρητό σημείο αφού $B/\mathfrak{M} = K$. Ως εκ τούτου, $\mathfrak{m}$ είναι ένα $K-$ρητό σημείο και $G_T = \langle w \rangle$.

Έστω C η ακέραια θήκη του B στο $L(X_1, \cdots, X_{r-1}) = \mathrm{quot}(P \times_K L)$ και

$$\mathfrak{N} = (X_1, \cdots, X_{s-1}, X_{s+1}, \cdots X_{r-1}, X_s - 1)C.$$

Το maximal ιδεώδες $\mathfrak{N}$ βρίσκεται πάνω από το $\mathfrak{M}$ και είναι αναλλοίωτο κάτω από τη δράση της σ, w και της σw. Έστω G'_Z και G'_T η ομάδα ανάλυσης και η ομάδα διακλάδωσης του $\mathfrak{N}/\mathfrak{m}$ στην επέκταση $\mathrm{quot}(P \times_K L)/\,\mathrm{quot}(P^w)$. Τότε, $C/\mathfrak{N} = L, A/\mathfrak{m} = K$ και $(L : K) = 2$ Ως εκ τούτου G'_Z/G'_T έχει τάξη 2 και $|G'_Z| = 4$ και $|G'_T| = 2$.

Έστω τώρα G^*_T (αντιστ. G^*_Z) η ομάδα διακλάδωσης (αντιστ. η ομάδα ανάλυσης) του $\mathfrak{N}$ στην επέκταση δακτυλίων C/D όπου $D = C \cap \mathrm{quot}(P \times_K L)^{\sigma w}$. Είναι προφανές ότι $G^*_Z = \langle \sigma w \rangle$.

Υπάρχουν δύο δυνατότητες για την G^*_T : ή $G^*_T = 1$ ή $G^*_T = \langle \sigma w \rangle$. Για να καταλήξουμε σε άτοπο υποθέτουμε ότι $G^*_T = \langle \sigma w \rangle$. Έστω $c \in C$ ένας γεννήτορας του L υπέρ το K. Χωρίς βλάβη της γενικότητας, μπορούμε να υποθέσουμε ότι το $c^2 \in K$. Τότε, $\sigma(c) = -c$ και $\sigma w(c) - c = \sigma(c) - c = -c - c = -2c \in \mathfrak{N}$, άτοπο, αφού το $-2c$ είναι αντιστρέψιμο του C. Συνεπώς $G^*_T = 1$ και έτσι $[(C/\mathfrak{N}) : D/\mathfrak{n})] = 2$ και $D/\mathfrak{n} = K$. Αυτό αποδεικνύει ότι το $\mathfrak{n}$ είναι ένα $K-$ρητό σημείο του $\bar{Y}$.

Το $(r-1)$-διάστατο $K-$scheme $\bar{Y}$ είναι Brauer-Severi με ένα $K-$ρητό σημείο. Ως εκ τούτου είναι ισόμορφο προς το $\mathbf{P}^{r-1}_K$.

❏

Θυμίζουμε ότι ένα scheme X υπέρ το K είναι rational διάστασης n, αν υπάρχουν birational μορφισμοί $f\colon X \dashrightarrow \mathbb{P}^n_K$ και $g\colon \mathbb{P}^n_K \dashrightarrow X$ με $f \circ g$ και $g \circ f$ οι ταυτοτικοί μορφισμοί εκεί που ορίζονται. Έτσι αποδεικνύεται η

Πρόταση 4.2.2. *Το Y είναι ένα ρητό scheme.*

4.3 Μία βοηθητική κατασκευή

Έστω $r = 2s$ ένας άρτιος αριθμός με s περιττό. Έστω $\langle \mathfrak{p} \rangle$ πρώτο ιδεώδες του A με $\gcd(\mathfrak{p}, T) = 1$, $L := K(\sqrt{\mathfrak{p}})$ και σ ο μη τετριμμένος αυτομορφισμός του L/K. Έστω ϕ ένα Drinfeld module τάξεως r υπέρ το L. Έστω $\phi_T = \sum a_i \tau^i$. Με ϕ^σ συμβολίζουμε το Drinfeld module, το οριζόμενο από την $T \mapsto \sum a_i^\sigma \tau^i$. Υπενθυμίζουμε για $\mathfrak{n} \in A$, το $\phi[\mathfrak{n}]$ συμβολίζει τα $\mathfrak{n}-$ torsion σημεία του ϕ. Με M_ϕ (αντ. M_{ϕ^σ}) συμβολίζουμε το $B-$module $L\{\tau\}$ -το σχετιζόμενο με το ϕ (αντ. με το ϕ^σ).

Υπόθεση 1. Υποθέτουμε ότι υπάρχει ισογένεια $\lambda : \phi \longrightarrow \phi^\sigma$ με

1. $\ker(\lambda) \le \phi[T]$
2. $\ker(\lambda) \le L$
3. $\#\ker(\lambda) = s$ και
4. $\lambda(\phi[T]) = \ker \lambda^\sigma$.

Λήμμα 4.3.1. *Έστω $\nu : \phi_1 \longrightarrow \phi_2$ ισογένεια υπέρ το L, με πυρήνα $\ker(\nu) \le L$. Τότε, κάθε άλλη ισογένεια $\mu : \phi_1 \longrightarrow \phi_2$ με $\ker(\nu) = \ker(\mu)$ είναι αριστερό πολλαπλάσιο του ν με μία μονάδα του L.*

Απόδειξη. Άμμεσο, από το Θεώρημα 1.4.1 στη σελίδα 9 και Πρόταση 1.6.2 στη σελίδα 13 του [13]. ❏

Λήμμα 4.3.2. *Έστω $\lambda : \phi \longrightarrow \phi^\sigma$ ισογένεια, που ικανοποιεί τις παραπάνω υποθέσεις «1-4». Έστω $\hat{\lambda}$ η δυική ισογένεια του λ. Τότε $\lambda^\sigma = u \cdot \hat{\lambda}$ για κατάλληλο $u \in \mathbf{F}^*_p$.*

Απόδειξη. Η λ^σ είναι πράγματι μία ισογένεια από το ϕ^σ στο ϕ: Για κάθε $\mathfrak{a} \in A$, $\lambda\phi_\mathfrak{a} = \phi^\sigma_\mathfrak{a}\lambda$ και άρα, $\lambda^\sigma\phi^\sigma_\mathfrak{a} = \phi_\mathfrak{a}\lambda^\sigma$. Θα δείξουμε ότι λ^σ και $\hat{\lambda}$ έχουν τον ίδιο πυρήνα. Έστω $x \in \ker \lambda^\sigma$. Από την υπόθεση (4), υπάρχει $y \in \phi[T]$ με $\lambda(y) = x$. Τότε $\hat{\lambda}(x) = \hat{\lambda}\lambda(y) = \phi_T(y) = 0$, δηλαδή $x \in \ker \hat{\lambda}$. Αφού το $\deg \hat{\lambda} = \deg \lambda^\sigma$, και από το λήμμα 4.3.1, υπάρχει ένα $u \in L$ με $\lambda^\sigma = u\hat{\lambda}$.

Απομένει να δειχθεί ότι $u \in \mathbf{F}_p^*$. $\forall \mathfrak{a} \in A$, $\lambda^\sigma \circ \phi^\sigma_\mathfrak{a} = u \cdot (\hat{\lambda} \circ \phi^\sigma_\mathfrak{a}) = u \cdot (\phi_\mathfrak{a} \circ \hat{\lambda})$ και από την άλλη μεριά, $\lambda^\sigma \circ \phi^\sigma_\mathfrak{a} = \phi_\mathfrak{a}(u\hat{\lambda})$. Άρα, $u \cdot (\phi_\mathfrak{a} \circ \hat{\lambda}) = \phi_\mathfrak{a} \lambda^\sigma$ και $u\phi_\mathfrak{a} = \phi_\mathfrak{a} u$ για όλα $\mathfrak{a} \in A$, δηλαδή η u είναι μία ισογένεια του ϕ. Έστω $\phi_T = \sum_i a_i \tau^i$. Τότε, $\sum_i u^{p^i-1}\tau^i = \sum_i a_i \tau^i$, και άρα, για όλα τα i με $a_i \neq 0$, $u^{p^i-1} = 1$, δηλαδή το u είναι ένα στοιχείο του $(\mathbf{F}_{p^r}) \cap L = \mathbf{F}_p$. ❑

Έστω $\phi, \mathfrak{p}$ και λ όπως παραπάνω. Ο περιορισμός του $\lambda : \phi \longrightarrow \phi^\sigma$ στο $\phi[\mathfrak{p}]$, επάγει ένα $A/\mathfrak{p}-$ισομορφισμό.

$$\phi[\mathfrak{p}] \xrightarrow{\sim} \phi^\sigma[\mathfrak{p}].$$

Ο παραπάνω ισομορφισμός, επάγει έναν ισομορφισμό στους αντίστοιχους προβολικούς (διανυσματικούς) χώρους

$$\mathbf{Proj}\ \phi[\mathfrak{p}] \xrightarrow{\sim} \mathbf{Proj}\ \phi^\sigma[\mathfrak{p}].$$

Ας σημειωθεί ότι κάθε άλλη ισογένεια $\mu : \phi \longrightarrow \phi^\sigma$ που ικανοποιεί τις υποθέσεις $(1) - (4)$, δίνει τον ίδιο ισομομορφισμό $\mathbf{Proj}\ \phi[\mathfrak{p}] \longrightarrow \mathbf{Proj}\ \phi^\sigma[\mathfrak{p}]$.

Έστω G_L (αντιστ. G_K) η ομάδα Galois $\mathrm{Gal}(K^{sep}/L)$ (αντ. $\mathrm{Gal}(K^{sep}/L)$). Η ομάδα G_L δρα στο σύνολο των $\mathfrak{p}-$torsion σημείων του ϕ. Αυτή η δράση επάγει την αναπαράσταση

$$\rho_L : G_L \longrightarrow \mathbf{Proj}\ \phi[\mathfrak{p}].$$

και την

$$\bar{\rho}_L : G_L \longrightarrow \mathrm{PGL}(\mathbf{Proj}\ \phi[\mathfrak{p}]).$$

Ορισμος 4.3.1. *Ορίζουμε μία δράση της G_K στο $\mathbf{Proj}\ \phi[\mathfrak{p}]$ ως ακολούθως: Έστω $g \in G_K$ και $x \in \phi[\mathfrak{p}]$. Τότε,*

- *αν $g \in G_L$, τότε $x^g := g(x)$ είναι η εικόνα του x μέσω της g;*
- *αν $g \in G_K \setminus G_L$ τότε $g(x) \in \phi^\sigma[\mathfrak{p}]$. Ορίζουμε $x^g := \lambda^{-1}(g(x))$*

Σημείωση 7. Για κάθε $y \in \mathbf{Proj}\ \phi^\sigma[\mathfrak{p}]$, $\hat{\lambda}(y) = \lambda^{-1}(y)$.

Λημμα 4.3.3. *Με τις παραπάνω υποθέσεις και ορισμούς σε ισχύ, ο $\bar{\rho}_L$ μπορεί να επεκταθεί σε ένα ομομορφισμό $\bar{\rho}_K : G_K \longrightarrow \mathrm{PGL}(\mathbf{Proj}\ \phi[\mathfrak{p}])$.*

Απόδειξη. Έστω $g \in G_K \setminus G_L$ και $h \in G_L$. Τότε $\lambda^h = \lambda, (\lambda^{-1})^h = \lambda^{-1}$ και $\lambda^g = \hat{\lambda} = \lambda^{-1}$ στον $\mathbf{Proj}\ \phi[T]$. Έστω $g_1, g_2 \in G_K$. Διακρίνουμε τις περιπτώσεις:

- Αν $g_1, g_2 \in G_L$ τότε $\bar{\rho}_K(g_1 g_2) = \bar{\rho}_K(g_1)\bar{\rho}_K(g_2)$.
- Αν $g_1 \in G_L$ αλλά $g_2 \in G_K \setminus G_L$, τότε, $g_1 g_2 \in G_K \setminus G_L$. Άρα,

$$\begin{array}{rcll} \bar{\rho}_K(g_1 g_2)(x) & = & \bar{\rho}_K(g_1)(\bar{\rho}_K(g_2)(x)) & \Longleftrightarrow \\ \lambda^{-1}(g_1(g_2(x))) & = & g_1(\lambda^{-1}(g_2(x))) & \Longleftrightarrow \\ \lambda^{-1}(g_1(g_2(x))) & = & \lambda^{-1}(g_1(g_2(x))) & \end{array}$$

και

$$\begin{array}{rcll} \bar{\rho}_K(g_2 g_1)(x) & = & \bar{\rho}_K(g_2)\bar{\rho}_K(g_1)(x) & \Longleftrightarrow \\ \lambda^{-1}(g_2 g_1(x)) & = & \lambda^{-1}(g_2(g_1(x))) & \end{array}$$

- Αν $g_1, g_2 \notin G_L$ τότε $g_1 g_2 \in G_L$. Άρα,

$$\begin{array}{rcll} \bar{\rho}_k(g_1 g_2)(x) & = & \bar{\rho}_k(g_1)\bar{\rho}_k(g_2)(x) & \Longleftrightarrow \\ g_1 g_2(x) & = & \lambda^{-1}(g_1(\lambda^{-1}(g_2(x)))) & \Longleftrightarrow \\ \lambda(g_1 g_2(x)) & = & g_1(\lambda^{-1}(g_2(x))) & \Longleftrightarrow \\ \lambda(g_1 g_2(x)) & = & g_1(\lambda^{g_1}(g_2(x))) & \Longleftrightarrow \\ \lambda(g_1 g_2(x)) & = & \lambda(g_1 g_2(x))) & \end{array}$$

❑

Σημείωση 8. Έστω $g \in G_K \setminus G_L$ και έστω $[\bar\rho_K(g)]$ η κλάση του $\bar\rho_K(g)$ στο $\mathrm{PGL}(\mathbf{Proj}\ \phi[\mathfrak{p}])$. Έστω $x, y \in [\bar\rho_K(g)]$. Τότε το κλάσμα $\frac{\det x}{\det y}$ είναι τετράγωνο (το r είναι άρτιος). Μπορούμε έτσι να ορίσουμε το σύμβολο του Jacobi της κλάσης $[\rho_K(g)]$. Πιο συγκεκριμένα,

$$\left(\frac{[\rho_K(g)]}{\mathfrak{p}}\right) := \left(\frac{\rho_K(g)}{\mathfrak{p}}\right)$$

Λημμα 4.3.4. *Έστω ϕ ένα Drinfeld module, που ικανοποιεί τις υποθέσεις* (1)-(4) της σελίδας 36. Τότε

$$\forall g \in G_K \setminus G_L \qquad \left(\frac{[\rho_K(g)]}{\mathfrak{p}}\right) = -\left(\frac{-uT}{\mathfrak{p}}\right)$$

όπου u η σταθερά του λήμματος 4.3.2

Απόδειξη. Έστω L^{alg} η αλγεβρική κλειστότητα του L. Ο μη τετριμμένος αυτομορφισμός σ του L/K επεκτείνεται σε ένα αυτομορφισμό του $L^{\mathrm{alg}}/K \cdot$ θα συμβολίζουμε επίσης με σ τον αυτομορφισμό αυτόν. Μπορούμε να δούμε τα ϕ και ϕ^σ (επεκτείνοντας τις σταθερές) ως Drinfeld modules υπέρ το L^{alg}.

Έστω $B = A \otimes_{\mathbf{F}_p} L\{\tau\}$ και $\bar M = L^{\mathrm{alg}}\{\tau\}$. Η ισογένεια λ επάγει έναν $\bar B = A \otimes_{\mathbf{F}_p} L^{\mathrm{sep}}\{\tau\}$ module ομομορφισμό

$$\begin{array}{rccc} \lambda: & \bar M_{\phi^\sigma} & \longrightarrow & \bar M_\phi \\ & m & \longmapsto & m \circ \lambda \end{array}$$

και ένα A-module ομομορφισμό

$$\begin{array}{rccc} \lambda: & (\bar M_{\phi^\sigma}/\mathfrak{p}\bar M_{\phi^\sigma})^\tau & \longrightarrow & (\bar M_\phi/\mathfrak{p}\bar M_\phi)^\tau \\ & m & \longmapsto & m \circ \lambda \end{array}$$

Έστω $x_1 = 1, x_2 = \tau \ldots, x_s = \tau^{s-1}, x_{s+1} = \hat\lambda, x_{s+2} = \tau\hat\lambda, \ldots x_r = \tau^{s-1}\hat\lambda$. Το σύνολο $\{x_1, \ldots, x_r\}$ γεννάει το M υπέρ το B και το $\bar M$ υπέρ το $\bar B$. Το module $\phi^\sigma[\mathfrak{p}]$ ως A-module, είναι ισόμορφο προς το $(A/\mathfrak{p})^r$ (δες την απόδειξη του πορίσματος 5.6.4, στην σελίδα 152 του [13]). Έστω $\{y_1, \ldots, y_r\}$ ένα $A-$ σύνολο γεννητόρων του $(M/\mathfrak{p}M)^\tau \cong (A/\mathfrak{p})^r$. Τότε, $\{y_1, \ldots, y_r\}$ είναι ένα $B-$ σύνολο γεννητόρων του $\bar M_\phi/\mathfrak{p}\bar M_\phi$. Μπορούμε να υποθέσουμε ότι $\{y_1, ..., y_r\}$ είναι μία $A/\mathfrak{p}$ βάση του $M_{\phi^\sigma}/\mathfrak{p}M_{\phi^\sigma}$.[1] Έστω $\alpha = (a_{ij}), a_{ij} \in \bar B$ και $\beta = (b_{ij}), b_{ij} \in A$ πίνακες που ικανοποιούν τις

$$\begin{pmatrix} \lambda(x_1) \\ \vdots \\ \lambda(x_r) \end{pmatrix} = \alpha \cdot \begin{pmatrix} x_1^\sigma \\ \vdots \\ x_r^\sigma \end{pmatrix} \quad \text{και} \quad \begin{pmatrix} \lambda(y_1) \\ \vdots \\ \lambda(y_r) \end{pmatrix} = \beta \cdot \begin{pmatrix} y_1^\sigma \\ \vdots \\ y_r^\sigma \end{pmatrix}$$

Έστω P ο πίνακας με στοιχεία από το $\bar B$ που μετασχηματίζει τη βάση $\{y_i\}$ στην $\{x_i\}$. Τότε, $\beta = P^{-1} \cdot \alpha \cdot P$ (ο λ είναι $\bar B$-ομομορφισμός και έτσι ο πίνακας P μετασχηματίζει τη βάση $\{\lambda(y_i)\}$ στην $\{\lambda(x_i)\}$.) Είναι εύκολο να δει κανείς

$$\alpha = \begin{pmatrix} 0 & \cdots & 0 & u \otimes 1 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & u \otimes 1 \\ 1 \otimes T & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 1 \otimes T & 0 & \cdots & 0 \end{pmatrix}$$

Λαμβάνοντας τον παραπάνω υπολογισμό υπόψην καθώς και το γεγονός ότι η σ περιοριζόμενη στο L δρα μη-τετριμμένα, συνάγουμε η ορίζουσα $\det \sigma$ —modulo τετράγωνο — ισούται προς $-\left(\frac{-uT}{\mathfrak{p}}\right)$ (αφού το s είναι περιττός αριθμός $(\gcd(2s, q^d - 1) = 2)$. ❑

[1] Από το θεώρημα του Lang για την $\mathrm{GL}(r)$, $(\bar M_{\phi^\sigma}/\mathfrak{p}\bar M_{\phi^\sigma})^\tau \otimes_{\mathbf{F}_p} L = M_{\phi^\sigma}/\mathfrak{p}M_{\phi^\sigma}$. Το σύνολο γεννητόρων $\{y_1, \ldots, y_r\}$ μπορεί να επεκταθεί σε μία $\mathbf{F}_p-$ βάση $\{y_1, \ldots, y_n\}, n = \dim_{\mathbf{F}_p}(\bar M_{\phi^\sigma}/\mathfrak{p}\bar M_{\phi^\sigma})^\tau$. Έστω $m \in M_{\phi^\sigma}/\mathfrak{p}M_{\phi^\sigma}$. Τότε, υπάρχει $\kappa_i \in \bar L$ με $m = \sum_{i=1}^n y_i\kappa_i$. Αλλά $\forall i = r+1, \ldots, n,\ m_i$ είναι ένας $A-$γραμμικός συνδυασμός του $m_1, \ldots, m_r$. Άρα, το m είναι ένας γραμμικός συνδυασμός των $y_1, \ldots, y_r$ υπέρ το $\bar B$.

Από τα παραπάνω δεν είναι ακόμα σαφές ότι το u δεν εξαρτάται από την επιλογή του ϕ. Το επόμενο λήμμα ξεκαθαρίζει το τοπίο.

Λημμα 4.3.5. *Το u του λήμματος 4.3.2 δεν εξαρτάται από την επιλογή του ϕ.*

Απόδειξη. Έστω $(\phi, flag)$ ένα $L-$ρητό σημείο του $Y_0^r(T) \times L$ που αντιστοιχεί σε ένα $K-$ρητό σημείο του Y. Το ϕ πάνω από το σώμα $L' = L(a_i)$ γράφεται ως

$$\phi_T = (a_1\tau + T)(a_2\tau + 1)\cdots(a_r\tau + 1).$$

Η ορίζουσα της ισογένειας $\lambda\colon \phi \longrightarrow \phi^\sigma$ που επάγεται στα M_ϕ, M_{ϕ^σ} υπολογίστηκε στο προηγούμενο λήμμα και είναι ίση προς $-uT^s$. Ακόμα, είναι φανερό ότι το $u \in \mathbf{F}_q$ είναι μία ρητή συνάρτηση των $a_1, a_2, \ldots, a_r$. Αλλάζοντας το ϕ, πιθανόν να αλλάξουμε και u —ωστόσο τα πιθανά $u_1, \ldots, u_m$ ορίζουν μία finite stratification στο Y. Έστω Y_i το subscheme το οριζόμενο από το u_i· τότε αφού κάθε Y_i είναι κλειστό (διότι καθορίζεται από μία αλγεβρική σχέση) και η ένωσή τους σχηματίζει ένα απολύτως ανάγωγο scheme υπέρ το K (το Y), θα έχουμε κατ' ανάγκη ότι κάποιο Y_i θα είναι το Y. Έτσι, $m = 1$ και το u είναι μοναδικό. ❑

Το θεώρημα αναγωγισιμότητας του Hilbert

Έστω F σώμα, $T_1, \ldots, T_r, X_1, \ldots, X_n$ υπερβατικές, αλγεβρικά ανεξάρτητες μεταβλητές υπέρ το F. Έστω

$$f_1(\boldsymbol{X}, \boldsymbol{T}), \ldots, f_m(\boldsymbol{X}, \boldsymbol{T})$$

πολυώνυμα ως προς $X_1, \ldots, X_n$ με συντεταγμένες στο $F(\boldsymbol{T})$. Υποθέτουμε ακόμα ότι είναι ανάγωγα στο δακτύλιο $F(\boldsymbol{T})[\boldsymbol{X}]$.

Συμβολισμός 5. Έστω $g \in K[\boldsymbol{T}]$ ένα μη μηδενικό πολυώνυμο. Συμβολίζουμε με $H_F(f_1, \ldots, f_m; g)$ το σύνολο των $r-$άδων $\boldsymbol{a} = (a_1, \ldots, a_r) \in K^r$ με $g(\boldsymbol{a}) \neq 0$ και $f_1(\boldsymbol{a}, \boldsymbol{X}), \ldots, f_m(\boldsymbol{a}, \boldsymbol{X})$ ορίζονται και είναι ανάγωγα στο $F[\boldsymbol{X}]$. Τα σύνολα αυτά ονομάζονται *σύνολα του Hilbert.*

Σημείωση 9. Τα H_L είναι πυκνά υποσύνολα του K^r ως προς κάθε $p-$αδική τοπολογία του K.

Το σώμα F ονομάζεται σώμα του *Hilbert* αν όλα τα Hilbert υποσύνολά του είναι μη κενά. Τα global σώματα είναι γνωστό ότι είναι σώματα του Hilbert (δες θεώρημα B, στη σελίδα 218 του [25]).

Έστω $X \longrightarrow k$ μορφισμός με X ανάγωγο scheme διάστασης m πάνω από το global σώμα k. Το θεώρημα αναγωγισιμότητας του Hilbert μας εξασφαλίζει ότι άπειρες ίνες του μορφισμού $X \longrightarrow k$ παραμένουν ανάγωγες.

Εφαρμόζουμε το θεώρημα αναγωγισιμότητας του Hilbert στην ακόλουθη περίπτωση: Έστω $Y^r(\mathfrak{p}) \times Y^r(T) \longrightarrow Y$ η κάλυψη που περιγράφεται στις παραγράφους 4 & 5. Τα $Y^r(\mathfrak{p})$ και Y είναι αφινικά, ανάγωγα και πεπερασμένου τύπου (finite type) πάνω από το K. Έστω $\mathcal{K}(Y^r(\mathfrak{p}))$ και $\mathcal{K}(Y)$ τα σώματα συναρτήσεων τους. Έχουμε δει ότι $\mathcal{K}(Y) = K(X_1, \ldots, X_{r-1})$. Έστω H το σύνολο των $(r-1)-$άδων $(a_1, \ldots, a_{i-1}) \in K^{r-1}$ που αντιστοιχούν σε σημεία του Hilbert της επέκτασης $\mathrm{K}(Y_0(T) \times Y(\mathfrak{p}))/\mathrm{K}(Y)$. Αφού το Y είναι ένα ρητό scheme, το $Y(K)$ είναι πυκνό υποσύνολο του K^{r-1}.

Θα δείξουμε ότι το $H \cap Y(K)$ είναι ένα άπειρο υποσύνολο του K^{r-1}. Έστω ότι το $H \cap Y(K)$ είναι πεπερασμένο. Έστω Z το συμπλήρωμα του $Y(K)$ στο $\mathbb{A}_K^{r-1}(K) = K^{r-1}$. Το Z είναι κλειστό υποσύνολο διάστασης $\leq r-2$. Το σύνολο $Y(K)$ έιναι υποσύνολο του συνόλου των σημείων των $(r-1)$-άδων $(a_1, a_2, \ldots, a_{r-1})$ με $a_i \neq 0, \forall i$. Μπορούμε να γράψουμε το $H = H' \cup H_1 \cup \cdots \cup H_{r-1}$ με $H' = H \cap Y(K)$ και H_i το υποσύνολο με $a_i = 0$. Αν το H' το υποθέσουμε πεπερασμένο, τότε, επειδή $\dim H_i \leq r-2$, $\forall i$, θα έχουμε $\dim H \leq r-2$ —άτοπο αφού το H είναι πυκνό. Έχουμε επομένως δείξει το επόμενο

Λημμα 4.3.6. *Το σύνολο $Y(K)$ είναι άπειρο. Μάλιστα, άπειρα σημεία του δεν διακλαδίζονται και δεν αναλύονται στο κάλυμμα $Y_0(T) \times Y(\mathfrak{p}) \longrightarrow Y$.*

Λημμα 4.3.7. *Για κάθε $d \geq 1$, υπάρχει ανάγωγο πολυώνυμο $\mathfrak{p}$ βαθμού d τέτοιο ώστε το σύμβολο $\left(\frac{T}{\mathfrak{p}}\right)$ να ισούται προς το δοσμένο $\varepsilon \in \{\pm 1\}$.*

Απόδειξη. Εφαρμόζοντας τον νόμο τετραγωνικής αντιστροφής στα σώματα συναρτήσεων, αρκεί να δείξουμε ότι το $\left(\frac{\mathfrak{p}}{T}\right)$ παίρνει τη δοθείσα τιμή ε. Αλλά το τετραγωνικό σύμβολο είναι ε αν και μόνο αν ο σταθερός όρος του $\mathfrak{p}$ ισούται προς ε στο $\mathbf{F}_q^*/\mathbf{F}_q^{*\,2}$. Άρα, αρκεί να βρεθεί ένα ανάγωγο πολυώνυμο $\mathfrak{p}$ βαθμού d υπέρ το K που ο σταθερός του όρος —έστω ξ— να είναι $\left(\frac{\xi}{\mathfrak{p}}\right) = \varepsilon$. Αλλά αυτό δεν είναι παρά το θεώρημα των Hansen-Mullen (δες [17, σελ. 642]). ❑

4.3.1 Το κυρίως θεώρημα

ΘΕΩΡΗΜΑ 4.3.1. *Έστω r άρτιος φυσικός, $q = p^d$ με $\gcd(r, q-1) = 2$. Η απλή ομάδα $\mathrm{PSL}(r, p^d)$ είναι υλοποιήσιμη ως ομάδα του Galois υπέρ το K.*

Απόδειξη. Διαλέγουμε ένα πρώτο πολυώνυμο $\mathfrak{p}$ ώστε σύμβολο $-\left(\frac{-uT}{\mathfrak{p}}\right) = 1$ σύμφωνα με το 4.3.7. Σύμφωνα με το πόρισμα 4.3.6 υπάρχουν άπειρα K-ρητά σημεία του Y που αντιστοιχούν σε μη διακλαδιζόμενα L-ρητά σημεία του $Y_0^r(T) \times L$ τα οποία δεν αναλύονται αλλά και δεν διακλαδίζονται στην $Y_0^r(T) \times Y^r(\mathfrak{p})$. Έστω y ένα από αυτά. Έστω x το (μοναδικό) σημείο $\in Y_0(T) \times L$ που βρίσκεται πάνω από το y. Σε αυτό αντιστοιχεί ένα $L-$ρητό ζεύγος $(\phi, \{C_1 \leq \cdots \leq C_s \leq C_{s+1} \leq \cdots C_r\})$ του $Y_0^r(T) \times L$. Στο ζεύγος αυτό αντιστοιχεί μία δυάδα (ϕ, flag), όπου ϕ είναι ένα Drinfeld module ορισμένο πάνω από το L και flag είναι μία full flag $\mathrm{Gal(K^{sep}/L)}$ αναλλοίωτων υποομάδων της $\phi[T]$. Ακόμα, αφού η ομάδα ανάλυσης $G_Z(x/y)$ είναι η $\langle \sigma w \rangle$, τα ϕ και ϕ^σ είναι ισογενή: υπάρχει δηλαδή ισογένεια $\lambda : \phi \longrightarrow \phi^\sigma$. Είναι εύκολο να δείξει κανείς ότι η ισογένεια λ ικανοποιεί τις υποθέσεις 1-4 της σελίδας 36. Πράγματι, γράφουμε $\phi_T = ab$ με $a, b \in L\{\tau\}$. Τότε, $C_s = \ker b$. Αφού το $(\phi, flag)$ είναι ένα σημείο του $Y_0^r(T) \times L$ θα είναι $\ker \lambda = \ker b = C_s \leq L$ και $\ker b \leq \ker ab = \phi[T]$. Για την υπόθεση 4: Θα δείξουμε ότι $\ker a = \ker b^\sigma$. Πράγματι, αφού $(\phi, flag) \longmapsto (\phi^\sigma, flag^\sigma) = (\phi^w, flag^w)$ θα είναι $\ker b^\sigma = \ker a$. Ακόμα επειδή $\deg_\tau a = \deg_\tau b^\sigma$ θα υπάρχει $u \in L \neq 0$ τέτοιο ώστε $ua = b^\sigma$. Έστω τώρα $x \in \phi[T]$. Τότε $0 = \phi_T(x) = ab(x)$ και έτσι $0 = uab(x) = b^\sigma b(x) = \lambda^\sigma \lambda(x)$, δηλαδή $x \in \ker \lambda^\sigma$.

Έστω L_ϕ το σώμα διάσπασης του πολυωνύμου που αντιστοιχεί στο $\phi_\mathfrak{p}$ πάνω από το L. Τότε, από υπόθεση, η επέκταση L_ϕ/L είναι Galois. Θα δείξουμε στην συνέχεια ότι και η επέκταση L_ϕ/K είναι Galois. Πράγματι, αφού $\gcd(T, \mathfrak{p}) = 1$ οι μορφισμοί

$$\lambda : \phi[\mathfrak{p}] \longrightarrow \phi^\sigma[\mathfrak{p}] \quad \text{και} \quad \hat{\lambda} : \phi^\sigma[\mathfrak{p}] \longrightarrow \phi[\mathfrak{p}]$$

είναι ισομορφισμοί. Έστω a ένα (οποιοδήποτε) $\mathfrak{p}$-torsion σημείο του ϕ. Το σημείο $\lambda(a)$ είναι ένα $\mathfrak{p}$-torsion σημείο του ϕ^σ *και* ένας πολυωνυμικός συνδυασμός του a υπέρ το L. Αυτό αποδεικνύει ότι το $L_{\phi^\sigma} \subset L_\phi$. Χρησιμοποιώντας την $\hat{\lambda}$ αντί της λ βλέπουμε ότι $L_\phi \subset L_{\phi^\sigma}$. Άρα, $L_\phi = L_{\phi^\sigma}$ και L_ϕ/K είναι Galois.

Έστω $\hat{G}$ η ομάδα Galois του L_ϕ/K. Θεωρούμε τον ομομορφισμό

$$\rho_K : G_K \longrightarrow \mathbf{Proj}\ \phi[\mathfrak{p}].$$

Έχουμε δει (δες το λήμμα 4.3.4) ότι $\forall g \in G_K$ η ορίζουσα $\det g$ modulo τετράγωνο ισούται προς $-\left(\frac{-uT}{\mathfrak{p}}\right) = 1$. Έτσι η ορίζουσα $\det g$ είναι τετράγωνο στο δακτύλιο $A/\mathfrak{p}$ και συνεπώς μία r-δύναμη —αφού $\gcd(r, q-1) = 2$. Άρα, ο παραπάνω μορφισμός, επάγει έναν επιμορφισμό

$$\alpha : G_K \longrightarrow \mathrm{PSL}(r, q).$$

Έστω U ο πυρήνας του α· η L_ϕ^U/K είναι επέκταση του Galois με ομάδα Galois ισόμορφη προς την $\mathrm{PSL}(r, q)$. ❏

Μέρος II

Modular αυτομορφισμοί

Modular αυτομορφισμοι

5.1 Δράση ομάδων στο Ω

Έστω q δύναμη πρώτου, $A = \mathbf{F}_q[T]$ ο πολυωνυμικός δακτύλιος μία μεταβλητής T και $K = \mathbf{F}_q(T)$ το αντίστοιχο σώμα πηλίκων. Ορίζουμε στο K την εκτίμηση $|f(T)/g(T)| = q^{\deg f(T) - \deg g(T)}$. Η πλήρωση του K ως προς την εκτίμηση αυτή είναι το σώμα $K_\infty = \mathbf{F}_q((1/T))$. Έστω $\mathbf{C}$ η πλήρωση της αλγεβρικής κλειστότητας του K_∞ και $\Omega = \mathrm{P}^1_{\mathbf{C}} \setminus \mathbf{P}^1_{K_\infty}$ το Drinfeld άνω ημιεπίπεδο. Το Ω δέχεται τη δομή ενός rigid αναλυτικού χώρου υπέρ το $\mathbf{C}$ (δες [7]). Η ομάδα $\mathrm{GL}(2, K_\infty)$ δρα στο Ω με τη μορφή γραμμικών μετασχηματισμών: αν $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathrm{GL}(2, K_\infty)$ και $z \in \Omega$, τότε

$$g \cdot z = \frac{az + b}{cz + d}.$$

Μία αριθμητική υποομάδα Γ της $\mathrm{GL}(2, A)$ με οδηγό $\mathfrak{n}$, είναι μία congruence υποομάδα της $\mathrm{GL}(2, \mathrm{A})$, *δηλ.*, μία υποομάδα της $\mathrm{GL}(2, \mathrm{A})$, η οποία περιέχει τον πυρήνα του ομομορφισμού

$$\mathrm{GL}(2, \mathrm{A}) \longrightarrow \mathrm{GL}(2, \mathrm{A}/\mathfrak{n})$$

για κάποιο πολυώνυμο $\mathfrak{n}$ του A.

Παραδείγματα τέτοιων υποομάδων (που θα συναντήσουμε παρακάτω) είναι:

$$\Gamma_0(\mathfrak{n}) = \left\{ g \in \mathrm{GL}(2, A) \; ; \; g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), c \equiv 0 \mod \mathfrak{n} \right\}$$

$$\Gamma_1(\mathfrak{n}) = \left\{ g \in \mathrm{GL}(2, A) \; ; \; g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), c \equiv 0 \bmod \mathfrak{n} \text{ και } a \equiv 1 \bmod \mathfrak{n} \right\} \text{ και}$$

$$\Gamma_1'(\mathfrak{n}) = \left\{ g \in \mathrm{GL}(2, A) \; ; \; g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right), c \equiv 0 \bmod \mathfrak{n} \text{ και } a \equiv d \equiv 1 \bmod \mathfrak{n} \right\}.$$

Για κάθε αριθμητική υποομάδα Γ της $\mathrm{GL}(2, A)$, το πηλίκο $Y(\Gamma) := \Gamma \backslash \Omega$ δέχεται τη δομή rigid αναλυτικού χώρου (δες [8, πόρισμα 3.2.7,σελ. 49]). Παριστάνουμε με $X(\Gamma)$ την κανονική (λεία) συμπαγοποίηση του $Y(\Gamma)$ (δες [8, πρόταση 3.2.17,σελ. 55]). Μέσω της GAGA, η $X(\Gamma)$ αντιστοιχεί σε μία προβολική, λεία και ανάγωγη καμπύλη $\mathcal{C}(\Gamma)$. Συμβολίζουμε με $\mathcal{N}_{\mathrm{PGL}(2, K_\infty)}(\Gamma)$ τον κανονικοποιητή της Γ στην $\mathrm{PGL}(2, K_\infty)$. Η ομάδα

$$\mathcal{M}(\Gamma) := \left(\mathcal{N}_{\mathrm{PGL}(2, K_\infty)}(\Gamma) \cdot K_\infty^* \right) / \Gamma \cdot K_\infty^*$$

μπορεί να ειδωθεί ως υποομάδα της ομάδας αυτομορφισμών της $\mathcal{C}(\Gamma)$ και ονομάζεται η «ομάδα των modular αυτομορφισμών» της $X(\Gamma)$.

Στην κλασική περίπτωση δηλ., στην περίπτωση των ελλειπτικών καμπύλων, έχει γίνει πολύ δουλειά σε ότι αφορά στο πρόβλημα υπολογισμού του κανονικοποιητή, congruence υποομάδων της $\mathrm{SL}(2, \mathbb{Z})$. Για παράδειγμα, στα άρθρα [3] και [24], υπολογίζονται οι κανονικοποιητές των κλασικών $\Gamma_0(N)$ και $\Gamma_1(N)$ στην $\mathrm{PSL}(2, \mathbb{R})$ αντιστοίχως. Στην περίπτωση των Drinfeld modules, στην εργασία του A. Schweizer (δες [29]), υπολογίζεται λεπτομερώς η ομάδα των modular αυτομορφισμών της Drinfeld modular καμπύλης $X(\Gamma_0(\mathfrak{n}))$.

Από εδώ και στο εξής, η καμπύλη $X(\Gamma_1(\mathfrak{n}))$, θα δηλώνεται για συντομία ως $X_1(\mathfrak{n})$.

5.1.1 Ιδιότητες της καμπύλης $X_1(\mathfrak{n})$

Το γένος

Στο άρθρο του E. Gekeker [10], μεταξύ άλλων, υπολογίζεται και το γένος της καμπύλη $X_1(\mathfrak{n})_{\mathbf{C}}$ το οποίο δίνεται από τη σχέση

$$g(X_1(\mathfrak{n})_{\mathbf{C}}) = 1 + \frac{\varphi(\mathfrak{n})}{(q^2-1)(q-1)} \left(\varepsilon(\mathfrak{n}) - (q+1) \left(q - 2 + \prod_{i=1}^{n} \left(d_i + 1 - \frac{d_i - 1}{q^{\deg \mathfrak{p}_i}} \right) \right) \right)$$

όπου

$$\mathfrak{n} = \prod_{i=1}^{n} \mathfrak{p}_i^{d_i}, \ \ \varphi(\mathfrak{n}) = q^{\deg(\mathfrak{n})} \prod_{i=1}^{n} (1 - q^{-\deg(\mathfrak{p}_i)}) \ \text{ και } \ \varepsilon(\mathfrak{n}) = q^{\deg \mathfrak{n}} \prod_{i=1}^{n} (1 + q^{-\deg \mathfrak{p}_i})$$

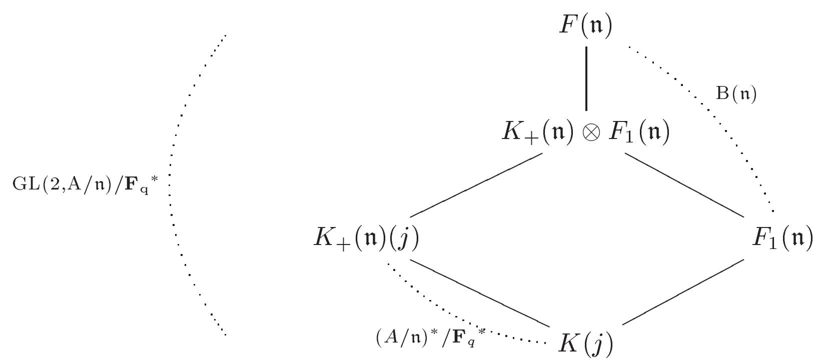
Εύκολα βλέπει κανείς, ότι $g(X_1(\mathfrak{n})_{\mathbf{C}}) = 0$, *δηλ.*, $X_1(\mathfrak{n})_{\mathbf{C}} \sim \mathbf{P}^1_{\mathbf{C}}$, αν $\deg(\mathfrak{n}) \leq 2$.

Το σώμα ορισμού

Η καμπύλη $X_1(\mathfrak{n})_{\mathbf{C}}$ ορίζεται υπέρ το K (δες [10]), δηλαδή υπάρχει μία γεωμετρικά συνεκτική καμπύλη, την οποία θα συμβολίζουμε επίσης με $X_1(\mathfrak{n})$, τέτοια ώστε $X_1(\mathfrak{n}) \times_K \mathbf{C} = X_1(\mathfrak{n})_{\mathbf{C}}$.

Σώματα μερόμορφων συναρτήσεων και επεκτάσεις του Galois

Έστω $K(\mathfrak{n})$ το σώμα που γεννάται, υπέρ το σώμα K από το τα $\mathfrak{n}$-tortion σημεία του Carlitz module. Με $K_+(\mathfrak{n})$ θα συμβολίζουμε το μέγιστο υπόσωμα του $K(\mathfrak{n})$, στο οποίο η θέση ∞ αδρανεί. Στα [9] και [10] έχει δειχθεί ότι τα $K_+(\mathfrak{n})$ και K είναι τα σώματα ορισμού των καμπύλων $X(\mathfrak{n})_{\mathbf{C}}$ και $X_1(\mathfrak{n})_{\mathbf{C}}$, αντιστοίχως. Έστω $F(\mathfrak{n})$ το αλγεβρικό σώμα συναρτήσεων της $X(\mathfrak{n})$ και $F_1(\mathfrak{n})$ το αλγεβρικό σώμα συναρτήσεων της $X_1(\mathfrak{n})$. Έστω $\mathrm{B}(\mathfrak{n}) := \left\{ \left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix} \right) \in \mathrm{GL}(2, A/\mathfrak{n})/\mathbf{F}_q^* : a, d \in \mathbf{F}_q^* \right\}$ και j η αναλλοίωτος ταξινόμησης των Drinfeld modules: $j \colon \mathrm{GL}(2,A)\backslash\Omega \xrightarrow{\sim} \mathbf{C}$ (δες [8, §3 και πόρισμα 3.3.10 σελ 63]). Το παρακάτω διάγραμμα δείχνει τις σχέσεις εγκλεισμού των παραπάνω σωμάτων, καθώς και τις ομάδες Galois που εμφανίζονται (δες [30, §1.3]):



5.1.2 Εισαγωγή

Όπως θα φανεί από τα παρακάτω, για να υπολογίσουμε τον κανονικοποιητή της $\bar{\Gamma}_1(\mathfrak{n})$ στην $\mathrm{PGL}(2, K_\infty)$, αρκεί να υπολογίσουμε τον κανονικοποιητή της $K_\infty^* \cdot \Gamma_1(\mathfrak{n})$ στην $\mathrm{GL}(2, K_\infty)$ (δες λήμμα 5.2.1, μέρος 3). Στο λήμμα 5.2.3 αποδυκνείεται ότι ο κανονικοποιητής της ομάδας $K_\infty^* \cdot \Gamma_1(\mathfrak{n})$ στην $\mathrm{GL}(2, K_\infty)$ είναι η ομάδα $K_\infty^* \cdot \mathcal{N}_{\mathrm{GL}(2,K)}(K^* \cdot \Gamma_1(\mathfrak{n}))$ ενώ στο πόρισμα 5.2.1 δείχνεται ότι $\mathcal{N}_{\mathrm{GL}(2,K)}(K^* \cdot \Gamma_1(\mathfrak{n})) = K^* \cdot \mathcal{N}_{\mathrm{GL}(2,K)}(\mathbf{F}_q^* \cdot \Gamma_1(\mathfrak{n}))$.

5.2 Ο κανονικοποιητής της $K_\infty^* \cdot \Gamma_1(\mathfrak{n})$ στην $\mathrm{GL}(2, K_\infty)$

Στην παράγραφο αυτή υπολογίζουμε τον κανονικοποιητή της $K_\infty^* \cdot \Gamma_1(\mathfrak{n})$ στην $\mathrm{GL}(2, K_\infty)$. Όπως θα φανεί στα παρακάτω, ο υπολογισμός αυτός είναι ουσιαστικός και επιπλέον απλοποιεί το πρόβλημα (δες λήμμα 5.2.2, μέρος 2).

Συμβολισμός 6. Έστω B δακτύλιος με $A \subset B$ και Δ μία υποομάδα της $\mathrm{GL}(2, B)$. Για απλότητα στο συμβολισμό θα γράφουμε $\mathcal{N}_B(\Delta)$ αντί για $\mathcal{N}_{\mathrm{GL}(2,B)}(\Delta)$. Το κέντρο της $\mathrm{GL}(2, B)$ θα δηλώνεται ως $\langle B^* \rangle$.

Θυμίζουμε ότι το $\mathbf{F}_q$ είναι το σώμα των σταθερών του πλήρους σώματος $K_\infty = \mathbf{F}_q((1/T))$ και η ομάδα $\mathbf{F}_q^*$ είναι η ομάδα των αντιστρέψιμων στοιχείων του δακτυλίου $A = \mathbf{F}_q[T]$. Έτσι έχουμε το ακόλουθο λήμμα:

Λημμα 5.2.1. *Για κάθε σώμα L με $K \subset L \subset K_\infty$ ισχύουν τα ακόλουθα:*

1. *Αν $g \in \mathcal{N}_L(L^* \cdot \Gamma_1(\mathfrak{n}))$ τότε $g^{-1}\Gamma_1(\mathfrak{n})g \subset \mathbf{F}_q^* \cdot \Gamma_1(\mathfrak{n})$.*
2. *Αν $g \in \mathcal{N}_L(L^* \cdot \Gamma_1'(\mathfrak{n}))$ τότε $g^{-1}\Gamma_1(\mathfrak{n})g \subset \langle -1 \rangle \cdot \Gamma_1'(\mathfrak{n})$.*
3. *$\mathcal{N}_L(L^* \cdot \Gamma_1(\mathfrak{n}))/L^* \cdot \Gamma_1(\mathfrak{n}) \cong \mathcal{N}_{\mathrm{PGL}(2,L)}(\bar{\Gamma}_1(\mathfrak{n}))/\bar{\Gamma}_1(\mathfrak{n})$, όπου $\bar{\Gamma}_1(\mathfrak{n})$ είναι η προβολή της $\Gamma_1(\mathfrak{n})$ στην $\mathrm{PGL}(2, L)$.*

Απόδειξη. 1. Έστω $\gamma \in \Gamma_1(\mathfrak{n})$ και $g \in \mathcal{N}_L(L^* \cdot \Gamma_1(\mathfrak{n}))$. Τότε, υπάρχουν $\kappa \in L^*$ και $\gamma' \in \Gamma_1(\mathfrak{n})$ με $g^{-1}\gamma g = \kappa \cdot \gamma'$. Οπότε (παίρνοντας ορίζουσες) $\kappa^2 = \det \gamma' (\det \gamma)^{-1}$ δηλαδή, το κ είναι αλγεβρικό υπέρ το $\mathbf{F}_q$ και άρα ανήκει στο ${\mathbf{F}_q}^* \cap L$.

2. Έστω $\gamma \in \Gamma_1'(\mathfrak{n})$ και $g \in \mathcal{N}_L(L^* \cdot \Gamma_1'(\mathfrak{n}))$. Τότε, υπάρχουν $\kappa \in L^*$ και $\gamma' \in \Gamma_1'(\mathfrak{n})$ με $g^{-1}\gamma g = \kappa \cdot \gamma'$. Οπότε $\kappa^2 = \det \gamma' (\det \gamma)^{-1} = 1$ δηλαδή, το $\kappa = \pm 1$.

3. Αρκεί να παρατηρήσουμε ότι η ομάδα $\mathcal{N}_L(L^* \cdot \Gamma_1(\mathfrak{n}))$ (αντ. η ομάδα $L^* \cdot \Gamma_1(\mathfrak{n})$) είναι η αντίστροφη εικόνα της $\mathcal{N}_{\mathrm{PGL}(2,L)}(\bar{\Gamma}_1(\mathfrak{n}))$ (αντ. της $\bar{\Gamma}_1(\mathfrak{n})$) μέσω του επιμορφισμού $\mathrm{GL}(2, L) \longrightarrow \mathrm{PGL}(2, L)$.

❏

Λημμα 5.2.2. *Ισχύουν τα ακόλουθα:*

1. *$\mathcal{N}_K(\Gamma_1'(\mathfrak{n})) = \mathcal{N}_K(K^* \cdot \Gamma_1'(\mathfrak{n}))$*
2. *$\mathcal{N}_K(K^* \cdot \Gamma_1(\mathfrak{n})) \subset \mathcal{N}_K(\Gamma_1'(\mathfrak{n}))$*

Απόδειξη. 1. Είναι προφανές ότι $\mathcal{N}_K(\Gamma_1'(\mathfrak{n})) \subset \mathcal{N}_K(K^* \cdot \Gamma_1'(\mathfrak{n}))$. Αντιστρόφως, έστω $g \in \mathcal{N}_K(K^* \cdot \Gamma_1(\mathfrak{n}))$. Μπορούμε, χωρίς βλάβη της γενικότητας, να υποθέσουμε ότι όλα τα στοιχεία του g ανήκουν στον A και μάλιστα, το ιδεώδες που παράγουν να είναι το A.

Έστω $\gamma \in \Gamma_1'(\mathfrak{n})$. Τότε υπάρχουν $\gamma' \in \Gamma_1'(\mathfrak{n})$ και $\kappa \in \{\pm 1\}$ (δες λήμμα 5.2.1) ώστε $\gamma g = \kappa \cdot g\gamma'$. Γράφουμε $\gamma = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right), g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ και $\gamma' = \left(\begin{smallmatrix} k & l \\ m & n \end{smallmatrix}\right)$. Θεωρούμε την έκφραση $\gamma g = \kappa \cdot g\gamma'$ modulo $\mathfrak{n}$: $\left(\begin{smallmatrix} 1 & y \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = \kappa \cdot \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & l \\ 0 & 1 \end{smallmatrix}\right)$. Αν η χαρακτηριστική $p = 2$, τότε δεν έχουμε τίποτα να δείξουμε. Υποθέτουμε λοιπόν ότι $p \geq 3$. Αν $\kappa = 1$ τότε πάλι προκύπτει άμεσα ότι $g \in \mathcal{N}_K(\Gamma_1'(\mathfrak{n}))$. Αν $\kappa = -1$, έχουμε

$$a + cy = -a,\ b + dy = -b - al,\ c = -c,\ d = -d - cl \mod \mathfrak{n} \tag{5.1}$$

οι οποίες οδηγούν σε άτοπο,[1] αφού εύκολα βλέπει κανείς ότι τότε, το $\mathfrak{n}$ διαιρεί όλα τα στοιχεία του g. Έτσι, $\kappa = 1$ και $g^{-1}\gamma g = \gamma' \in \Gamma_1'(\mathfrak{n})$.

2. Έστω $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathcal{N}_K(K^* \cdot \Gamma_1(\mathfrak{n}))$. Για το g υποθέτουμε ότι και παραπάνω, δηλαδή ότι $g \in \mathrm{Mat}(2, A)$ $\langle a, b, c, d \rangle = A$. Θα δείξουμε ότι το $g \in \mathcal{N}_K(K^*, \Gamma_1'(\mathfrak{n}))$. Έστω $\gamma = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \in \Gamma_1'(\mathfrak{n})$. Υπάρχουν $\gamma' = \left(\begin{smallmatrix} k & l \\ m & n \end{smallmatrix}\right) \in \Gamma_1(\mathfrak{n})$ και $\kappa \in \mathbf{F}_q^*$ (δες λήμμα 5.2.1) ώστε $\gamma g = \kappa \cdot g\gamma'$. Έτσι προκύπτουν οι παρακάτω σχέσεις modulo $\mathfrak{n}$:

$$a + cy = \kappa a, b + dy = \kappa(al + bn), c = \kappa c, d = \kappa(cl + dn) \tag{5.2}$$

Το ζητούμενο είναι να δειχθεί ότι $n \equiv 1 \mod \mathfrak{n}$. Υποθέτουμε, για να καταλήξουμε σε άτοπο, ότι $n \not\equiv 1 \mod \mathfrak{n}$. Τότε το $n - 1$ είναι μονάδα στον $A/\mathfrak{n}$. Όμως $1 = \det(g^{-1}\gamma g) = \kappa^2 \det \gamma' \in A$ και $\det \gamma' \equiv n \mod \mathfrak{n}$. Έτσι $\kappa \neq 1$ και επομένως το $\kappa - 1$ είναι μονάδα στον δακτύλιο $A/\mathfrak{n}$. Όμως τότε οι σχέσεις της εξίσωσης (5.2) οδηγούν σε άτοπο. [2] Συνεπώς $n \equiv 1 \mod \mathfrak{n}$.

❏

[1] Ξεκίνα από το c

[2] Ξεκίνα από το c

Από το προηγούμενα λήμματα, βλέπουμε ότι για να μελετήσουμε τον κανονικοποιητή της $\bar{\Gamma}_1(\mathfrak{n})$ στην $\mathrm{PGL}(2,L)$ αρκεί να μελετήσουμε τον κανονικοποιητή της $L^* \cdot \Gamma_1(\mathfrak{n})$ στην $\mathrm{GL}(2,L)$. Για οποιαδήποτε αριθμητική ομάδα Γ με οδηγό $\mathfrak{n}$, το επόμενο λήμμα συνδέει τον κανονικοποιητή της $K^* \cdot \Gamma$ στην $\mathrm{GL}(2,K)$ με τον κανονικοποιητή της $L^* \cdot \Gamma$ στην $\mathrm{GL}(2,L)$· αποτελεί δε, μία ασθενή γενίκευση του λήμματος [29, θεώρημα 1, α)], για όλες τις αριθμητικές ομάδες του τύπου αυτού.

Λημμα 5.2.3. *Έστω L/K επέκταση σωμάτων με $L \subset K_\infty$ και Γ αριθμητική ομάδα με οδηγό $\mathfrak{n}$. Τότε,*

$$\mathcal{N}_L(L^* \cdot \Gamma) = L^* \cdot \mathcal{N}_K(K^* \cdot \Gamma).$$

Απόδειξη. Προφανώς $L^* \cdot \mathcal{N}_K(K^* \cdot \Gamma) \subset \mathcal{N}_L(L^* \cdot \Gamma)$. Αντιστρόφως, έστω $g := \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ πίνακας $\mathcal{N}_L(L^* \cdot \Gamma)$. Παρατηρούμε αρχικά ότι οι πίνακες $x := \left(\begin{smallmatrix} 1 & \mathfrak{n} \\ 0 & 1 \end{smallmatrix}\right)$ και $y := \left(\begin{smallmatrix} 1 & 0 \\ \mathfrak{n} & 1 \end{smallmatrix}\right)$ ανήκουν σε κάθε αριθμητική ομάδα με οδηγό $\mathfrak{n}$. Αφού τα $g^{-1}xg$ και $g^{-1}yg$ πρέπει να ανήκουν στη $\mathbf{F}_q{}^* \cdot \Gamma$ (δες λήμμα 5.2.1), τα $\frac{\mathfrak{n}dc}{\det g}, \frac{\mathfrak{n}d^2}{\det g}, \frac{\mathfrak{n}c^2}{\det g}$ και τα $\frac{\mathfrak{n}ab}{\det g}, \frac{\mathfrak{n}a^2}{\det g}, \frac{\mathfrak{n}b^2}{\det g}$ είναι στοιχεία του A. Επίσης ($\det g = ad - cb$):

1. $\frac{a^2}{\det g} \cdot \frac{dc}{\det g} - \frac{ab}{\det g} \cdot \frac{c^2}{\det g} = \frac{ac}{\det g} \in K$

2. $\frac{c^2}{\det g} = \frac{ca}{\det g}\frac{cd}{\det g} - \frac{c^2}{\det g}\frac{cb}{\det g} \Longrightarrow \frac{cb}{\det g} \in K$ και

3. $\frac{db(ad-bc)}{\det^2 g} = \frac{db}{\det g} \in K$

Αν τώρα $c \neq 0$, τότε ο πίνακας $\frac{c}{\det g} \cdot g \in \mathcal{N}_K(K^* \cdot \Gamma)$. Αν $c = 0$, τότε $d \neq 0$ και ομοίως, ο πίνακας $\frac{d}{\det g} \cdot g \in \mathcal{N}_K(K^* \cdot \Gamma)$. ❏

Πορισμα 5.2.1. $\mathcal{N}_{\mathrm{GL}(2,K)}(K^* \cdot \Gamma_1(\mathfrak{n})) = K^* \cdot \mathcal{N}_{GL(2,A)}(\mathbf{F}_q^* \cdot \Gamma_1(\mathfrak{n}))$.

5.2.1 Ο κανονικοποιητής της $\mathcal{N}_K(\Gamma_1'(\mathfrak{n}))$

Για απλοποίηση των πράξεων (δες λήμμα 5.2.1), αλλά και επειδή θα χρειαστεί στα παρακάτω, αρχικά υπολογίζουμε τον κανονικοποιητή $\mathcal{N}_K(\Gamma_1'(\mathfrak{n}))$ της $\Gamma_1'(\mathfrak{n})$ στην $\mathrm{GL}(2,K)$.

Λημμα 5.2.4. *Τα στοιχεία $g \in \mathcal{N}_K(\Gamma_1'(\mathfrak{n}))$ μπορούν να γραφούν —κατά προσέγγιση πολλαπλασιασμού με πίνακα $k \cdot \mathrm{Id}_2$, $k \in K^*$— στη μορφή $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ έτσι ώστε τα $a,b,c,d \in A$ και $\langle a,b,c,d\rangle = A$. Η ορίζουσα $\mathfrak{q}$ του g ή είναι μονάδα του A (και άρα $g \in \mathcal{N}_A(\Gamma_1'(\mathfrak{n}))$) ή*

1. *$\mathfrak{q} \mid a, d, \gcd(\mathfrak{q}, b) = 1, \gcd(a, \mathfrak{n}) = (d, \mathfrak{n}) = \mathfrak{q}$ και $\mathfrak{n} \mid c$ είτε*

2. *$ad = 0, a, d \in \langle \mathfrak{n}\rangle = \langle c\rangle$ και b είναι μονάδα του A.*

Αντιστρόφως, τα στοιχεία $k \cdot \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ με $k \in K^*$ και $a,b,c,d \in A$ που ικανοποιούν τις παραπάνω σχέσεις, είναι στοιχεία του $\mathcal{N}_K(\Gamma_1'(\mathfrak{n}))$.

Απόδειξη. Έστω $g' \in \mathcal{N}_K(\Gamma_1'(\mathfrak{n}))$. Αφού το σώμα πηλίκων του A είναι το K και ο A είναι περιοχή κυρίων ιδεωδών, υπάρχει $\kappa \in K$ ώστε ο πίνακας $\kappa \cdot g' =: \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathcal{N}_K(\Gamma_1'(\mathfrak{n}))$ και $a,b,c,d \in A$, $\langle a,b,c,d\rangle = A$. Έστω $\mathfrak{q}$ η ορίζουσα του $g := \kappa \cdot g'$. Αν το $\mathfrak{q}$ είναι μονάδα τότε $g \in \mathcal{N}_A(\Gamma_1'(\mathfrak{n}))$. Αν το $\mathfrak{q}$ δεν είναι μονάδα του A, τότε προχωράμε ως εξής: Οι πίνακες $x = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, $y = \left(\begin{smallmatrix} 1 & \mathfrak{n} \\ 0 & 1 \end{smallmatrix}\right)$, και $z = \left(\begin{smallmatrix} 1 & 0 \\ \mathfrak{n} & 1 \end{smallmatrix}\right)$, ανήκουν στην $\Gamma_1'(\mathfrak{n})$. Επειδή $g \in \mathcal{N}_A(\Gamma_1'(\mathfrak{n}))$, έπεται ότι και οι πίνακες $g^{-1}xg, g^{-1}yg, g^{-1}zg \in \Gamma_1'(\mathfrak{n})$. Υπολογίζουμε τα στοιχεία των πινάκων αυτών και λαμβάνοντας υπόψιν τον ορισμό της ομάδας $\Gamma_1'(\mathfrak{n})$ καταλήγουμε στο συμπέρασμα ότι υπάρχουν υπάρχουν $a_i, b_i \in A, i = 1,2,3$ τέτοια ώστε

(1)	$cd = \mathfrak{n}\mathfrak{q}a_1$	(4)	$ab = \mathfrak{q}b_1$
(2)	$d^2 = \mathfrak{q}a_2$	(5)	$a^2 = \mathfrak{q}b_2$
(3)	$c^2 = \mathfrak{n}\mathfrak{q}a_3$	(6)	$\mathfrak{n}b^2 = \mathfrak{q}b_3$

Αν $b = 0$ τότε συνδυάζοντας τις $(2), (3), (5)$ και τον τύπο της ορίζουσας, έχουμε ότι $d = aa_2, a_2b_2 = 1$ και $c^2 = a^2 a_2 a_3 \mathfrak{n}$, άτοπο.[3] Έτσι $b \neq 0$. Ανάλογα δείχνουμε (χρησιμοποιώντας τις $(2), (4), (5)$ και τον τύπο της ορίζουσας) ότι το c δεν μπορεί επίσης να είναι μηδέν. [4]
Έστω $a = 0$. Από την (3) (και τον τύπο της ορίζουσας) έχουμε ότι $-c = \mathfrak{n} b a_3$. Πολλαπλασιάζοντας τις (3) και (6) κατά μέλη παίρνουμε $a_3 b_3 = 1$. Έτσι από την (3) έχουμε $d^2 = b^2 a_2 a_3 \mathfrak{n}$. Άρα $\langle a, b, c, d \rangle \subset \langle b \rangle$ άτοπο· εκτός εάν το b είναι μονάδα. Εύκολα βλέπει κανείς τότε, ότι το $\langle c \rangle = \langle \mathfrak{n} \rangle = \langle \mathfrak{q} \rangle$ και (με χρήση της (1)) $d \equiv 0 \mod \mathfrak{n}$.

Για λόγους συμμετρίας, αν τώρα υποθέσουμε ότι $d = 0$ τότε μπορούμε να δείξουμε ότι $b \in \mathbf{F}_q^*, \langle c \rangle = \mathfrak{q} = \langle \mathfrak{n} \rangle$ και $a \equiv 0 \mod \mathfrak{n}$.[5]

Στην περίπτωση κατά την οποία ισχύει $ad = 0$ έχουμε αποδείξει την (2).

Από εδώ και στο εξής, υποθέτουμε ότι όλα τα στοιχεία του g είναι μη μηδενικά. Θα αποδείξουμε τα ακόλουθα:

(1) $\mathfrak{q} \mid \mathfrak{n}$. Από τις $(2), (3)$ και (5) βλέπουμε ότι κάθε πρώτος διαιρέτης του $\mathfrak{q}$ διαιρεί τα a, d και c. Από την (6) βλέπουμε ότι το $\mathfrak{q}$ διαιρεί το $\mathfrak{n} b^2$. Αν $\mathfrak{p}$ είναι πρώτος διαιρέτης του $\mathfrak{q}$ τότε δεν μπορεί $\gcd(\mathfrak{p}, \mathfrak{n}) = 1$, γιατί τότε $\mathfrak{p} \mid b$ και δεδομένου ότι διαιρεί τα a, c, d καταλήγουμε σε άτοπο. Έτσι $\gcd(\mathfrak{q}, b) = 1$ και $\mathfrak{q} \mid \mathfrak{n}$.

(2) $\mathfrak{n} \mid c$. Πολλαπλασιάζοντας τις (2) και (3) κατά μέλη και υψώνοντας την (1) στο τετράγωνο [6] βλέπουμε ότι $\mathfrak{n}\mathfrak{q}^2 a_2 a_3 = \mathfrak{n}^2 \mathfrak{q}^2 a_1^2$, δηλ., $a_2 a_3 = \mathfrak{n} a_1^2$ και $\mathfrak{n} \mid a_2 a_3$. Θα δείξουμε ότι $\gcd(\frac{\mathfrak{n}}{\mathfrak{q}}, a_2) = 1$. Αν $\gcd(\frac{\mathfrak{n}}{\mathfrak{q}}, a_2) \neq 1$, έστω $\mathfrak{p}$ ένας πρώτος διαιρέτης του·

$$\begin{aligned} \mathfrak{q}^2 &= (ad - bc)^2 = a^2 d^2 + b^2 c^2 - 2ab \cdot cd = \\ &= \mathfrak{q}^2 b_2 a_2 + b^2 \mathfrak{n}\mathfrak{q} a_3 - 2\mathfrak{q}^2 \mathfrak{n} b_1 a_1, \end{aligned}$$

και διαιρώντας με $\mathfrak{q}^2$, παίρνουμε $1 = b_2 a_2 + b^2 \frac{\mathfrak{n}}{\mathfrak{q}} a_3 - 2\mathfrak{n} b_1 a_1$. Το $\mathfrak{p}$ διαιρεί τα $\frac{\mathfrak{n}}{\mathfrak{q}}, \mathfrak{n}, a_2$. Άρα, από την παραπάνω εξίσωση, το $\mathfrak{p}$ θα διαιρεί και το 1, άτοπο. Έτσι $\frac{\mathfrak{n}}{\mathfrak{q}} \mid a_3$. Τότε, από την (3) βλέπουμε ότι το $\mathfrak{n}^2 \mid c^2$, δηλ., $\mathfrak{n} \mid c$.

(3) $\mathfrak{q} \mid a$. Από την (4) βλέπουμε ότι $\mathfrak{q}$ διαιρεί το ab και από το προηγούμενο μέρος $\gcd(b, \mathfrak{q}) = 1$, έτσι το $\mathfrak{q}$ διαιρεί και το a.

(4) $\langle \mathfrak{q}, \frac{\mathfrak{n}}{\mathfrak{q}} \rangle = A$. Έστω $\mathfrak{q}'$ το γινόμενο των πρώτων διαιρετών του $\mathfrak{q}$. Από την (2) βλέπουμε ότι $\mathfrak{q}' \mid d$. Έχουμε δείξει ότι το $\mathfrak{q} \mid a$, $\mathfrak{n} \mid c$. Υπάρχουν κατάλληλα $\alpha, \gamma, \delta \in A$ ώστε $a = \mathfrak{q}\alpha$, $c = \mathfrak{n}\gamma$ και $d = \mathfrak{q}'\delta$. Τότε, $\mathfrak{q} = ad - bc = \mathfrak{q}\mathfrak{q}'\alpha\delta - \mathfrak{n} b\gamma$, έτσι $1 = \mathfrak{q}'\alpha\delta - \frac{\mathfrak{n}}{\mathfrak{q}} b\gamma$. Άρα, $1 = \gcd(\mathfrak{q}', \frac{\mathfrak{n}}{\mathfrak{q}}) = \gcd(\mathfrak{q}, \frac{\mathfrak{n}}{\mathfrak{q}})$.

(5) $\mathfrak{q} \mid d$. Από την περίπτωση **(4)** προκύπτει ότι ο μέγιστος κοινός διαιρέτης του γ και του $\mathfrak{q}$ είναι ένα. Τώρα (από την (1)) αφού $A \ni \frac{cd}{\mathfrak{n}\mathfrak{q}} = \frac{\gamma d}{\mathfrak{q}}$, βλέπουμε ότι $\frac{d}{\mathfrak{q}} \in A$.

(6) $\langle a, \mathfrak{n} \rangle = \langle d, \mathfrak{n} \rangle = \langle \mathfrak{q} \rangle$. Έχουμε ήδη δείξει ότι $\mathfrak{q} \mid a, \mathfrak{n}, d$. Έστω θ ο μέγιστος κοινός διαιρέτης του a και του $\mathfrak{n}$. Το $\mathfrak{q}$ διαιρεί το θ. Αφού το $\mathfrak{n}$ διαιρεί το c και το θ διαιρεί το $\mathfrak{n}$, θα πρέπει το θ να διαιρεί το c. Από την σχέση $\mathfrak{q} = ad - bc$ βλέπουμε ότι το θ διαιρεί το $\mathfrak{q}$. Ομοίως δείχνουμε ότι $\langle d, \mathfrak{n} \rangle = \langle \mathfrak{q} \rangle$.

---

[3] Τότε $a \mid a, c, d$ και άρα το a είναι μονάδα. Αλλά $\langle a \rangle = \langle d \rangle$ και άρα και η ορίζουσα $\mathfrak{q} = ad$ είναι μονάδα.

[4] $a_2 b_2 = 1, d = aa_2, a = db_2, b = aa_2 b_1, \mathfrak{q} = ad$.

[5] $(3) \Rightarrow c^2 = -\mathfrak{n} bc_3 = -\mathfrak{n} bca_3 \Rightarrow c = -\mathfrak{n} ba_3$. $(4) \Rightarrow ab = -bcb_1 \Rightarrow a = -bb_1$. Άρα το b διαιρεί τα a, b, c, d άτοπο· εκτός και αν το b είναι μονάδα. Πολλαπλασιάζοντας τις $(3), (6)$ κατά μέλη έχουμε $a_3 b_3 = 1$. Έτσι $\langle c \rangle = \langle \mathfrak{n} \rangle = \langle \mathfrak{q} \rangle$. Ακόμα $(4) \Rightarrow ab = -bcb_1 \Rightarrow a = -cb_1 \in \langle \mathfrak{n} \rangle$.

[6] $(2) \cdot (3) \Rightarrow (cd)^2 = \mathfrak{n}\mathfrak{q}^2 a_2 a_3$, $(1) \Rightarrow (cd)^2 = \mathfrak{n}^2 \mathfrak{q}^2 a_1^2$. Έτσι $\mathfrak{n}\mathfrak{q}^2 a_2 a_3 = \mathfrak{n}^2 \mathfrak{q}^2 a_1^2 \Rightarrow a_2 a_3 = \mathfrak{n} a_1^2$.

Στην περίπτωση που όλα τα στοιχεία του g είναι διάφορα μηδενός αποδείξαμε ότι ισχύει η (1) του λήμματος. Αντιστρόφως, αν υποθέσουμε ότι ισχύει η (2), τότε ο g θα έχει κατ΄ ανάγκη τη μορφή $g = \left(\begin{smallmatrix} 0 & w \\ \mathfrak{n} & m\mathfrak{n} \end{smallmatrix}\right)$ ή $\left(\begin{smallmatrix} m\mathfrak{n} & w \\ \mathfrak{n} & 0 \end{smallmatrix}\right)$ όπου w είναι μονάδα του A· έτσι $g \in \mathcal{N}_K(\Gamma_1'(\mathfrak{n}))$.

Πράγματι, αν h είναι ο τυχόν $h := \left(\begin{smallmatrix} 1+\mathfrak{n}X & Y \\ \mathfrak{n}Z & 1+\mathfrak{n}W \end{smallmatrix}\right) \in \Gamma_1'(\mathfrak{n})$, με $X, Y, Z, W \in A$, τότε:

$$\left(\begin{smallmatrix} 0 & w \\ \mathfrak{n} & m\mathfrak{n} \end{smallmatrix}\right)^{-1} h \left(\begin{smallmatrix} 0 & w \\ \mathfrak{n} & m\mathfrak{n} \end{smallmatrix}\right) = \begin{pmatrix} 1-Ymw^{-1}\mathfrak{n}+W\mathfrak{n} & * \\ Yw^{-1}\mathfrak{n} & 1+Ymw^{-1}\mathfrak{n}+X\mathfrak{n} \end{pmatrix} \in \Gamma_1'(\mathfrak{n})$$
$$\left(\begin{smallmatrix} m\mathfrak{n} & w \\ \mathfrak{n} & 0 \end{smallmatrix}\right)^{-1} h \left(\begin{smallmatrix} m\mathfrak{n} & w \\ \mathfrak{n} & 0 \end{smallmatrix}\right) = \begin{pmatrix} 1+W\mathfrak{n}+Zm\mathfrak{n} & * \\ Yw^{-1}\mathfrak{n}-Wm\mathfrak{n}^2+Xmw^{-1}\mathfrak{n}^2-Zm^2w^{-1}\mathfrak{n}^2 & 1+X\mathfrak{n}-Zm\mathfrak{n} \end{pmatrix} \in \Gamma_1'(\mathfrak{n})$$

Τέλος, κλείνοντας, θα δείξουμε ότι οι πίνακες της μορφής $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ με $a, b, c, d, \alpha, \gamma, \delta, \mathfrak{q} \in A, abcd \neq 0, \mathfrak{q} = \det g, a = \mathfrak{q}\alpha, c = \mathfrak{n}\gamma, d = \mathfrak{q}\delta$ και $\gcd(\mathfrak{n}, d) = \gcd(\mathfrak{n}, a) = \mathfrak{q}, \gcd(\mathfrak{n}, c) = \mathfrak{n}$, κανονικοποιούν την $\Gamma_1'(\mathfrak{n})$. Θέτουμε $\left(\begin{smallmatrix} a_1 & a_2 \\ a_3 & a_2 \end{smallmatrix}\right) := g^{-1}hg$. Αποδεικνύεται η ύπαρξη κατάλληλων σταθερών $\mathfrak{x}, \mathfrak{y}, \mathfrak{z} \in A$ με

$$\begin{aligned} a_1 = (\frac{d(1+\mathfrak{n}x)}{\mathfrak{q}} - \frac{b\mathfrak{n}z}{\mathfrak{q}})a + (\frac{dy}{\mathfrak{q}} - \frac{b(1+\mathfrak{n}w)}{\mathfrak{q}})c = \delta a - b\gamma\frac{\mathfrak{n}}{\mathfrak{q}} + \mathfrak{n}\cdot\mathfrak{x} = 1 + \mathfrak{n}\cdot\mathfrak{x} \\ a_2 = \frac{d(Yd + b(X\mathfrak{n}+1))}{\mathfrak{q}} - \frac{b(Zb\mathfrak{n} + d(W\mathfrak{n}+1))}{\mathfrak{q}} \\ a_3 = (-\frac{c(1+\mathfrak{n}X)}{\mathfrak{q}} + \frac{a\mathfrak{n}Z}{\mathfrak{q}})a + (-\frac{cY}{\mathfrak{q}} + \frac{a(1+\mathfrak{n}W)}{\mathfrak{q}})c = \mathfrak{n}\cdot\mathfrak{y} \\ a_4 = (-\frac{c(1+\mathfrak{n}X)}{\mathfrak{q}} + \frac{a\mathfrak{n}Z}{\mathfrak{q}})b + (-\frac{cY}{\mathfrak{q}} + \frac{a(1+\mathfrak{n}W)}{\mathfrak{q}})d = -b\gamma\frac{\mathfrak{n}}{\mathfrak{q}} + \delta a + \mathfrak{n}\cdot\mathfrak{z} = 1 + \mathfrak{n}\cdot\mathfrak{z} \end{aligned}$$

❏

Συμβολισμός 7. Από δω και στο εξής, ένας πίνακας «τύπου Α» θα είναι κάθε πίνακας της μορφής $\left(\begin{smallmatrix} 0 & w \\ \mathfrak{n} & m\mathfrak{n} \end{smallmatrix}\right)$ ή $\left(\begin{smallmatrix} m\mathfrak{n} & w \\ \mathfrak{n} & 0 \end{smallmatrix}\right)$ με $w \in \mathbf{F}_q^*, m \in A$ και ένας πίνακας «τύπου Β» θα είναι κάθε πίνακας $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ όπου τα a, b, c, d ικανοποιούν τις σχέσεις του πρώτου σκέλους του λήμματος 5.2.4. Επίσης, κάθε φορά που αναφερόμαστε σε ένα πίνακα $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \mathcal{N}_K(\Gamma_1'(\mathfrak{n}))$ «τύπου Β», θα θεωρούμε την ύπαρξη -χωρίς καμία επιπλέον αναφορά- των αντίστοιχων ελληνικών γραμμάτων α, γ, δ και του γοτθικού γράμματος $\mathfrak{q} = \det g$, τα οποία θα υποθέτουμε ότι ικανοποιούν τις σχέσεις $a = \mathfrak{q}\alpha, c = \mathfrak{n}\gamma, d = \mathfrak{q}\delta$, και $\gcd(\mathfrak{q}, b) = 1, \gcd(a, \mathfrak{n}) = (d, \mathfrak{n}) = \mathfrak{q}$.

5.2.2 Η δομή της $\Gamma_1(\mathfrak{n})$

Με W θα συμβολίζουμε την υποομάδα της $\Gamma_1(\mathfrak{n})$ η οποία αποτελείται από τους πίνακες της μορφής $\left(\begin{smallmatrix} 1 & 0 \\ 0 & w \end{smallmatrix}\right)$ όπου w είναι μονάδα του $A = \mathbf{F}_q[T]$· η W είναι κυκλική και πεπερασμένη.

Λημμα 5.2.5. $\Gamma_1(\mathfrak{n}) = \Gamma_1'(\mathfrak{n}) \rtimes W$.

Απόδειξη. Παρατηρούμε ότι η παρακάτω ακολουθία είναι split, αφού ${\mathbf{F}_q}^* \cong W$.

$$1 \longrightarrow \Gamma_1'(\mathfrak{n}) \longrightarrow \Gamma_1(\mathfrak{n}) \xrightarrow{\det} {\mathbf{F}_q}^* \longrightarrow 1.$$

❏

Σημείωση 10. Η τάξη της πολλαπλασιαστικής ομάδας $(A/\mathfrak{n}A)^*$, με $\mathfrak{n} \in A$ είναι, ως γνωστόν ίση προς $\varphi(\mathfrak{n}) = q^{\deg(\mathfrak{n})}\prod_{\mathfrak{p}|\mathfrak{n}}(1 - q^{-\deg(\mathfrak{p})})$ (δες [30, §1.1]).

Λημμα 5.2.6. *Έστω $\mathfrak{n} \in A$ ένα μη τετριμμένο πολυώνυμο. Τότε, $\varphi(\mathfrak{n}) = 1$ αν και μόνο αν $q = 2$ και το $\mathfrak{n}$ είναι γινόμενο (πρώτων) πολυωνύμων βαθμού ένα.*

Απόδειξη. Έστω $\mathfrak{n} = \prod_{\mathfrak{p}} \mathfrak{p}^{d_{\mathfrak{p}}}$. Τότε,
$\varphi(\mathfrak{n}) = q^{\deg(\mathfrak{n})}\prod_{\mathfrak{p}|\mathfrak{n}}(1 - q^{-\deg(\mathfrak{p})}) = \prod_{\mathfrak{p}|\mathfrak{n}}(q^{\deg(\mathfrak{p})d_{\mathfrak{p}}} - q^{\deg(\mathfrak{p})d_{\mathfrak{p}}-\deg(\mathfrak{p})})$. Άρα, $\varphi(\mathfrak{n}) = 1$ αν και μόνο αν, $\forall\mathfrak{p}, q^{\deg(\mathfrak{p})d_{\mathfrak{p}}} - q^{\deg(\mathfrak{p})d_p-\deg(\mathfrak{p})} = 1$. Έτσι, $\forall\mathfrak{p}, d_{\mathfrak{p}} = 1, \deg(\mathfrak{p} = 1)$ και $q = 2$. ❏

Ως συνέπεια του λήμματος 5.2.5 έχουμε το παρακάτω

Πορισμα 5.2.2. *Αν $q = 2$ τότε $\Gamma_1(\mathfrak{n}) = \Gamma_1'(\mathfrak{n})$ και αν $\varphi(\mathfrak{n}) = 1$ τότε $\Gamma_0(\mathfrak{n}) = \Gamma_1(\mathfrak{n}) = \Gamma_1'(\mathfrak{n})$.*

Απόδειξη. Έστω $g = \left(\begin{smallmatrix} k & l \\ m & n \end{smallmatrix}\right) \in \Gamma_1(\mathfrak{n})$. Τότε $\det g = 1$ και $k \equiv 1 \mod \mathfrak{n}$, $m \equiv 0 \mod \mathfrak{n}$. Ακόμα, $1 = kn - lm \equiv n \mod \mathfrak{n}$, δηλ., $g \in \Gamma_1'(\mathfrak{n})$. ❑

5.2.3 Ο κανονικοποιητής της $\mathbf{F}_q^* \cdot \Gamma_1(\mathfrak{n})$ στην $\mathrm{GL}(2, A)$

Λημμα 5.2.7. *Ο κανονικοποιητής $\mathbf{F}_q^* \cdot \Gamma_1(\mathfrak{n})$ στην $\mathrm{GL}(2, A)$ είναι η ομάδα $\Gamma_0(\mathfrak{n})$.*

Απόδειξη. Είναι προφανές ότι η $\Gamma_0(\mathfrak{n})$ κανονικοποιεί την $\mathbf{F}_q^*, \Gamma_1(\mathfrak{n})$. [7] Αντιστρόφως, έστω $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ ένα στοιχείο του κανονικοποιητή της $\mathbf{F}_q^* \cdot \Gamma_1(\mathfrak{n})$ στην $\mathrm{GL}(2, A)$. Έστω $\mathfrak{q}$ η ορίζουσα του. Έστω $z := \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right) \in \Gamma_1(\mathfrak{n})$. Αφού $g^{-1} z g = \begin{pmatrix} 1+cd/\mathfrak{q} & d^2/\mathfrak{q} \\ -c^2/\mathfrak{q} & 1-cd/\mathfrak{q} \end{pmatrix} \in \mathbf{F}_q^* \cdot \Gamma_1(\mathfrak{n})$, θα πρέπει το $c^2 \equiv 0 \mod \mathfrak{n}$ και το $1 + cd/\mathfrak{q}$ να είναι μονάδα modulo $\mathfrak{n}$. Έστω λοιπόν $w \in \mathbf{F}_q^*$ τέτοιο ώστε $w \equiv 1 + cd/\mathfrak{q} \mod \mathfrak{n}$. Όμως $\mathfrak{q} = ad - bc$ και έτσι $\mathfrak{q}^2 \equiv ad(ad - 2bc) \mod \mathfrak{n}$, δηλαδή τα a, d είναι αντιστρέψιμα στοιχεία του δακτυλίου $A/\mathfrak{n}$. Αν $w \equiv 1 \mod \mathfrak{n}$, τότε $cd/\mathfrak{q} \equiv 0 \mod \mathfrak{n}$ και έτσι θα είναι $c \equiv 0 \mod \mathfrak{n}$. Αν τώρα $w \not\equiv 1 \mod \mathfrak{n}, x$ τότε $c + c^2 d/\mathfrak{q} \equiv wc \mod \mathfrak{n}$ και έτσι $(1 - w)c \equiv 0 \mod \mathfrak{n}$, δηλαδή και σε αυτή την περίπτωση $c \equiv 0 \mod \mathfrak{n}$. ❑

Ο κανονικοποιητής της $\Gamma_1(\mathfrak{n})$ στην $\mathrm{GL}(2, K)$

Έστω $\mathfrak{n} \in A$ ένα μη τετριμμένο πολυώνυμο και $\mathfrak{n} = \prod_i^n \mathfrak{p}_i^{d_i}$ η παραγοντοποίησή του σε γινόμενο αναγώγων πολυωνύμων. Για κάθε i, θέτουμε $\mathfrak{q}_i = \mathfrak{p}_i^{d_i}$. Αν $n \geq 2$ τότε για κάθε i υπάρχουν μη μηδενικά $a_i, b_i \in A$ με

$$\mathfrak{q}_i a_i - \frac{\mathfrak{n}}{\mathfrak{q}_i} b_i = 1. \tag{5.3}$$

Στην περίπτωση αυτή, για κάθε i θέτουμε

$$g_{\mathfrak{q}_i} := \left(\begin{smallmatrix} \mathfrak{q}_i a_i & b_i \\ \mathfrak{n} & q_i \end{smallmatrix}\right) \tag{5.4}$$

διαφορετικά ($\mathfrak{q}_1 = \mathfrak{n}$) θέτουμε

$$g_{\mathfrak{n}} := \left(\begin{smallmatrix} 0 & 1 \\ \mathfrak{n} & 0 \end{smallmatrix}\right) \tag{5.5}$$

Προταση 5.2.1. *Ο κανονικοποιητής της $K^* \cdot \Gamma_1(\mathfrak{n})$ στην $\mathrm{GL}(2, K)$ είναι*

1. *$K^* \cdot \Gamma_0(\mathfrak{n}) \cdot \langle \left(\begin{smallmatrix} 0 & 1 \\ \mathfrak{n} & 0 \end{smallmatrix}\right) \rangle$, αν $q \geq 3$.*
2. *$K^* \cdot \Gamma_0(\mathfrak{n}), \left(\begin{smallmatrix} 0 & 1 \\ \mathfrak{n} & 0 \end{smallmatrix}\right)$, αν $q \geq 2$ και το $\mathfrak{n}$ είναι δύναμη πρώτου ή*
   $K^* \cdot \Gamma_0(\mathfrak{n}), g_{\mathfrak{q}_1}, \ldots, g_{\mathfrak{q}_n}$ αν $q = 2$ και $\varphi(\mathfrak{n}) \geq 2$, όπου τα $g_{\mathfrak{q}_i}$ είναι όπως παραπάνω. Ακόμα, για όλα τα $i, g_{\mathfrak{q}_i^2} \in \langle K^* \cdot \Gamma_0(\mathfrak{n}) \rangle$ και

   $$K^* \cdot \langle \cdot g_{\mathfrak{q}_1}, \ldots, g_{\mathfrak{q}_n} \rangle \cap K^* \cdot \langle \Gamma_0(\mathfrak{n}) \rangle = K^* \cdot \langle g_{\mathfrak{q}_1}^2, \ldots, g_{\mathfrak{q}_n}^2 \rangle.$$

3. *$K^* \cdot \Gamma_0(\mathfrak{n}) \cdot \langle \left(\begin{smallmatrix} 0 & 1 \\ \mathfrak{n} & 0 \end{smallmatrix}\right) \rangle$, αν $q = 2, \varphi(\mathfrak{n}) = 1$ και $\mathfrak{n} = T, T+1$ ή*
   $\langle K^* \cdot \Gamma_0(\mathfrak{n}), \left(\begin{smallmatrix} 0 & 1 \\ \mathfrak{n} & 0 \end{smallmatrix}\right), \left(\begin{smallmatrix} T & 1 \\ T(T+1) & T \end{smallmatrix}\right) \rangle$, αν $q = 2, \varphi(\mathfrak{n}) = 1$ και $\mathfrak{n} = T(T+1)$.

Απόδειξη. Έστω $g \in \mathcal{N}_K(K^* \cdot \Gamma_1(\mathfrak{n}))$. Τότε από το λήμμα 5.2.2, $g \in \mathcal{N}_K(\Gamma_1'(\mathfrak{n}))$ και έτσι, υπάρχει $k \in K^*$ τέτοιο ώστε το $g_0 := k \cdot g$ να ικανοποιεί τις υποθέσεις του λήμματος 5.2.4. Αν $\det g_0 \in A^*$ τότε $g_0 \in \mathcal{N}_A(\mathbf{F}_q^* \cdot \Gamma_1(\mathfrak{n}))$ και έτσι από το λήμμα 5.2.7, $g_0 \in \Gamma_0(\mathfrak{n})$. Αν $\det g_0 \notin A^*$ τότε $g_0 = \left(\begin{smallmatrix} 0 & w \\ \mathfrak{n} & m\mathfrak{n} \end{smallmatrix}\right), g_0 = \left(\begin{smallmatrix} m\mathfrak{n} & w \\ \mathfrak{n} & 0 \end{smallmatrix}\right)$ με $w \in \mathbf{F}_q^*, m \in A$ ή $g_0 = \begin{pmatrix} \mathfrak{q}\alpha & b \\ \mathfrak{n}\gamma & \mathfrak{q}\delta \end{pmatrix}$ με $a = \alpha\mathfrak{q}, b, c = \gamma\mathfrak{n}, d = \delta\mathfrak{q}$ και $\mathfrak{q}$ όπως το λήμμα 5.2.4.

Αν το g_0 είναι «τύπου A», τότε το γινόμενο $g_0 \left(\begin{smallmatrix} 0 & 1 \\ \mathfrak{n} & 0 \end{smallmatrix}\right) \in K^* \cdot \Gamma_0(\mathfrak{n}) \cdot$ [8] έτσι η υποομάδα που γεννιέται από το K^* την $\Gamma_0(\mathfrak{n})$ και τους «τύπου A» πίνακες είναι η $K^* \cdot \Gamma_0(\mathfrak{n})$ -η οποία κανονικοποιεί την $K^* \cdot \Gamma_1(\mathfrak{n})$, αφού ο

---

[7] Έστω $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(\mathfrak{n})$ και $h = \left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \Gamma_1(\mathfrak{n})$. Τότε, $g^{-1} h g \equiv \begin{pmatrix} 1 & \frac{b+dy-bw}{a} \\ 0 & w \end{pmatrix} \mod \mathfrak{n}$.

[8] Αν $g_0 = \left(\begin{smallmatrix} 0 & w \\ \mathfrak{n} & m\mathfrak{n} \end{smallmatrix}\right)$ τότε $g_0 \left(\begin{smallmatrix} 0 & 1 \\ \mathfrak{n} & 0 \end{smallmatrix}\right) = \begin{pmatrix} \mathfrak{n}w & 0 \\ m\mathfrak{n}^2 & \mathfrak{n} \end{pmatrix} = \mathfrak{n}w^{-1} \cdot \left(\begin{smallmatrix} 1 & 0 \\ wm\mathfrak{n} & w \end{smallmatrix}\right) \in K^* \cdot \Gamma_1(\mathfrak{n})$

πίνακας $\left(\begin{smallmatrix} 0 & 1 \\ \mathfrak{n} & 0 \end{smallmatrix}\right)$ την κανονικοποιεί [9] (δες επίσης το λήμμα 5.2.7).

Αν το g_0 είναι «τύπου Β» με $\det g = \mathfrak{n}$, τότε $g\left(\begin{smallmatrix} 0 & 1 \\ \mathfrak{n} & 0 \end{smallmatrix}\right) \in K^* \cdot \Gamma_0(\mathfrak{n})$. [10]

(1) $q \geq 3$. Θα δείξουμε ότι κανένας πίνακας g_0 «τύπου Β» δεν ανήκει στον κανονικοποιητή - εκτός και αν $\langle \det g \rangle = \langle \mathfrak{n} \rangle$ (δες παραπάνω). Έστω $g' := \left(\begin{smallmatrix} 1 & 0 \\ 0 & w' \end{smallmatrix}\right) \in \Gamma_1(\mathfrak{n})$ με w' μονάδα του A και $w' \neq 1$. Υποθέτουμε ότι υπάρχει $g_0 = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ «τύπου Β» με $\det g_0 = \mathfrak{q}, \langle \mathfrak{n} \rangle \neq \langle \mathfrak{q} \rangle$ και $g_0^{-1} g' g_0 \in K^* \cdot \Gamma_1(\mathfrak{n})$. Τότε, κατ' ανάγκη $g_0^{-1} g' g_0 \in \mathbf{F}_q \cdot \Gamma_1(\mathfrak{n})$ (δες λήμμα 5.2.1). Κάνοντας πράξεις, παίρνουμε $g_0^{-1} g' g_0 = \begin{pmatrix} 1+b\frac{c}{\mathfrak{q}}(1-w') & * \\ \frac{ac(w'-1)}{\mathfrak{q}} & 1-\frac{ad}{\mathfrak{q}}(1-w') \end{pmatrix}$. Θα πρέπει επομένως, η παράσταση $1-\frac{ad}{\mathfrak{q}}(1-w') \in \mathbf{F}_q^* \mod \mathfrak{n}$. Έστω $u \in \mathbf{F}_q^*$ ώστε $1-\frac{ad}{\mathfrak{q}}(1-w') \equiv u \mod \mathfrak{n}$. Τότε $1-u \equiv \frac{a}{\mathfrak{q}}d(1-w') \mod \mathfrak{n}$. Αν $u \neq 1$, το $1-u$ είναι μονάδα στον $A/\mathfrak{n}$ και έτσι είναι και το d· άτοπο, αφού $\gcd(d,\mathfrak{n}) = \mathfrak{q}$. Αν το $u = 1$ τότε κατ' ανάγκη $1 + b\frac{c}{\mathfrak{q}}(1-w') \equiv w' \mod \mathfrak{n}$ και άρα $b\frac{c}{\mathfrak{q}}(1-w') \equiv -(1-w') \mod \mathfrak{n}$. Αφού $\gcd(b,\mathfrak{n}) = 1$ και $w' \neq 1$ θα είναι το κλάσμα $\frac{c}{\mathfrak{q}}$ είναι αντιστρέψιμο στον $A/\mathfrak{n}$· άτοπο γιατί τότε $\mathfrak{q} = \mathfrak{n}$ ($\gcd(c,\mathfrak{n}) = \mathfrak{n}$). Έτσι, σύμφωνα με τα λήμματα 5.2.4 και 5.2.7, $\mathcal{N}_K(K^* \cdot \Gamma_1(\mathfrak{n})) = K^* \cdot \Gamma_0(\mathfrak{n}) \cdot \langle \left(\begin{smallmatrix} 0 & 1 \\ \mathfrak{n} & 0 \end{smallmatrix}\right) \rangle$.

Στα παρακάτω υποθέτουμε ότι $q = 2$. Σύμφωνα με το πόρισμα 5.2.2, $\Gamma_1(\mathfrak{n}) = \Gamma_1'(\mathfrak{n})$. Έστω g_0, g_0' δύο πίνακες «τύπου Β». Αν $\langle \det g_0 \rangle = \langle \det g_0' \rangle = \langle \mathfrak{q} \rangle$ τότε είναι εύκολο να δει κανείς ότι $\frac{1}{\mathfrak{q}} g_0 g_0' \in \Gamma_0(\mathfrak{n})$.[11] Αν $\langle \det g_0 \rangle \neq \langle \det g_0' \rangle$ τότε αρκεί να θεωρήσουμε μόνο την περίπτωση που $\gcd(\det g_0, \det g_0') = 1$ διότι τότε ο πίνακας $g_0 g_0'$ είναι επίσης «τύπου Β». Έτσι

$$\mathcal{N}_K(K^* \cdot \Gamma_1(\mathfrak{n})) = K^* \cdot \Gamma_0(\mathfrak{n}) \cdot \langle g_{\mathfrak{q}_1}, \ldots, g_{\mathfrak{q}_n} \rangle \text{ αν } n \geq 2$$
$$\mathcal{N}_K(K^* \cdot \Gamma_1(\mathfrak{n})) = K^* \cdot \Gamma_0(\mathfrak{n}) \text{ αν } n = 1.$$

Συνεχίζοντας θέτουμε $G := K^* \cdot \langle g_{\mathfrak{q}_1}, \ldots, g_{\mathfrak{q}_i} \rangle$. Είναι προφανές ότι για κάθε $i \neq j, g_{\mathfrak{q}_i}^2 \in \mathfrak{q}_i \cdot \Gamma_0(\mathfrak{n})$ και $g_{\mathfrak{q}_i} g_{\mathfrak{q}_j} g_{\mathfrak{q}_i}^{-1} g_{\mathfrak{q}_j}^{-1} \in \Gamma_0(\mathfrak{n})$. [12] Έτσι

$$G \cap (K^* \cdot \Gamma_0(\mathfrak{n})) = K^* \cdot \langle \mathfrak{q}_1^2, \ldots, g_{\mathfrak{q}_n}^2 \rangle.$$

Έτσι έχει δειχθεί η **(2)**.

(3) $\mathbf{q = 2}$ και $\boldsymbol{\varphi(\mathfrak{n}) = 1}$. Τα μοναδικά πολυώνυμα $\mathfrak{n} \in \mathbf{F}_q[T]$ για τα οποία ισχύει $\varphi(\mathfrak{n}) = 1$ είναι τα $T, T+1$ και $T(T+1)$. Διακρίνουμε τις περιπτώσεις:

(1) Η περίπτωση $\mathfrak{n} = T$. Θέτουμε $g_T := \left(\begin{smallmatrix} T & T+1 \\ T & T \end{smallmatrix}\right)$ και $g_0 := \left(\begin{smallmatrix} 0 & 1 \\ T & 0 \end{smallmatrix}\right)$. Τότε $g_T g_0 = T \cdot \left(\begin{smallmatrix} T+1 & 1 \\ T & 1 \end{smallmatrix}\right)$. Άρα

$$\mathcal{N}_K(K^* \cdot \Gamma_1(\mathfrak{n})) = K^* \cdot \Gamma_0(\mathfrak{n}) \cdot \langle g_0 \rangle.$$

(2) Η περίπτωση $\mathfrak{n} = T+1$. Θέτουμε $g_{T+1} := \left(\begin{smallmatrix} T+1 & T \\ T+1 & T+1 \end{smallmatrix}\right)$ και $g_0 := \left(\begin{smallmatrix} 0 & 1 \\ T+1 & 0 \end{smallmatrix}\right)$. Τότε $g_T g_0 = (T+1) \cdot g'$, όπου $g' = \left(\begin{smallmatrix} T & 1 \\ T+1 & 1 \end{smallmatrix}\right) \in \Gamma_0(\mathfrak{n})$ και έτσι

$$\mathcal{N}_K(K^* \cdot \Gamma_1(\mathfrak{n})) = K^* \cdot \Gamma_0(\mathfrak{n}) \cdot \langle g_0 \rangle.$$

(3) Η περίπτωση $\mathfrak{n} = T(T+1)$. Θέτουμε $g_T := \left(\begin{smallmatrix} T & 1 \\ T(T+1) & T \end{smallmatrix}\right)$, $g_{T+1} = \begin{pmatrix} T+1 & 1 \\ T(T+1) & T+1 \end{pmatrix}$ και $g_{\mathfrak{n}} = \left(\begin{smallmatrix} 0 & 1 \\ \mathfrak{n} & 0 \end{smallmatrix}\right)$. Τότε $g_T g_{T+1} = g_{\mathfrak{n}}$. Ακόμα

$$\mathcal{N}_K(K^* \cdot \Gamma_1(\mathfrak{n})) = K^* \cdot \Gamma_0(\mathfrak{n}) \cdot \langle g_0 \rangle.$$

❏

---

[9] $g = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(\mathfrak{n})$. Τότε $a \equiv 1 \mod \mathfrak{n}, c \equiv 0 \mod \mathfrak{n}, d \in \mathbf{F}_q^* \mod \mathfrak{n}$ και $\left(\begin{smallmatrix} 0 & 1 \\ \mathfrak{n} & 0 \end{smallmatrix}\right)^{-1} g \left(\begin{smallmatrix} 0 & 1 \\ \mathfrak{n} & 0 \end{smallmatrix}\right) = \begin{pmatrix} d & \frac{c}{\mathfrak{n}} \\ b\mathfrak{n} & a \end{pmatrix} \in K^* \cdot \Gamma_1(\mathfrak{n})$.

[10] $g = \begin{pmatrix} \alpha\mathfrak{n} & b \\ \gamma\mathfrak{n} & \delta\mathfrak{n} \end{pmatrix} \Rightarrow g\left(\begin{smallmatrix} 0 & 1 \\ \mathfrak{n} & 0 \end{smallmatrix}\right) = \begin{pmatrix} b\mathfrak{n} & \alpha\mathfrak{n} \\ \delta\mathfrak{n}^2 & \gamma\mathfrak{n} \end{pmatrix} = \mathfrak{n} \cdot \begin{pmatrix} b & \alpha \\ \delta\mathfrak{n} & \gamma \end{pmatrix} \in K^* \cdot \Gamma_0(\mathfrak{n})$

[11] Αν $g_0 = \begin{pmatrix} \alpha\mathfrak{q} & b \\ \gamma\mathfrak{n} & \delta\mathfrak{q} \end{pmatrix}$ και $g_0' = \left(\begin{smallmatrix} x\mathfrak{q} & y \\ z\mathfrak{n} & w\mathfrak{q} \end{smallmatrix}\right)$ τότε $\frac{1}{\mathfrak{q}} g_0 g_0' = \begin{pmatrix} \alpha\mathfrak{q}x + bz\frac{\mathfrak{n}}{\mathfrak{q}} & bw+\alpha y \\ \gamma\mathfrak{q}x\frac{\mathfrak{n}}{\mathfrak{q}} + \delta\mathfrak{q}z\frac{\mathfrak{n}}{\mathfrak{q}} & \delta\mathfrak{q}w + \gamma y\frac{\mathfrak{n}}{\mathfrak{q}} \end{pmatrix}$

[12] Αν $g_{\mathfrak{q}_i} = \begin{pmatrix} a_i\mathfrak{q}_i & b_i \\ \mathfrak{n} & \mathfrak{q}_i \end{pmatrix}$ τότε $\frac{1}{\mathfrak{q}_i} \cdot g_{\mathfrak{q}_i}^2 = \begin{pmatrix} b_i\frac{\mathfrak{n}}{\mathfrak{q}_i} + a_i^2\mathfrak{q}_i & b_i + a_i b_i \\ \mathfrak{n}(1+a) & b_i\frac{\mathfrak{n}}{\mathfrak{q}_i} + \mathfrak{q}_i \end{pmatrix}$. Ακόμα, $\mathfrak{q}_i \cdot g_{\mathfrak{q}_i}^{-1} = \begin{pmatrix} \mathfrak{q}_i & -b_i \\ -n & a_i\mathfrak{q}_i \end{pmatrix}$, δηλαδή είναι ένας πίνακας «τύπου Β». Αν τώρα $g_{\mathfrak{q}_j} = \begin{pmatrix} a_j\mathfrak{q}_j & b_j \\ \mathfrak{n} & \mathfrak{q}_j \end{pmatrix}$ με $i \neq j$, τότε ο πίνακας $\frac{1}{\mathfrak{q}_i\mathfrak{q}_j} g_{\mathfrak{q}_i} g_{\mathfrak{q}_j} (\mathfrak{q}_i \cdot g_{\mathfrak{q}_i}^{-1})(\mathfrak{q}_j \cdot g_{\mathfrak{q}_j}^{-1})$ είναι γινόμενο δύο πινάκων «τύπου Β» με ίσες ορίζουσες και άρα ανήκει στην $\Gamma_0(\mathfrak{n})$.

ΘΕΩΡΗΜΑ 5.2.1. *Η ομάδα των modular αυτομορφισμών της $\Gamma_1(\mathfrak{n})\backslash\Omega$ είναι ισόμορφη προς:*

1. *Την ομάδα $(\mathrm{A}/\mathfrak{n})^*/\mathbf{F}_q^* \rtimes (\mathbb{Z}/2\mathbb{Z})$, αν $q \geq 3$*
2. *Μία επέκταση της $(\mathrm{A}/\mathfrak{n})^*/\mathbf{F}_q^*$ με την $(\mathbb{Z}/2\mathbb{Z})^n$, αν $q = 2$ και $\varphi(\mathfrak{n}) \geq 2$, όπου το n συμβολίζει τον αριθμό των διαφορετικών πρώτων διαιρετών του $\mathfrak{n}$*
3. *Την ομάδα $(\mathbb{Z}/2\mathbb{Z})^n$, αν $q = 2$ και $\varphi(\mathfrak{n}) = 1$, όπου το n συμβολίζει τον αριθμό των διαφορετικών πρώτων διαιρετών του $\mathfrak{n}$ και $n = 1$ ή 2.*

Απόδειξη. Σε κάθε περίπτωση η ομάδα $K_\infty^* \cdot \Gamma_0(\mathfrak{n})/K_\infty^* \cdot \Gamma_1(\mathfrak{n})$ είναι κανονική υποομάδα της $\mathcal{N}_{K_\infty}(K_\infty^* \cdot \Gamma_1(\mathfrak{n}))/K_\infty^* \cdot \Gamma_1(\mathfrak{n})$. Ορίζουμε τον ομομορφισμό

$$K_\infty^* \cdot \Gamma_0(\mathfrak{n})/K_\infty^* \cdot \Gamma_1(\mathfrak{n}) \longrightarrow (\mathrm{A}/\mathfrak{n})^*/\mathbf{F}_{\mathrm{q}}^* \cdot \quad \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \mathrm{K}_\infty^* \cdot \Gamma_1(\mathfrak{n}) \longmapsto d,$$

ο οποίος είναι στην πραγματικότητα ένας αυτομορφισμός: 1. Αν $m \in A$ με $\gcd(m, \mathfrak{n}) = 1$, τότε, υπάρχουν $a, b \in A$ με $am + n\mathfrak{n} = 1$· έτσι ο πίνακας $g := \left(\begin{smallmatrix} am & bm \\ \mathfrak{n} & m \end{smallmatrix}\right) \in \Gamma_0(\mathfrak{n})$ και απεικονίζεται στο m. 2. Έστω $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_0(\mathfrak{n})$ με $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) K_\infty^* \cdot \Gamma_1(\mathfrak{n}) \longmapsto d \cdot \mathbf{F}_q^* = \mathbf{F}_q^*$. Τότε, αφού $\mathbf{F}_q^* \ni u := ad - bc$ θα έχουμε $u \mod \mathfrak{n} = ad \mod \mathfrak{n}$ και επειδή $d \in \mathbf{F}_q^*$ υπάρχει $v \in \mathbf{F}_q^*$ με $v \mod \mathfrak{n} = d \mod \mathfrak{n}$ και έτσι ο πίνακας $v^{-1}\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in \Gamma_1(\mathfrak{n})$.

(1) Η περίπτωση $q \geq 3$. Από την πρόταση 5.2.1,

$$\mathcal{N}_{K_\infty}(K_\infty^* \cdot \Gamma_1(\mathfrak{n})) = K_\infty^* \cdot \Gamma_0(\mathfrak{n}) \cdot \langle \left(\begin{smallmatrix} 0 & 1 \\ \mathfrak{n} & 0 \end{smallmatrix}\right) \rangle.$$

Η παρακάτω ακολουθία

$$1 \longrightarrow \frac{K_\infty^* \cdot \Gamma_0(\mathfrak{n})}{K_\infty^* \cdot \Gamma_1(\mathfrak{n})} \longrightarrow \frac{\mathcal{N}_{K_\infty^*}(K_\infty^* \cdot \Gamma_1(\mathfrak{n}))}{K_\infty^* \cdot \Gamma_1(\mathfrak{n})} \longrightarrow \frac{K_\infty^* \cdot \Gamma_1(\mathfrak{n}) \cdot \langle \left(\begin{smallmatrix} 0 & 1 \\ \mathfrak{n} & 0 \end{smallmatrix}\right) \rangle}{K_\infty^* \cdot \Gamma_1(\mathfrak{n})} \longrightarrow 1$$

είναι ακριβής και split αφού

$$\mathbb{Z}/2\mathbb{Z} \sim K_\infty^* \cdot \Gamma_1(\mathfrak{n}) \langle \left(\begin{smallmatrix} 0 & 1 \\ \mathfrak{n} & 0 \end{smallmatrix}\right) \rangle / K_\infty^* \cdot \Gamma_1(\mathfrak{n}) \lhd \mathcal{N}_{K_\infty^*}(K_\infty^* \cdot \Gamma_1(\mathfrak{n}))/K_\infty^*, \Gamma_1(\mathfrak{n}).$$

(2) Η περίπτωση $q = 2$ και $\varphi(\mathfrak{n}) \geq 2$. Έστω $\mathfrak{n} = \prod_1^n \mathfrak{q}_i$ και g_{q_i} όπως στην πρόταση 5.2.1. Αν $n = 1$ τότε τα πράγματα έχουν όπως στην προηγούμενη περίπτωση. Έστω λοιπόν ότι $n \geq 2$. Από την πρόταση 5.2.1,

$$\mathcal{N}_{K_\infty}(K_\infty^* \cdot \Gamma_1(\mathfrak{n})) = K_\infty^* \cdot \Gamma_0(\mathfrak{n}) \cdot \langle g_{\mathfrak{q}_1}, \ldots, g_{\mathfrak{q}_n} \rangle$$

και

$$\frac{K_\infty^* \cdot \Gamma_0(\mathfrak{n}) \cdot \langle g_{\mathfrak{q}_1}, \ldots, g_{\mathfrak{q}_n} \rangle}{K_\infty^* \cdot \Gamma_0(\mathfrak{n})} \sim (\mathbb{Z}/2\mathbb{Z})^n.$$

Από την παρακάτω ακολουθία

$$1 \longrightarrow \frac{K_\infty^* \cdot \Gamma_0(\mathfrak{n})}{K_\infty^* \cdot \Gamma_1(\mathfrak{n})} \longrightarrow \frac{\mathcal{N}_{K_\infty}(\Gamma_1(\mathfrak{n}))}{K_\infty^* \cdot \Gamma_1(\mathfrak{n})} \longrightarrow \frac{\mathcal{N}_{K_\infty}(\Gamma_1(\mathfrak{n}))}{K_\infty^* \cdot \Gamma_0(\mathfrak{n})} \longrightarrow 1,$$

φτάνουμε στο επιθυμητό αποτέλεσμα.

$$1 \longrightarrow (A/\mathfrak{n}A)^*/\mathbf{F}_q^* \longrightarrow \frac{\mathcal{N}_{K_\infty}(\Gamma_1(\mathfrak{n}))}{K_\infty^* \cdot \Gamma_1(\mathfrak{n})} \longrightarrow (\mathbb{Z}/2\mathbb{Z})^n \longrightarrow 0.$$

(3) Η περίπτωση $q = 2$ και $\varphi(\mathfrak{n}) = 1$. Στην περίπτωση αυτή $(A/\mathfrak{n})^* = \mathbf{F}_q^*$. Έτσι, από την πρόταση (5.2.1)

$$\frac{\mathcal{N}_{K_\infty^*}(K_\infty^* \cdot \Gamma_1(\mathfrak{n}))}{K_\infty^* \cdot \Gamma_1(\mathfrak{n})} \sim (\frac{\mathbb{Z}}{2\mathbb{Z}})^n$$

όπου $n = 1$ ή 2. ❏

Βιβλιογραφία

[1] ABHYANKAR, S. S., AND KESKAR, P. Descent principle in modular galois theory. *Proc. Indian Acad. Sci 111*, 2 (2001), 139–149.

[2] ABHYANKAR, S. S., AND SUNDARAM, G. Galois groups of generalized iterates of generic vectorial polynomials. *Finite Fields Appl. 7*, 1 (2001), 92–109.

[3] ATKIN, A. O. L., AND LEHNER, J. Hecke operators on $\Gamma_0(m)$. *Math. Ann. 185* (1970), 134–160.

[4] BOURBAKI, N. *Commutative algebra. Chapters 1–7.* Springer-Verlag, Berlin, 1998. Translated from the French, Reprint of the 1989 English translation.

[5] DELIGNE, P., AND HUSEMOLLER, D. Survey of Drinfel′d modules. In *Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985).* Amer. Math. Soc., Providence, RI, 1987, pp. 25–91.

[6] DEMEYER F., I. E. *Separable algebras over commutative rings.* Springer-Verlag, Berlin, 1971. Lectures Notes in Mathematics, Vol. 181.

[7] DRINFEL′D, V. G. Elliptic modules. *Mat. Sb. (N.S.) 94(136)* (1974), 594–627, 656.

[8] GEKELER, E.-U. *Drinfeld-Moduln und modulare Formen über rationalen Funktionenkörpern.* Universität Bonn, Mathematisches Institut, Bonn, 1980. Dissertation, Rheinische Friedrich-Wilhelms-Universität, Bonn, 1979.

[9] GEKELER, E.-U. Modulare Einheiten fuer Funktionenkoerper. *J. Reine Angew. Math. 348* (1984), 94–115.

[10] GEKELER, E.-U. Invariants of some algebraic curves related to Drinfeld modular curves. *J. Number Theory 90*, 1 (2001), 166–183.

[11] GEKELER, E.-U., VAN DER PUT, M., REVERSAT, M., AND VAN GEEL, J., Eds. *Drinfeld modules, modular schemes and applications*, World Scientific Publishing Co. Inc. River Edge, NJ, 1997.

[12] GEKELER, E.-U., *Drinfeld modular Curves*, Lecture Notes in Mathematics, Vol. 1231, Springer-Verlag, Berlin, 1986.

[13] GOSS, D. *Basic structures of function field arithmetic.* Springer-Verlag, Berlin, 1996.

[14] GOSS, D., HAYES, D. R.,ROSEN, M. I., EDITORS. *The arithmetic of function fields,* Ohio State University Mathematical Research Institute Publications, 2, 1992. Proceedings of the workshop held at The Ohio State University, Columbus, Ohio, June 17–26, 1991.

[15] VAN DER HEIDEN, G., J. *Weil Pairing for Drinfeld Modules*, preprint, Groningen 2002.

[16] H., Voelklein. *Group as Galois groups, An introduction.* Cambridge Univ. Press, Cambridge, 1996. Cambridge Studies in Advanced Mathematics, Vol. 53.

[17] Hansen, T., and Mullen, G. L. Primitive polynomials over finite fields. *Math. Comp. 59*, 200 (1992), 639–643, S47–S50.

[18] Harbater, D. Abhyankar's conjecture on Galois groups over curves *Invent. Math. 117*, No.1, 1-25 (1994).

[19] Harris J., M. I. *Moduli of curves.* Springer-Verlag, Berlin, 1998. Graduate Texts in Mathematics, Vol. 187.

[20] Hartshorne, R. *Algebraic geometry.* Springer-Verlag, New York, 1977. Graduate Texts in Mathematics, No. 52.

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

[22] Jahnel, J. The brauer-severi variety associated with a central simple algebra: A survey. *Linear Algebraic Groups and Related Structures 52* (2000), 1–60. available in electronic form at http://www.mathematik.uni-bielefeld.de/LAG.

[23] Katz, Nicholas M. and Mazur, Barry. *Arithmetic moduli of elliptic curves.* Princeton University Press, 1985. Annals of Mathematics Studies, Vol. 108.

[24] Kim, C. H., and Koo, J. K. The normalizer of $\Gamma_1(N)$ in $PSL_2(\mathbb{R})$. *Commun. Algebra 28*, 11 (2000), 5303–5310.

[25] Matzat, B. H. *Konstruktive Galoistheorie.* Springer-Verlag, Berlin, 1987.

[26] Mumford, D., Fogarty, J., and Kirwan, F. *Geometric invariant theory*, third ed. Springer-Verlag, Berlin, 1994.

[27] Nagata, M. *Local rings.* Interscience Publishers a division of John Wiley & Sons New York-London, 1962.

[28] Saïdi, M. Moduli schemes of Drinfeld modules. In *Drinfeld modules, modular schemes and applications (Alden-Biesen, 1996).* World Sci. Publishing, River Edge, NJ, 1997, pp. 17–31.

[29] Schweizer, A. Modular automorphisms of the Drinfeld modular curves $X_0(\mathfrak{n})$. *Collect. Math. 48*, 1-2 (1997), 209–216.

[30] Shweizer, A. *Zur Arithmetik der Drinfeld'schen Modulkurven* $X_0(\mathfrak{n})$. PhD thesis, Universität Saarbrücken, 1996.

[31] van der Put, M., and Top, J. Algebraic compactification and modular interpretation. In *Drinfeld modules, modular schemes and applications (Alden-Biesen, 1996).* World Sci. Publishing, River Edge, NJ, 1997, pp. 141–166.