1 Επιφάνιες Riemann και αλγεβρικές καμπύλες

1.1 Επιφάνειες Riemann

Ορισμός 1.1 *Μιά επιφάνεια Riemann είναι ένας τοπολογικός χώρος Hausdorff X με τις παρακάτω ιδιότητες:*

- *Υπάρχει μιά οικογένεια (U_z, z) όπου U_z ανοιχτά υποσύνολα του X , z συναρτήσεις $z : U_z \longrightarrow \mathbb{C}$,τοπολογικοί ομοιομορφισμοί μέσα σε ανοιχτά του $\mathbb{C}$ και επιπλέον τα U_z καλύπτουν τον X δηλαδή:*
$$X = \bigcup U_z$$
- *Αν $U_{z_1} \cap U_{z_2} \neq \emptyset$, τότε η συνάρτηση $z_2 \circ z_1^{-1}$ από το $z_1(U_{z_1} \cap U_{z_2})$ στο $z_2(U_{z_1} \cap U_{z_2})$ είναι ολόμορφη.*
- *Η οικογένεια χαρτών (U_z, z) είναι μεγίστη ως προς αυτές τις ιδιότητες.*

Σε ότι ακολουθεί θα περιορίσουμε την μελέτη μας σε συμπαγείς συνεκτικές επιφάνειες Riemann.

Ορισμός 1.2 *Μιά συνάρηση $f : Y \longrightarrow X$ μεταξύ δυό επιφανειών Riemann X,Y θα λέγεται ολόμορφη (αντίστοιχα διαφορίσιμη) όταν έχει τις παρακάτω ιδιότητες: $\forall \;\; p \in Y$ και $f(p) \in X$ υπάρχουν περιοχές συντεταγμένων (U, z) του p και (V, w) του $f(p)$ τέτοιες ώστε $f(U) \subset V$ και η*
$$w \circ f \circ z^{-1} : z(U) \longrightarrow w(V)$$
να είναι ολόμορφη (αντίστοιχα πραγματικά διαφορίσιμη)συνάρτηση.

Ορισμός 1.3 *Μιά συνάρτηση της επιφάνειας Riemann X στο $\mathbb{C}$ θα λέγεται μερόμορφη όταν είναι ορισμένη και ολόμορφη στο συμπλήρωμα ένος διακριτού πεπερασμένου συνόλου B της X και επιπλέον αν $q \in B$ τότε $f(p) \to \infty$ καθώς $p \to q$. Τα σημεία της B ονομάζονται πόλοι της f.*

Το σύνολο των μερομόρφων συναρτήσεων επί της X , θα το συμβολίζουμε με $\mathcal{M}(X)$ αποτελεί σώμα με πράξεις την συνήθη πρόσθεση και πολλαπλασιασμό συναρτήσεων .
Παρατήρηση: Κάθε μερόμορφη συνάρτηση $f : X \longrightarrow \mathbb{C}$, μπορεί να επεκταθεί σε ολόμορφη συνάρτηση $\bar{f} : X \longrightarrow \mathbb{P}^1(\mathbb{C})$ θέτοντας $\bar{f}(q) = \infty \; \forall q \in B$.

Ορισμός 1.4 *Μιά 1-διαφορική μορφή ω στην επιφάνεια Riemann X είναι μιά συλλογή 1-μορφών $\omega_x dx + \omega_y dy$ σε κάθε χάρτη συντεταγμενών (U, z) (όπου $z = x + iy$) τέτοια ώστε σε επικαλυπτόμενους χάρτες να υπάρχει συμβατότητα: αν $U_{z_1} \cap U_{z_2} \neq \emptyset$ και $p = z_2 \circ z_1^{-1} = u + iv$ τότε:*
$$\omega_{x_1} dx_1 + \omega_{y_1} dy_1 = p^*(\omega_{x_2} dx_2 + \omega_{y_2} dy_2)$$
όπου ω_x και ω_y είναι συναρτήσεις $z(U) \longrightarrow \mathbb{C}$. Η συμβατότητα μπορεί να εκφραστεί λοιπόν και ως:
$$\omega_{x_1} = (\omega_{x_2} \circ p)\frac{\partial u}{\partial x_1} + (\omega_{y_2} \circ p)\frac{\partial v}{\partial x_1}$$

$$\omega_{y_1} = (\omega_{x_2} \circ p)\frac{\partial u}{\partial y_1} + (\omega_{y_2} \circ p)\frac{\partial v}{\partial y_1}$$

μέσα στο $z_1(U_{z_1} \cap U_{z_2})$.

Ορισμός 1.5 *Ολόμορφες (αντίστοιχα μερόμορφες)1-μορφές είναι οι διαφορικές 1-μορφές που σε κάθε χάρτη* $(U, z), z = x + iy$, ω_x *και* ω_y *είναι ολόμορφες (αντίστοιχα μερόμορφες) συναρτήσεις καί επιπλέον* $\omega_y = i\omega_x$. *Τοπικά κάθε ολόμορφη (αντίστοιχα μερόμορφη) 1-μορφή ισούται με* $f(z)dz$ *,όπου* f *είναι ολόμορφη (αντίστοιχα μερόμορφη) συνάρτηση. Αν η ολόμορφη 1-μορφή παρίσταται ως:*$f(z_1)dz_1$, $g(z_2)dz_2$ *σε δυό διαφορετικούς χάρτες τότε η συμβατότητα εκφράζεται με την παρακάτω απλή σχέση:* $g(z_2) = f(z_1)dz_1/dz_2$ *στην επικάλυψη των δυό χαρτών.*

Ορισμός 1.6 *Αν* $\gamma(t)$ *κατά τμήματα διαφορίσιμη καμπύλη επάνω στην επιφάνεια Riemann* X *και* $\gamma_i(t)$ *τμήματα της παραπάνω καμπύλης που βρίσκονται εξ' ολοκλήρου σε ένα χάρτη* (U_i, z_i), *ορίζουμε το ολοκλήρωμά της:*

$$\int_\gamma \omega := \sum_i \int_{\gamma_i} \omega := \sum_i \int_{z_i(\gamma_i)} (\omega_x dx + \omega_y dy).$$

Το ολοκλήρωμα είναι καλά ορισμένο λόγω της συμβατότητας της διαφορικής μορφής σε διαφορετικούς χάρτες.

Ορισμός 1.7 *(Ολοκληρωτικό υπόλοιπο.) Εστω* ω *μιά μερόμορφη 1-μορφή και* $P \in X$. *Θεωρούμε μιά καμπύλη* γ *με δείκτη στροφής 1 ,που περιέχεται εξ ολοκλήρου μέσα σε μιά περιοχή συντεταγμένων του* P. *Ορίζουμε*

$$res_P := \frac{1}{2\pi i}\int_\gamma \omega$$

το ολοκληρωτικό υπόλοιπο της μερόμορφης 1-μορφής στο σημείο P.

Θεώρημα 1.8 *Αν* X *συμπαγής επιφάνεια Riemann και* ω *μερόμορφη 1-μορφή αυτής, τότε το άθροισμα των ολοκληρωτικών της υπολοίπων είναι* 0.

<u>Απόδειξη:</u> Εστω $P_1, ..., P_n$ οι πόλοι της ω και $(U_1, z_1), ..., (U_n, z_n)$ χάρτες συντεταγμένων ξένοι ανα δύο, με $P_i \in U_i$. Επιπλέον υποθέτουμε ότι $z_i(P_i) = 0 \in \mathbb{C}$. Εστω S_i^* ανοιχτός δίσκος έντος του $z_i(U_i)$ με κέντρο το 0 , R_i ομόκεντρος κύκλος με τον S_i^* έντος του $z_i(U_i)$. Υπάρχουν συνάρτησεις f_i^* κλάσεως C^1 με $f_i^* = 1$ στο S_i^* και 0 εκτός του R_i. Θέτουμε $S_i := z_i^{-1}(S_i^*)$ και $f_i := f_i^* \circ z_i$. Εστω S η ένωση των S_i και $f = \sum f_i$. Αρκεί να δείξουμε ότι $\int_{\partial S} \omega = 0$. Η $(1-f)\omega$ είναι συνεχώς διαφορίσιμη 1-μορφή με συμπαγή φορέα $M - S$. Καλύπτουμε τον συμπαγή φορέα με πεπερασμένες το πλήθος περιοχές συντεταγμένων και από το θεώρημα του Green στο επίπεδο έχουμε:

$$\int\int_{M-S} d[(1-f)\omega] = \int_{\partial S} (1-f)\omega = 0$$

Ομως η ω είναι ολόμορφη στο $M - S$ συνεπώς $d\omega = 0$ στο $M - S$. Συνεπώς ο παραπάνω τύπος γράφεται:

$$\int\int_{M-S} d(f\omega) = 0$$

Από την άλλη όμως, λόγω θεωρήματος Green και της πρώτης σχέσης, έχουμε:

$$2\pi i \sum_k res_{P_k}\omega = \int_{\partial S} \omega = \int_{\partial S} f\omega = \iint_{M-S} d(f\omega) = 0$$

Ορισμός 1.9 *Ενα υποσύνολο V του K^n θα λέγεται αλγεβρικό σύνολο όταν ορίζεται ως τόπος μηδενισμού ενός πεπερασμένου συνόλου πολυωνύμων. Σε κάθε αλγεβρικό σύνολο V αντιστοιχεί ένα ιδεώδες $I(V)$ του $\mathrm{K}[x_1, ..., x_n]$ που ορίζεται σαν το σύνολο των πολυωνύμων που μηδενίζονται σε κάθε σημείο του V. Αντιστρόφως σε κάθε ιδεώδες I του $K[x_1, ..., x_n]$ αντιστοιχεί ένα αλγεβρικό σύνολο $V(I)$,λόγω του θεωρήματος βάσης του Hilbert [A-M]. Ανάγωγη αλγεβρική πολλαπλότητα είναι κάθε αλγεβρικό σύνολο V του οποίου το ιδεώδες $I(V)$ είναι πρώτο. Μπορούμε λοιπόν σε αυτή την περίπτωση να ορίσουμε σαν δακτύλιο συντεταγμένων την ακεραία περιοχή:*

$$K[V] := \frac{K[x_1, ..., x_n]}{I(V)}.$$

Τέλος ορίζουμε σαν σώμα ρητών συναρτήσεων $K(V)$ της V το σώμα πηλίκων του $K[V]$. Διάσταση του V είναι εξ ορισμού ο βαθμός υπερβατικότητας της $K(V)$ υπέρ το K.

Γιά να έχουμε μιά ικανοποιητική και ομοιόμορφη θεωρία τομών στην γεωμετρία, είναι αναγκαίο να εγκαταλείψουμε τον αφινικό χώρο και να ορίσουμε τις παραπάνω έννοιες προβολικά:

Ορισμός 1.10 *Ο προβολικός χώρος διάστασης n, $\mathbb{P}^n(K)$ είναι το σύνολο πηλίκο, των ισοδυνάμων $(n+1)-$άδων με στοιχεία από το K, όπου η σχέση ισοδυναμίας δίνεται από τον τύπο:*

$$(x_0, x_1, ...x_n) \sim (y_0, y_1, ..., y_n) \Leftrightarrow \exists \lambda \in K^* : x_i = \lambda y_i.$$

Ορισμός 1.11 *Ενα πολυώνυμο $f \in \bar{K}[X] = \bar{K}[x_0, ..., x_n]$ είναι ομογενές βαθμού d αν:*

$$f(\lambda x_0, ..., \lambda x_n) = \lambda^d f(x_0, ..., x_n).$$

Ενα ιδεώδες είναι ομογενές αν γεννιέται από ομογενή πολυώνυμα. Αν I είναι ένα ομογενές πολυώνυμο ορίζουμε τον τόπο μηδενισμού:

$$V_I := \{P \in \mathbb{P}^n : f(P) = 0, \ \forall \ \ f \in I, \ \ f \text{ ομογενές}\}.$$

Ορισμός 1.12 *Ονομάζουμε προβολική αλγεβρική πολλαπλότητα κάθε αλγεβρικό σύνολο $V(I)$, όπου I πρώτο και ομογενές ιδεώδες του $\bar{K}[X]$. Αντιστρόφως σε κάθε προβολικό αλγεβρικό σύνολο αντιστοιχίζουμε το πρώτο ιδεώδες του $\bar{K}[X]$ που γεννάται από:*

$$\{f \in \bar{K}[X] : f \text{ ομογενές και } f(P) = 0 \, \forall P \in V\}.$$

Μεγάλο ενδιαφέρον γιά την θεωρία των αριθμών έχουν οι παραπάνω έννοιες γιά σώματα όχι αλγεβρικά κλειστά.

Ορισμός 1.13 *Αν το K δεν είναι αλγεβρικά κλειστό τότε η αλγεβρική πολλαπλότητα ορίζεται υπέρ το K ανν το ιδεώδες $I(V)$ γενιέται από ομογενή πολυώνυμα του $K[X]$. Το σύνολο των K σταθερών σημείων του V είναι το σύνολο:*

$$V(K) := V \bigcap \mathbb{P}^n(K) = \{P \in V : P^\sigma = P \;\forall\; \sigma \in Gal(\bar{K}/K)\}.$$

(Γιά ομάδες του Galois απείρων επεκτάσεων βλέπε παράρτημα.)

Ορισμός 1.14 *Ορίζουμε το σώμα συναρτήσεων $K(V)$ της προβολικής πολλαπλότητας V ώς το σώμα ρητών συναρτήσεων της μορφής: $F(x) = f(x)/g(x)$ οπού τα f, g ομογενή πολυώνυμα ιδίου βαθμού, το πολυώνυμο $g \notin I(V)$. Δυό πηλίκα $f/g, f'/g'$ ορίζουν την ίδια συνάρτηση ανν $fg' - f'g \in I(V)$.*

Ορισμός 1.15 *Εστω V_1, V_2 δύο προβολικές πολλαπλότητες. Μία ρητή συνάρτηση από την V_1 στην V_2 είναι κάθε συνάρτηση της μορφής:*

$$\Phi : V_1 \longrightarrow V_2$$

με $\Phi = [f_0, ..., f_n]$, όπου $f_i \in K(V)$ και με την επιπλέον ιδιότητα: γιά κάθε σημείο $P \in V_1$, όπου όλες οι f_i ορίζονται, απαιτούμε το $\Phi(P) = [f_0(P), ..., f_n(P)] \in V_2$. Επιπλέον αν $\exists\; g \in K(V_1)$, τέτοια ώστε gf_i ορισμένη στο P γιά κάθε i, και υπάρχει i τέτοιο ώστε $gf_i(P) \neq 0$ τότε ο Φ θα λέγεται κανονικός στο σημείο P. Ρητή συνάρτηση μεταξύ αλγεβρικών πολλαπλοτήτων που επιπλέον είναι κανονική σε κάθε σημείο θα λέγεται μορφισμός.

Στα επόμενα θα ασχοληθούμε με καμπύλες δηλαδή με αλγεβρικές πολλαπλότητες διάστασης 1. Ειδικότερα θα ασχοληθούμε με επίπεδες αλγεβρικές καμπύλες δηλαδή μονοδιάσταιες αλγεβρικές καμπύλες σε δυό συντεταγμένες x_1, x_2. Ενα από τα κύρια αποτελέσματα αυτής της παραγράφου θα είναι η ταύτιση αλγεβρικών καμπύλων υπέρ το $\mathbb{C}$ και επιφανειών Riemann.

Θεώρημα 1.16 *Γιά κάθε ανάγωγη αλγεβρική καμπύλη $\Sigma \subset \mathbb{P}^2\mathbb{C}$ υπάρχει μιά συμπαγής επιφάνεια Riemann $\tilde{\Sigma}$ και μιά ολόμορφη απεικόνιση*

$$\sigma : \tilde{\Sigma} \longrightarrow \mathbb{P}^2\mathbb{C}$$

τέτοια ώστε $\sigma(\tilde{\Sigma}) = \Sigma$, η οποία είναι 1-1 στην αντίστροφη εικόνα του συνόλου των ομαλών σημείων της Σ. Αυτή η κατασκευή λέγεται κανονικοποίηση της αλγεβρικής καμπύλης Σ. Αντιστρόφως κάθε επιφάνεια Riemann X δίνεται ως κανονικοποίηση κάποιας επίπεδης αλγεβρικής καμπύλης.

Απόδειξη: (σκιαγράφιση)
Οσον αφορά το πρώτο μέρος του θεωρήματος παρατηρούμε ότι η απόδειξη είναι εύκολη αν η αλγεβρική καμπύλη δεν έχει ιδιομορφίες, λόγω του θεωρήματος των πεπλεγμένων συναρτήσεων. Αλλιώς χρειαζόμαστε στοιχεία από την θεωρία επίλυσης ιδιομορφιών. Οσον αφορά την απόδειξη του δευτέρου μέρους θα χρειαστεί να αναφέρουμε μερικά στοιχεία από την θεωρία των καλυμμάτων και την σχέση τους με τα σώματα μερομόρφων συναρτήσεων.

Ορισμός 1.17 *Ενα μη διακλαδιζόμενο κάλυμμα ενός τοπολογικού χώρου X είναι ένας τοπολογικός χώρος Y και μιά συνάρτηση $p : Y \longrightarrow X$ γιά την οποιά ισχύει: Κάθε σημείο $x \in X$ έχει μιά ανοιχτή περιοχή U τέτοια ώστε η αντίστροφη εικόνα*

$$p^{-1}(U) = \bigcup_{i \in J} V_j$$

είναι ένωση ξένων ανά δυό ανοιχτών περιοχών του Y και $p|_{V_j} : V_j \longrightarrow U$ είναι τοπολογικός ομοιομορφισμός.

Ορισμός 1.18 *Ενα διακλαδιζόμενο κάλυμμα ενός τοπολογικού χώρου X είναι ένας τοπολογικός χώρος Y και μιά συνάρτηση $p : Y \longrightarrow X$ συνεχής ,ανοιχτή και διακριτή (δηλαδή η αντίστροφη εικόνα κάθε σημείου $x \in X$ είναι διακριτό σύνολο). Σημεία διακλάδωσης είναι το σύνολο των $y \in Y$ τέτοια ώστε να μην υπάρχει ανοιχτή περιοχή τους V έτσι ώστε η $p|_V$ να είναι 1-1.*

Πρόταση 1.19 *Οι ολόμορφες απεικονίσεις μεταξύ συμπαγών επιφανειών Riemann είναι διακριτές, συνεχείς και ανοιχτές. Τέλος τα σημεία διακλάδωσης είναι διακριτά καί το πλήθος (μετρώντας την πολλαπλότητα) των αντιστρόφων εικόνων είναι σταθερό.*

Το πλήθος των αντιστρόφων εικόνων θα το ονομάζουμε πλήθος των φύλλων του καλύμματος.

Είναι ιδιαίτερα ενδιαφέρουσα η αντιστοιχία μεταξύ ολόμορφων καλυμμάτων επιφανειών Riemann και των αντίστοιχων σωμάτων μερόμορφων συναρτήσεων. Συγκεκριμένα ισχύει το παρακάτω :

Θεώρημα 1.20 *Εστω X,Y επιφάνειες Riemann και έστω $\pi : Y \longrightarrow X$ μιά ολόμορφη πεπερασμένων φύλλων κάλυψη. Αν $f \in \mathcal{M}(\mathrm{Y})$ και $c_1, ..., c_n \in \mathcal{M}(X)$ οι στοιχειώδεις συμμετρικές συναρτήσεις του f, δηλαδή τα $c_i(x)$ είναι οι συντελεστές του πολυωνύμου $\prod_{y_i \in \pi^{-1}(x)}(T - f(y_i))$, τότε το f ικανοποιεί την παρακάτω αλγεβρική σχέση:*

$$f^n + (\pi^* c_1) f^{n-1} + ... + (\pi^* c_{n-1}) f + (\pi^* c_n) = 0.$$

Ο μονομορφισμός $\pi^* : \mathcal{M}(X) \longrightarrow \mathcal{M}(Y)$ είναι μιά αλγεβρική επέκταση βαθμού $\leq n$. Αντιστρόφως σε κάθε αλγεβρική επέκταση του σώματος των μερόμορφων συναρτήσεων του $\mathcal{M}(\mathrm{X})$ αντιστοιχεί μιά επιφάνεια Riemann Y κάλυμμα της X.

Παρατηρούμε ότι το παραπάνω θεώρημα δίνει κατευθείαν τήν ιδέα γιά την ταύτιση επιφανειών Riemann και αλγεβρικών καμπύλων.

Θεώρημα 1.21 *Αν η X είναι μία συμπαγής συνεκτική επιφάνεια Riemann και $\mathcal{M}(\mathrm{X})$ το σώμα μερόμορφων συναρτήσεων της, τότε ο βαθμός υπερβατικότητας του $\mathcal{M}(\mathrm{X})$ υπέρ του $\mathbb{C}$ είναι 1.*

Απόδειξη: Εστω z μιά μερόμορφη μη-σταθερά συνάρτηση στην X. Τότε η $z : \mathrm{X} \longrightarrow \mathbb{P}^1$ είναι ολόμορφη και παίρνει κάθε τιμή το ίδιο συχνά λόγω του θεωρήματος 1.8, έστω n φορές. Εστω τώρα $f \in \mathcal{M}(\mathrm{X})$. Θα δείξουμε ότι υπάρχει αλγεβρική σχέση μεταξύ των f, z. Θεωρούμε συνάρτηση f_0 τέτοια ώστε: $deg[\mathbb{C}(z, f_0) : \mathbb{C}(z)]$ να είναι μέγιστος. Συνεπώς γιά όλες τις $f \in \mathcal{M}(\mathrm{X})$ ισχύει :

$$[\mathbb{C}(z, f, f_0) : \mathbb{C}(z)] = [\mathbb{C}(z, f, f_0) : \mathbb{C}(z, f_0)][\mathbb{C}(z, f_0) : \mathbb{C}(z)].$$

Επειδή $\mathbb{C}(z, f, f_0)$ διαχωρίσιμη επέκταση υπέρ του $\mathbb{C}(z)$ έπεται ότι υπάρχει $g \in \mathcal{M}(\mathrm{X})$ τέτοιο ώστε $\mathbb{C}(z, f, f_0) = \mathbb{C}(z, g)$ και συγκρίνοντας τους βαθμούς βλέπουμε ότι $\mathbb{C}(z, f_0) = \mathcal{M}(\mathrm{X})$.

Επομένως $\mathcal{M}(\mathrm{X}) = \mathbb{C}(z, f)$ γιά δυό μερόμορφες συναρτήσεις f, z. Επειδή ο βαθμός υπερβατικότητας του $\mathcal{M}(X)$ ύπερ το $\mathbb{C}(z)$ είναι 1 έπεται ότι υπάρχει πολυώνυμο $P \in \mathbb{C}[X, Y]$ τέτοιο ώστε $P(z, f) = 0$ συνεπώς έχουμε ένα χάρτη $U \longrightarrow \Sigma$ όπου U είναι το ανοιχτό υποσύνολο του X στο οποίο οι z, f δεν έχουν πόλους καί Σ είναι αφινική (ενδεχομένως ιδιόμορφη) καμπύλη στο z, f επίπεδο που δίνεται από τον τόπο μηδενισμού του πολυωνύμου $P[X, Y] = 0$. Η απεικόνιση αυτη σιέλνει ένα σημείο Q στο $(z(Q), f(Q))$.

Παρατήρηση: Εχουμε λοιπόν δυό ορισμούς γιά το ίδιο μαθηματικό αντικείμενο. Το πλεονέκτημα της επιφάνειας Riemann είναι η τοπική μελέτη που μας επιτρέπει την χρήση μεθόδων της ανάλυσης, ενώ το πλεονέκτημα των αλγεβρικών καμπύλων είναι η καθολική θέαση του προβλήματος και επιπλέον η δυναιότητα να δουλέψουμε πάνω από οποιοδήποτε σώμα.

Οι επιφάνειες Riemann-αλγεβρικές καμπύλες είναι προσαναιολίσιμες. Πράγμαιι αν τις θεώρησουμε ως σιαθμικά σύνολα πολυωνύμων τότε η ύπαρξη κάθετου ανάδελτα μας εξασφαλίζει τον προσαναιολισμό ενώ αν τις θεώρησουμε ως επιφάνειες Riemann, οι συνθήκες Cauchy-Riemann εξασφαλίζουν το ότι η ορίζουσα αλλαγής χάρτη είναι θετική. Από το γνωστό θεώρημα ταξινόμισης δυδιάσταιων πραγμαιικών πολλαπλοτήτων [Mas] έχουμε ότι είναι συνεκτικό άθροισμα g το πλήθος τόρων. Τον αριθμό αυτό g θα τον ονομάζουμε γένος της επιφάνειας.

Ορισμός 1.22 *(Πόλοι και ρίζες μερομόρφων συναρτήσεων.) Ρίζα μιάς συνάρτησης $f : X \longrightarrow \mathbb{P}^1$ λέγεται κάθε αντίστροφη εικόνα του $0 \in \mathbb{P}^1$. Τάξη της ρίζας λέγεται ο βαθμός διακλάδωσης της συνάρτησης στην συγκεκριμένη αντίστροφη εικόνα. Αντιστρόφως πόλο και τάξη του πόλου καλούμε τις αντίστροφες εικόνες του ∞ και τον βαθμό διακλάδωσης σε εκείνο το σημείο.*

Οι παραπάνω ορισμοί είναι ισοδύναμοι με τους γνωστούς από την θεωρία μιγαδικών συναρτήσεων αν θεώρησουμε την συμπεριφορά της σειράς Laurent της συνάρτησης γραμμένης σε τοπικό σύστημα συνιεταγμένων. Βασικό πλεονέκτημα της μιγαδικής θεώρησης είναι η τοπική ανάλυση κάθε συνάρτησης σε δυναμοσειρά. Μπορούμε να κάνουμε μία παρόμοια κατασκευή σε οποιοδήποτε σώμα. Πράγμαιι αν C είναι μιά καμπύλη και P ένα ομαλό σημείο τότε το M_P/M_P^2 έχει διάσταση 1 υπέρ το $\bar{K} = \bar{K}[C]_P/M_P$, οπότε [A-M] ο $\bar{K}[C]_P$ είναι διακριτός δακτύλιος εκτιμήσης.

Ορισμός 1.23 *Εστω C καμπύλη και $P \in C$, μη ιδιόμορφο σημείο. Η κανονικοποιημένη εκτίμηση του $\bar{K}[C]_P$ δίνεται από:*

$$ord_P : \bar{K}[C]_P \longrightarrow \{0, 1, 2, ...\} \bigcup \{\infty\}$$

$$ord_P(f) = max\{d \in \mathbb{Z} : f \in M_P^d\}.$$

Η παραπάνω εκτίμηση, επεκτείνεται σε όλο το $\bar{K}(C)$ απλά θέτοντας $ord_P(f/g) := ord_P(f) - ord_P(g)$. Μιά γενικευμένη τοπική συντεταγμένη της C στο σημείο P είναι μία συνάρτηση $t \in \bar{K}(C)$ με $ord_P(t) = 1$ δηλαδή ένας γεννήτορας του ιδεώδους M_P. Η συνάρτηση f έχει ρίζα (αντίσοιχα πόλο) στο P ανν $ord_P(f) > 0$ (αντίστοιχα $ord_P(f) < 0$).

Θεώρημα 1.24 *Εστω K ένα τέλειο σώμα, εστω $X(K)$ μία καμπύλη και έστω $t \in K(X)$ τοπική συντεταγμένη στο μη ιδιόμορφο σημείο $P \in X$. Τότε το $K(X)$ είναι μία πεπερασμένη διαχωρίσιμη επέκταση του $K(t)$.*

<u>Απόδειξη:</u> Το $K(X)$ είναι σαφώς μία πεπερασμένη επέκταση του $K(t)$ αφού είναι πεπερασμένα παραγώμενη πάνω από το K, έχει βαθμό υπερβατικότητας 1 υπέρ το K και t υπερβατικό στοιχείο $t \notin K$. Εστω $x \in K(X)$. Θα δείξουμε ότι είναι διαχωρίσιμο υπέρ το $K(t)$. Σε κάθε περίπτωση το x είναι αλγεβρικό, συνεπώς ικανοποιεί μιά πολυωνυμική σχέση της μορφής:

$$\sum a_{ij} t^i x^j = 0, \text{ και έστω } \Phi(T,X) = \sum a_{ij} T^i X^j = 0 \in K[X,T].$$

Μπορούμε επιπρόσθετα να υποθέσουμε ότι το Φ είναι ελαχίστου βαθμού ως προς X. Εστω $p = char(K)$, αν η χαρακτηριστική ήταν μηδέν δεν θα είχαμε τίποτα να αποδείξουμε. Αν το Φ περιέχει ένα μη μηδενικό όρο $a_{ij} T^i X^j$ με $j \not\equiv 0 mod\, p$ τότε $\partial \Phi(X,T)/\partial X$ δεν είναι ταυτοτικά 0 και το x είναι διαχωρίσιμο υπέρ το $K(t)$. Ας υποθέσουμε λοιπόν ότι

$$\Phi(T,X) = \Psi(T,X^p).$$

Παρατηρούμε ότι αν $F(T,X) \in K[X,T]$ είναι κάποιο πολυώνυμο τότε το $F(T^p,X^p)$ είναι μιά p-δύναμη. Αυτό είναι αληθές γιατί κάθε στοιχείο του K είναι μιά p-δύναμη αφού αν $a \in K$ και $a^{1/p} \notin K$ τότε τότε το ανάγωγο πολυώνυμό του είναι:

$$x^p - a = x^p - (a^{1/p})^p = (x - a^{1/p})^p$$

το οποίο φυσικά δεν είναι διαχωρίσιμο. Αν $F(T,X) = \sum a_{ij} T^i X^j$ τότε θέτοντας $b_{ij}^p = a_{ij}$, έχουμε ότι

$$F(T^p,X^p) = \left(\sum b_{ij} T^i X^j\right)^p.$$

Συνεπώς έχουμε:

$$\Phi(T,X) = \Psi(T,X^p) = \sum_{k=0}^{p-1} \left(\sum_{i,j} b_{ijk} T^{ip} X^{jp}\right) T^k = \sum_{k=0}^{p-1} \Phi_k(T,X)^p T^k$$

από την άλλη έχουμε

$$ord_P(\Phi_k(t,x)^p t^k) = p\, ord_P \Phi_k(t,x) + k\, ord_P t \equiv k mod\, p.$$

Το $\Phi(t,x)$ πρέπει να είναι 0 και από την παραπάνω σχέση βλέπουμε ότι κάθε προσθεταίος στο άθροισμα έχει διαφορετική τάξη στο P, όλοι τους λοιπόν μηδενίζονται,

$$\Phi_0(t,x) = \Phi_1(t,x) = \Phi_2(t,x) = \ldots.. = \Phi_{p-1}(t,x) = 0$$

όμως κάποιος από τους $\Phi_k(T,X)$ περιέχει το X και είναι μικροτέρου βαθμού από το $\Phi(T,X)$, άτοπο.

1.2 Θεώρημα των Riemann-Roch

Στην παρακάτω ανάλυση θα ορίσουμε όλες τις έννοιες στο σώμα $\mathbb{C}$ παρόλο που τα πάντα δουλεύουν παρόμοια σε κάθε αλγεβρικά κλειστό σώμα.

Ορισμός 1.25 *Θα ονομάζουμε ομάδα διαιρετών (divisors) της επιφάνειας Riemann X την ελεύθερη αβελιανή ομάδα παραγόμενη από τα σημεία $P \in X$ δηλαδή την ομάδα των τυπικών αθροισμάτων της μορφής:*

$$D = \sum_{P \in X} n_P P$$

όπου τα $n_P \in \mathbb{Z}$ και όλα εκτός από πεπερασμένο πλήθος είναι μηδέν. Την ομάδα αυτή θα την συμβολίζουμε με $Div(X)$. Βαθμός ενός διαιρέτη D είναι $degD := \sum n_p$ και εύκολα διαπιστώνουμε ότι $deg : Div(X) \longrightarrow \mathbb{Z}$ είναι μορφισμός προσθετικών ομάδων. Ο πυρήνας της απεικόνισης deg είναι υποομάδα της $Div(X)$ και θα την συμβολίζουμε με $Div^0(X)$. Σε κάθε μερόμορφη συνάρτηση $f \in \mathcal{M}(X)$ αντιστοιχίζουμε τον διαιρέτη $div(f) = \sum ord_P(f)P$. Παρατηρούμε ότι η συνάρτηση div είναι μορφισμός αβελιανών ομάδων $div : \mathcal{M}(X) \longrightarrow Div(X)$. Τέλος ορίζουμε την ομάδα του Picard

$$Pic(X) := Div(X)/div(\mathcal{M}(X))$$

.

Πρόταση 1.26 *Σε συμπαγείς επιφάνειες Riemann ισχύουν τα παρακάτω:*

- $div(f) = 0 \Longleftrightarrow f \in \mathbb{C}^*$
- $deg(div(f)) = 0$

Απόδειξη:

- Αν $div(f) = 0$ τότε η συνάρτηση f δεν έχει πόλους άρα είναι φραγμένη στο συμπαγές συνεκτικό σύνολο X και συνεπώς σύμφωνα με το θεώρημα του Liouville είναι σταθερή, δηλαδή $f \in \mathbb{C}^*$.
- Εύκολα διαπιστώνουμε ότι το ολοκληρωτικό υπόλοιπο της διαφορικής μορφής $f'(z)/f(z)dz$ ταυτίζεται με τον αριθμό ριζών (λαμβάνω υπόψιν και τις πολλαπλότητες) αν αφαιρέσουμε τον αριθμό των πόλων συνεπώς, σύμφωνα με το θεωρήμα 1.8 εφαρμοζόμενο για την $f(z)'/f(z)dz$ μας δίνει τελικά το ζητούμενο.

Λόγω της παραπάνω πρότασης μπορούμε να ορίσουμε και την ομάδα:

$$Pic^0(X) := Div^0(X)/div(\mathcal{M}(X))$$

και να συνοψίσουμε τα παραπάνω στην ακριβή ακολουθία:

$$1 \longrightarrow \mathbb{C}^* \longrightarrow \mathcal{M}(X)^* \longrightarrow Div^0X \longrightarrow Pic^0X \longrightarrow 0.$$

Ο αριθμοθεωρητικός θα παρατηρήσει σίγουρα την αναλογία μεταξύ της παραπάνω ακριβούς ακολουθίας και της ακριβούς ακολουθίας της ομάδας κλάσεων ενός αλγεβρικού σώματος αριθμών:

$$1 \longrightarrow \text{μονάδες} \longrightarrow K^* \longrightarrow \begin{pmatrix} \text{κλασματικά} \\ \text{ιδεώδη} \end{pmatrix} \longrightarrow \begin{pmatrix} \text{ομάδα} \\ \text{κλάσεων} \end{pmatrix} \longrightarrow 1$$

Ορισμός 1.27 *Αν* $D = \sum n_P P, D' = \sum n'_P P$ *δυό διαιρέτες της επιφάνειας Riemann* X *τότε ορίζουμε* $D \geq D'$ *ανν* $n_p \geq n'_p \quad (\forall P \in X)$

Εστω $D \in Div(X)$ *ορίζουμε το σύνολο των συναρτήσεων:*

$$\mathcal{L}(D) := \{f \in \mathcal{M}(X) : div(f) \geq -D\} \cup \{0\}$$

Αποδυκνείεται ότι $\mathcal{L}(D)$ είναι πεπερασμένης διάστασης $\mathbb{C}$-διανυσματικός χώρος και θα συμβολίζουμε με $\ell(D) = dim_{\mathbb{C}}\mathcal{L}(D)$

Πρόταση 1.28 *Εστω* $D \in Div(X)$

- *Αν* $deg(D) < 0$ *τότε* $\mathcal{L}(D) = \{0\}$ *και* $\ell(D) = 0$
- *Αν* D, D' *διαιρέτες που διαφέρουν κατά κύριο, τότε* $\mathcal{L}(D) = \mathcal{L}(D')$ *και* $\ell(D) = \ell(D')$.

Απόδειξη:

- Εσιω $f \in \mathcal{L}(D)$ τότε $0 = deg\,(div(f)) \geq deg(-D) = -deg(D) > 0$.
- Αν $D = D' + div(g)$ τότε η συνάτηση

$$\mathcal{L}(D) \longrightarrow \mathcal{L}(D')$$

$$f \longmapsto fg$$

είναι ισομορφισμός $\mathbb{C}$-διανυσματικών χώρων.

Εσιω τώρα $K_X \in Div(X)$ διαιρέτης στό X, ορισμένος ως

$$K_X = div(\omega), \text{ γιά κάποια μορφή } \omega.$$

Τότε κάθε συνάρτηση $f \in \mathcal{L}(K_X)$ έχει την ιδιότητα :

$$div(f) \geq -div(\omega) \quad \text{άρα} \quad div(f\omega) \geq 0$$

και επομένως η $f\omega$ είναι ολόμορφη.

Αντισιρόφως αν $f\omega$ είναι ολόμορφη τότε $f \in \mathcal{L}(K_X)$. Αφού κάθε διαφορική μορφή είναι της μορφής $f\omega$ γιά κάποιο $f \in \mathcal{M}(X)$ έχουμε τον παρακάτω ισομορφισμό διανυσματικών χώρων:

$$\mathcal{L}(K_X) \simeq \omega \in \Omega_X : \omega \quad \text{ολόμορφο}$$

Η διάσταση $\ell(K_X)$ ισούται με το γένος g της επιφάνειας X. Στην συνέχεια θα αναφέρουμε μερικά θεμελιώδη θεωρήματα της θεωρίας των αλγεβρικών καμπύλων. Γιά μία απόδειξη γιά την $\mathbb{C}$-περίπτωση [Fo,κεφ 2], ενώ γιά καμπύλη ορισμένη σε τυχαίο σώμα [Ha,κεφ. IV]

Θεώρημα 1.29 *(Riemann Roch): Εστω X λεία καμπύλη και K_X κανονικός διαιρέτης της X. Υπάρχει ένας ακέραιος $g \geq 0$, το γένος της καμπύλης X, τέτοιος ώστε γιά κάθε διαιρέτη $D \in Div(X)$ νά έχουμε:*

$$\ell(D) - \ell(K_{\mathrm{X}} - D) = degD - g + 1$$

Πόρισμα 1.30

- $\ell(K_X) = g$
- $deg(K_X) = 2g - 2$
- *αν* $degD > 2g - 2$ *τότε* $\ell(D) = deg(D) - g + 1$

Θεώρημα 1.31 *(Hurwitz) Εστω $F : X_1 \longrightarrow X_2$ μιά μη σταθερή ολόμορφη συνάρτηση μεταξύ επιφανειών Riemann. Εστω $g(X_i)$ το γένος της X_i. Εστω z τοπική συντεταγμένη του $P \in X_1$ και w μιά τοπική συντεταγμένη του $F(P)$ στην X_2. Αν υπάρχει $k \in \mathbb{Z}$ τέτοιο ώστε $w = z^k$, το k θα το ονομάζουμε δείκτη διακλάδωσης της F στο P. Αν $k \geq 1$ τότε η F διακλαδίζεται στο P και θα συμβολίζουμε το k με $v_F(P)$. Ισχύει ο τύπος των Riemann-Hurwitz:*

$$2 - 2g(X_1) = d\left(2 - 2g(X_2)\right) - \sum_{P \in X_1} \left(v_F(P) - 1\right)$$

όπου d ο αριθμός φύλλων του καλλύματος.

Εστω X συμπαγής επιφάνεια Riemann. Σταθεροποιούμε ένα σημείο O και έστω $\phi_1, ..., \phi_g$ μια βάση του μιγαδικού διανυσματικού χώρου των ολόμορφων διαφορικών μορφών στο X. Θεωρούμε την καλά ορισμένη υποομάδα του $\mathbb{C}^g$

$$Per(\phi_1 ... \phi_g) = \left(\int_\alpha \phi_1 ... \int_\alpha \phi_g \right)$$

όπου το α διατρέχει την θεμελιώδη ομάδα $\pi_1(X)$ ή ισοδύναμα την πρώτη ομάδα ομολογίας $H_1(X, \mathbb{Z})$. Εύκολα βλέπουμε ότι πρόκειται γιά μιά διακριτή υποομάδα του $\mathbb{C}^g$ και ορίζουμε την Ιακωβιανή πολλαπλότητα:

$$Jac(X) := \frac{\mathbb{C}^g}{Per(\phi_1, ..., \phi_g)}$$

η οποία δίνει την αντίστροφη απάντηση για το πότε ένας διαιρέτης βαθμού μηδέν είναι κύριος:

Θεώρημα 1.32 *(Abel Jacobi)*

$$Pic^0(X) = Jac(X)$$

Απόδειξη: [Fo]

2 Ελλειπτικές καμπύλες

2.1 Ελλειπτικές Καμπύλες

Ορισμός 2.1 *Ελλειπτική καμπύλη είναι κάθε αλγεβρική προβολική καμπύλη E, γένους 1 με ένα σταθερό προκαθορισμένο σημείο O επάνω της.*

Θεώρημα 2.2 *(Κανονική μορφή Weierstrass): Κάθε ελλειπτική καμπύλη E δίνεται στο αφινικό επίπεδο από μιά κυβική αλγεβρική εξίσωση της μορφής:*

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

η οποία είναι μη-ιδιόμορφη. Επιπλέον μπορούμε να ορίσουμε δομή αβελιανής ομάδας στά σημεία της καμπύλης με ουδέτερο στοιχείο το καθορισμένο σημείο O.

Απόδειξη: Θα δείξουμε πρώτα την δομή ομάδας κάνοντας χρήση του θεωρήματος Riemann-Roch και των πορισμάτων του. Εστω P, Q δυό σημεία της καμπύλης. Θεωρούμε τον διαιρέτη:

$$A := (P) + (Q) - (O)$$

Ισχύει $degA = 1$, το γένος g ισούται με 1, και λόγω του πορίσματος 1.30 έχουμε $dim\mathcal{L}(A) = 1$. Συνεπώς υπάρχει μοναδική κατά προσέγγιση σταθεράς f με δυό απλούς πόλους στα P, Q και δυό ρίζες. Η μιά είναι το O την άλλη την ονομάζουμε $P + Q$. Εύκολα αποδεικνύεται ότι η πράξη αυτή δίνει δομή μεταθετικής ομάδας στην καμπύλη.Ας αποδείξουμε γιά παράδειγμα τον προσεταιρισμό:

$$(P + Q) + R = P + (Q + R)$$

Ορίζουμε $\Sigma := (P + Q) + R$ και θεωρούμε τους πρωταρχικούς διαιρέτες:

$$(f) = (P) + (Q) - (P + Q) - (O)$$

$$(g) = (P + Q) + (R) - (\Sigma) - (O)$$

$$(h) = (Q) + (R) - (Q + R) - (O)$$

έχουμε τότε :

$$(f \cdot g) = (P) + (Q) + (R) - (\Sigma) - 2(O)$$

$$(1/h) = (Q + R) + (O) - (Q) - (R)$$

$$(f \cdot g/h) = (P) + (Q + R) - (\Sigma) - (O)$$

άρα

$$\Sigma = P + (Q + R).$$

Γιά να δείξουμε την αλγεβρικη σχέση : έχουμε $\mathcal{L}(O) =< 1 >$,

$$dim\mathcal{L}(2.O) = deg(2 \cdot O) = 2$$

και μία βάση αποτελούν οι συναρτήσεις $\{1, x\}$ όπου η x είναι συνάρτηση στό σώμα συναρτήσεων της ελλειπτικής καμπύλης E με διπλό πόλο στο O και κανένα άλλο πόλο. Συνεχίζουμε με όμοιο τρόπο και

$$dim(\mathcal{L}(3 \cdot O)) = 3 \Rightarrow \mathcal{L}(3 \cdot 0) =< 1, x, y >$$

δηλαδή υπάρχει συνάρτηση y με μοναδικό πόλο στο O τάξης ακριβώς 3.

$$dim(\mathcal{L}(4 \cdot 0)) = 4 \Rightarrow \mathcal{L}(4 \cdot O) =< 1, x, y, x^2 >$$

δηλαδή δεν χρειάζεται να προσθέσουμε καινούργια συνάρτηση.

$$dim(\mathcal{L}(5 \cdot 0)) = 5 \Rightarrow \mathcal{L}(5 \cdot 0) =< 1, x, y, x^2, xy >$$

και

$$dim(\mathcal{L}(6 \cdot 0)) = 6 \Rightarrow \mathcal{L}(6 \cdot 0) =< 1, x, y, x^2, xy, x^3, y^2 >$$

συνεπώς οι παραπάνω 7 συναρτήσεις είναι γραμμικά εξαρτημένες, άρα ικανοποιούν μιά σχέση της μορφής

$$ay^2 + bxy + cxy = dx^3 + hx^2 + ex + g$$

η οποία μετά από κατάλληλο μετασχηματισμό έρχεται στην μορφή:

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

<u>Παρατήρηση:</u> : Η παραπάνω αλγεβρική καμπύλη είναι μη ιδιόμορφη αλγεβρική υποπολαπλότητα του $\mathbb{C}^2$ δηλαδή το κάθετο διάνυσμα που δίνεται από τις $(\partial f/\partial x, \partial f/\partial y)$ δεν μηδενίζεται πουθενά. Αυτό συμβαίνει γιατί αν η κυβική καμπύλη είχε ιδιομορφίες τότε θα δέχονταν ρητή παραμετρικοποίηση,απλά περιστρέφοντας μιά ευθεία γύρω από την ιδιομορφία, και συνεπώς γένος 0. Με βάση αυτό τον τύπο μπορούμε να ορίσουμε ελλειπτικές καμπύλες σε οποιοδήποτε σώμα, ως τις μη ιδιόμορφες κυβικές καμπύλες της παραπάνω μορφής. Επιπλέον αν η χαρακτηριστική του σώματος που δουλεύουμε είναι διάφορη του $2, 3$, τότε η παραπάνω εξίσωση γράφεται στην παρακάτω μορφή

$$y^2 = x^3 + ax + b$$

την λεγόμενη κανονική μορφή του Weierstrass. Θα ακολουθήσουμε αυτή την διαδικασία ορίζοντας ένα πλήθος σταθερές οι οποίες θα μας φανούν χρήσιμες στην παρακάτω μελέτη μας. Ο μετασχηματισμός $y \longrightarrow \frac{1}{2}(y - a_1x - a_3)$ δίνει στην καμπύλη την μορφή:

$$E : y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

με

$$\begin{aligned} b_2 &= a_1^2 + 4a_2, \\ b_4 &= 2a_4 + a_1a_3, \\ b_6 &= a_3^2 + 4a_6. \end{aligned}$$

ορίζουμε επιπλέον τις σταθερές:

$$\begin{aligned} b_8 &= a_1^2 a_6 + 4a_2 a_6 - a_1 a_3 a_4 + a_2 a_3^2 - a_4^2, \\ c_4 &= b_2^2 - 24b_4, \\ c_6 &= b_2^3 + 36b_2 b_4 - 216b_6, \\ \Delta &= -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6 \\ j &= c_4^3/\Delta \end{aligned}$$

και ο μετασχηματισμός :$(x, y) \longrightarrow ((x - 3b_2)/36, y/216)$, οδηγεί στην εξίσωση του Weierstrass:

$$E : y^2 = x^3 - 27c_4 x - 56c_6$$

Ορισμός 2.3 *Η ποσότητα Δ λέγεται διακρίνουσα της E και η j απόλυτη αναλλοίωτος.*

Θεώρημα 2.4 *Δυό εξισώσεις του Weierstrass γιά την ελλειπτική καμπύλη E σχετίζονται με ένα γραμμικό μετασχηματισμό της μορφής:*

$$X = u^2 X' + r$$

$$Y = u^3 Y' + su^2 X' + t$$

όπου $u, r, s, t \in K, u \neq 0$.

Απόδειξη: Εστω $\{x, y\}$ και $\{x', y'\}$, δυό σύνολα συντεταγμένων Weierstrass στην ελλειπτική καμπύλη E. Τότε τα x και x' έχουν πόλους τάξης 2 στο O, και τα y, y' έχουν πόλους τάξης 3 στο O. Συνεπώς τα $\{1, x\}$ και $\{1, x'\}$ είναι και τα δυό βάσεις του $\mathcal{L}(2O)$ και ομοίως τα $\{1, x, y\}$ και $\{1, x', y'\}$ είναι και τα δύο βάσεις του $\mathcal{L}(3O)$. Αρα υπάρχουν σταθερές $u_1, u_2, r, s_2, t \in K$ με $u_1 u_2 \neq 0$ τέτοια ώστε:

$$x = u_1 x' + r, \quad y = u_2 y' + s_2 x' + t.$$

Ομως τα $\{1, x\}$ και $\{1, x'\}$ ικανοποιούν εξισώσεις Weierstrass συνεπώς πρέπει $u_1^3 = u_2^2$. Θέτουμε λοιπόν $u = u_2/u_1$ και $s = s_2/u_1^2$ από όπου προκύπτει η ζητούμενη σχέση.

Στα παρακάτω θα ακολουθήσουμε μιά διαφορετική προσέγγιση του παραπάνω θέματος. Ολες οι ελλειπτικές καμπύλες είναι τοπολογικά ισόμορφες και προκύπτουν ως χώροι πηλίκα του καθολικού καλύμματος τους, που εδώ είναι το $\mathbb{C}$, με κάποιο δικτυωτό (lattice) Λ, δηλαδή διακριτή υποομάδα του $\mathbb{C}$, $\mathbb{Z}$-διάστασης 2.

$$E(\mathbb{C}) \simeq \frac{\mathbb{C}}{\Lambda}$$

Αυτή η κατασκευή δίνει αυτόματα και την μιγαδική δομή στην $E(\mathbb{C})$ και όπως θα δούμε αργότερα έχουμε ισόμορφες (στην κατηγορία των επιφανειών Riemann) ελλειπτικές καμπύλες μόνο στην περίπτωση που τα αντίστοιχα δικτυωτά είναι ομόθετα, δηλαδή αν Λ_1, Λ_2 δύο δικτυωτά του $\mathbb{C}$ τότε

$$\left(\frac{\mathbb{C}}{\Lambda_1} \simeq \frac{\mathbb{C}}{\Lambda_2}\right) \Leftrightarrow (\Lambda_1 = \alpha\Lambda_2, \;\; \alpha \in \mathbb{C}^*).$$

Δηλαδή δύο δικτυωτά $\Lambda = \mathbb{Z}\omega_1 \bigoplus \mathbb{Z}\omega_2$ και $\Lambda' = \mathbb{Z}\omega_1' \bigoplus \mathbb{Z}\omega_2'$ είναι ομόθετα ανν οι δυό βάσεις διαφέρουν κατά μετασχηματισμό του $SL_2(\mathbb{Z})$. Αν γράψουμε τα δικτυωτά κατά τρόπο που η πρώτη τους συντεταγμένη να είναι 1 δηλαδή: $\Lambda = \mathbb{Z} \bigoplus \mathbb{Z}\omega$,όπου $\omega = \omega_2/\omega_1$ τότε κάθε δικτυωτό περιγράφεται από ένα μιγαδικό αριθμό με θετικό φανταστικό μέρος.

Ορισμός 2.5 *Το υπερβολικό επίπεδο $\mathbb{H}$ είναι το σύνολο των μιγαδικών αριθμών με θετικό φανταστικό μέρος.*

Είναι γνωστό ότι το $\mathbb{H}$ μπορεί να αποκτήσει μετρική Riemann που να δίνεται από τον τύπο

$$\begin{pmatrix} \frac{1}{y^2} & 0 \\ 0 & \frac{1}{y^2} \end{pmatrix}$$

και η ομάδα των ισομετριών είναι η $SL_2(\mathbb{R})$ [Ca]. Θεωρούμε την διακριτή υποομάδα των ισομετριών $SL_2(\mathbb{Z})$,η οποία δρά στο $\mathbb{H}$ ώς εξής:

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

Η δράση είναι εντός του $\mathbb{H}$ λόγω της θετικής ορίζουσας του παραπάνω πίνακα.
Παρατήρηση: Το πηλίκο

$$SL_2(\mathbb{Z})\backslash\mathbb{H}$$

παραμετρίζει το σύνολο των μη αναλυτικά ισόμορφων, υπέρ το $\mathbb{C}$ ελλειπτικών καμπύλων. Πράγματι έστω οί $\mathbb{Z}$ βάσεις, $\{\omega_1, \omega_2\}$, $\{\omega_1', \omega_2'\}$, τών δικυωτών Λ και Λ' αντιστοίχως. Τα δικτυωτά είναι ισόμορφα ανν υπάρχει μετασχηματισμός του $SL_2(\mathbb{Z})$ τέτοιως ώστε :

$$\begin{pmatrix} \omega_1 \\ \omega_2 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_1' \\ \omega_2' \end{pmatrix} \Rightarrow$$

$$\frac{\omega_1}{\omega_2} = \frac{a\omega_1' + b\omega_2'}{c\omega_1' + d\omega_2'} = \frac{a\frac{\omega_1'}{\omega_2'} + b}{c\frac{\omega_1'}{\omega_2'} + d}$$

συνεπώς το πηλίκο $z := \omega_1/\omega_2 \in \mathbb{H}$ που δίνει την κλάση ισοδυναμίας μετασχηματίζεται υπό την $SL_2(\mathbb{Z})$ ακριβώς με την δράση που ορίσαμε. Θα προσπαθήσουμε τώρα να περιγράψουμε, δεδομένης μιάς ελλειπτικής καμπύλης $E/\mathbb{C}$, το σώμα των μερόμορφων συναρτήσεων της, έστω $\mathbb{C}(E)$ και κατά συνέπεια να καταλήξουμε στο πολυώνυμο από το οποίο αυτή ορίζεται. Είναι σαφές ότι το σώμα $\mathbb{C}(E)$ είναι ισόμορφο με το σώμα των διπλά περιοδικών συναρτήσεων από το $\mathbb{C}$ στο $\mathbb{C}$ ώς προς το δικτυωτό Λ. Κάθε τέτοια μη σταθερή συνάρτηση πρέπει να έχει τουλάχιστον δυό πόλους ή ένα πόλο τουλάχιστον τάξης 2. Πράγματι αν $f \in \mathbb{C}(E)$ τότε η διαφορική μορφή $f(z)dz$ γραμμένη στον τοπικό χάρτη (U_z, z) έχει άθροισμα ολοκλήρωτικων υπολοίπων 0, και συνεπώς τουλάχιστον δυό πόλους, ή ένα πόλο τάξης 2. Ακολουθώντας τα βήματα του Weierstrass θα προσπαθήσουμε να ορίσουμε διπλά περιοδική συνάρτηση με διπλό πόλο σε κάθε περίοδο:[Ap]

$$\wp(z) := \frac{1}{z^2} + \sum_{\omega \neq 0} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right)$$

όπου τα ω διατρέχουν όλα τα στοιχεία του δικυωτού Λ, με $\mathbb{Z}$ βάση την: $\{\omega_1, \omega_2\}$. Θα δείξουμε ότι είναι Λ-περιοδική και καλώς ορισμένη συνάρτηση του z. Αρχίζουμε αποδεικνύοντας την σύγκλιση της παραπάνω σειράς.

Ισχυρισμός: υπάρχει σταθερά $M(R)$ που εξαρτάται από την ακτίνα R τέτοια ώστε:

$$\left|\frac{1}{(z-\omega)^2}\right| \leq \frac{M(R)}{|\omega|^2} \quad \forall \omega : |\omega| > R$$

Πράγματι θεωρούμε όλες τις περιόδους με $|\omega| > R$ και διαλέγουμε μία με το μικρότερο μέτρο έστω, $|\omega| = R + d, d > 0$. Γιά $|z| \leq R$ και γιά $|\omega| \geq R + d$ ισχύει:

$$\left|\frac{z-\omega}{\omega}\right| = \left|1 - \frac{z}{\omega}\right| \geq 1 - \left|\frac{z}{\omega}\right| \geq 1 - \frac{R}{R+d}$$

συνεπώς αρκεί γιά $M(R)$ να πάρουμε το $M = (1 - R/(R+d))^2$.

Θεωρούμε τον δίσκο:$|z| \leq R$ και εξαιρούμε τις πεπερασμένες περιόδους που περιέχονται στον δίσκο αυτό και σύμφωνα με τον παραπάνω ισχυρισμό έχουμε:

$$\left|\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right| = \left|\frac{z(2\omega - z)}{\omega^2(z-\omega)^2}\right| \leq \frac{MR(2|\omega| + R)}{\omega^4} \leq \frac{MR(2 + R/|\omega|)}{|\omega|^3} \leq \frac{3MR}{|\omega|^3}$$

οπότε το άθροισμα πάνω σε όλες τις εξωτερικές περιόδους είναι αναλυτική συνάρτηση γιά όλα τα εσωτερικά $|z| < R$. Πράγματι οι σειρές

$$\sum_{\omega \in \Lambda \ \ \omega \neq 0} |\omega|^{-\alpha}$$

είναι συγκλίνουσες γιά $\alpha > 2$ όπως εύκολα διαπιστώνει κανείς συγκρίνοντας τες με το

$$\iint \frac{dxdy}{(x^2+y^2)^{\alpha/2}}.$$

Για την περιοδικότητα της $\wp$ παρατηρούμε ότι η παράγωγος γράφεται :

$$\wp(z)' = -2\sum_{\omega \in \Lambda} \frac{1}{(z-\omega)^3}$$

συνάρτηση περιοδική ως προς το δικτυωτό Λ.Αρα

$$\wp'(z+\omega) = \wp'(z) \quad \forall\, \omega \in \Lambda$$

άρα η συνάρτηση $\wp(z-\omega) - \wp(z)$ είναι σταθερή και θέτοντας την τιμή $z = -\omega/2$ βλέπουμε ότι είναι σταθερή ίση με 0, συνεπώς η $\wp$ είναι περιοδική.

Θεώρημα 2.6 *(Το ανάπτυγμα Laurent της $\wp$ στο 0.) Εστω $r = min\{|\omega| : \omega \neq 0\}$ γιά $0 < |z| < r$ έχουμε*

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(2n+1)G_{2n+2}z^{2n}$$

όπου $G_n = \sum \omega^{-n}, n \geq 3$ οι σειρές του Eisenstein.

Απόδειξη: αφού $0 < |z| < r$ έχουμε $|z/\omega| < 1$. Συνεπώς

$$\frac{1}{(z-\omega)^2} = \frac{1}{\omega^2(1-\frac{z}{\omega})^2} = \frac{1}{\omega^2}\left(1 + \sum_{n=1}^{\infty}(n+1)\left(\frac{z}{\omega}\right)^n\right)$$

συνεπώς

$$\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} = \sum_{n=1}^{\infty}\frac{n+1}{\omega^{n+2}}z^n$$

Αθροίζουμε ως προς τα $\omega \in \Lambda$ και τελικά βρίσκουμε:

$$\wp(z) = \frac{1}{z^2} + \sum_{n=1}^{\infty}(n+1)\sum_{\omega\neq 0}\frac{z^n}{\omega^{n+2}} = \frac{1}{z^2} + \sum_{n=1}^{\infty}(n+1)G_{n+2}z^n.$$

Παρατηρούμε ότι η $\wp$ είναι άρτια συνάρτηση συνεπώς όλοι οι συντελεστές $G_{2n+1} = 0$.

Θεώρημα 2.7 *(Διαφορική εξίσωση της $\wp$)*
Ισχύει ότι :

$$\wp^{2\prime}(z) = 4\wp^3(z) - 60G_4\wp(z) - 140G_6$$

Θα καταλήξουμε στο παραπάνω αποτέλεσμα θεωρώντας γραμμικούς συνδιασμούς δυνάμεων των $\wp, \wp'$ που εξουδετερώνουν τον πόλο $z = 0$. Απο το ανάπτυγμα της $\wp$ στο 0 έχουμε το αντίστοιχο ανάπτυγμα της παραγώγου:

$$\wp'(z) = -\frac{2}{z^3} - 6G_4z + 20G_6z^3 + ...+$$

$$\wp^{2\prime}(z) = \frac{4}{z^6} - \frac{24}{z^2}G_4 - 80G_6 + ...+$$

$$4\wp^3(z) = \frac{4}{z^6} + \frac{36}{z^2}G_4 + 60G_6 + ...$$

$$\wp^{2\prime}(z) - 4\wp^3(z) - \frac{60}{z^2}G_4\wp(z) = -140G_6 + ...$$

όπου η τελευταία έκφραση δεν έχει πόλους, είναι σταθερή και συνεπώς ίση με $-140G_6$.

Η παραπάνω έκφραση είναι σημαντική γιατί παραμετρίζει την ελλειπτική καμπύλη, δηλαδή δίνει μιά συνάρτηση

$$\mathcal{F} : \mathbb{C} \longrightarrow \mathbb{C}/\Lambda \subset \mathbb{P}^2(\mathbb{C})$$

$$z \longmapsto (\wp(z), \wp'(z), 1)$$

Εύκολα διαπιστώνουμε ότι το σώμα των ελλειπτικών συναρτήσεων είναι ισόμορφο με την παρακάτω αλγεβρική επέκταση του $\mathbb{C}(X)$:

$$\mathbb{C}(E) = \mathbb{C}(\wp, \wp') \simeq \frac{\mathbb{C}(X)[Y]}{< Y^2 - 4X^3 + g_2X + g_3 >}$$

όπου $g_2 := 60G_4$ και $g_3 = 140G_6$. Οι ελλειπτικές καμπύλες υπέρ του $\mathbb{C}$ είναι αβελιανές ομάδες ως πηλίκα των αβελιανών ομάδων $\mathbb{C}/\Lambda$ ή λόγω Riemann-Roch όπως είδαμε στην αρχή. Οι εξισώσεις του Weierstrass $\wp, \wp'$ δίνουν μιά κομψή αλγεβρική έκφραση της δομής ομάδας. Πράγματι παρατηρούμε ότι:

$$\begin{vmatrix} \wp(z) & \wp'(z) & 1 \\ \wp(u) & \wp'(u) & 1 \\ \wp(u+z) & -\wp'(u+z) & 1 \end{vmatrix} = 0$$

και συνεπώς τρία σημεία έχουν άθροισμα 0 ανν είναι συνευθειακά. Η παρατήρηση αυτή μας δίνει την δυνατότητα να ορίσουμε δομή ομάδας σε οποιοδήποτε σώμα από τις αλγεβρικές εξισώσεις της ιδιότητας του συνευθειακού.

Παρατήρηση: Οι ελλειπτικές καμπύλες είναι οι μοναδικές καμπύλες που δέχονται δομή ομάδας όπου οι πράξεις είναι ολόμορφες συναρτήσεις. Πράγματι η δομή ομάδας μας επιτρέπει να ορίσουμε ένα πουθενά μη μηδενιζόμενο διανυσματικό πεδίο, το οποίο όπως είναι γνωστό [Hi,σελ. 133] γίνεται μόνο αν η χαρακτηριστική Euler είναι 0, δηλαδή αν το γένος είναι 1.

Παρατήρηση: Οι ελλειπτικές καμπύλες επεκτείνουν με θαυμάσιο τρόπο την έννοια του κυκλοτομικού σώματος αριθμών. Πράγματι στα κυκλοτομικά σώματα αριθμών μας ενδιαφέρει η αριθμητική των σημείων πεπερασμένης τάξης του κύκλου S^1, ένω στις ελλειπτικές καμπύλες η αριθμητική του των σημείων πεπερασμένης τάξης του τόρου $S^1 \bigoplus S^1$. Οι ομοιότητες είναι πολλές, γιά παράδειγμα οι n ρίζες της μονάδας υπολογίζονται με τις υπερβατικές συναρτήσεις $e^{2\pi i x}$ στο σημείο $\frac{1}{n}\mathbb{Z}$, ομοίως τα σημεία τάξης n υπολογίζονται από τις τιμές στο $\frac{1}{n}\Lambda$ των συναρτήσεων Weierstrass $\wp, \wp'$. Η αναλογία αυτή είναι μεγάλης σημασίας γιά την απόδειξη του Θεωρήματος Fermat όπως θα διαπιστώσουμε στην συνέχεια.

2.2 Κυβικές καμπύλες του Weierstrass

Θεώρημα 2.8 *Ισχύουν τα παρακάτω:*

1. *Μια κυβική καμπύλη (σε οποιοδήποτε σώμα K) που δίνεται απο μια εξίσωση Weierstrass ταξινομείται:*
   - *μη ιδιόμορφη ανν $\Delta \neq 0$*
   - *ιδιόμορφη τύπου κόμβου (node form) ανν $\Delta = 0$ και $c_4 \neq 0$*
   - *ιδιόμορφη τύπου ακίδας (cusp form) ανν $\Delta = c_4 = 0$*
2. *Δύο ελλειπτικές καμπύλες είναι ισόμορφες στο $\bar{K}$ ανν έχουν την ίδια j-αναλλοίωτο.*
3. *Εστω $j_0 \in \bar{K}$ τότε υπάρχει ελλειπτική καμπύλη, ορισμένη στο $\mathrm{K}(j_0)$, με j αναλλοίωτο j_0*

Απόδειξη:

1. Εστω ότι η Ε δίνεται από την εξίσωση τού Weierstrass

$$\mathrm{E} : f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$$

Ξεκινούμε δείχνοντας ότι το σημείο στο άπειρο δεν είναι ποτέ ιδιόμορφο. Μελετούμε λοιπόν την ομογενή εξίσωση στο $\mathbb{P}^2(K)$

$$F(x,y,z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$$

στο σημείο $0 = [0,1,0]$

$\partial F/\partial z(0,0) = 1 \neq 0$ αρα όχι ιδιόμορφο σημείο. Ας υποθέσουμε ότι E είναι ιδιόμορφη στο σημείο $P_0 = (x_0, y_0)$. Ο μετασχηματισμός $x = x' + x_0, y = y' + y_0$ αφήνει το Δ και το c_4 αναλλοίωτα άρα χωρίς περιορισμό της γενικότητας μπορούμε να υποθέσουμε ότι η E είναι ιδιόμορφη στο (0,0). Τότε

$$a_6 = f(0,0) = 0, \;\; a_4 = \frac{\partial F}{\partial x}(0,0) = 0, \;\; a_3 = \frac{\partial F}{\partial y}(0,0) = 0$$

και η εξίσωση έχει την μορφή:

$$\mathrm{E} : f(x,y) = y^2 + a_1xy - x^3 - a_2x^2$$

$$c_4 = (a_1^2 + 4a_2)^2, \;\; \Delta = 0$$

Τώρα όπως είναι γνωστό η συμπεριφορά των εφαπτομένων στο σημειο $(0,0)$ δίνεται από την τετραγωνική μορφή:

$$y^2 + a_1xy - a_2x^2$$

και το αν θα έχουμε ή όχι δύο η μία διπλή εφαπτομένη εξαρτάται από το αν η διακρίνουσα της τετραγωνικής αυτής μορφής δηλαδή η

$$c_4 = (a_1^2 + 4a_2)^2$$

είναι 0 η όχι. Τέλος είναι εύκολο να δούμε ότι αν $\Delta = 0$ τότε η κυβική καμπύλη είναι ιδιόμορφη.

2. Είδαμε ότι οι μετασχηματισμοί που διατηρούν αναλλοίωτη την μορφή της εξίσωσης Weierstrass είναι οι:

$$\begin{aligned} x &= u^2x' + r \\ y &= u^3y' + u^2sx' + t \end{aligned}$$

με $u, r, s, t \in \bar{K}, u \neq 0$. Επιπλέον παρατηρούμε ότι πρόκειται γιά ισομορφισμούς ελλειπτικών καμπύλων αφού μεταφέρουν ευθείες σε ευθείες, και τέλος αφήνουν την j συνάρτηση αναλλοίωτη.

Για το αντίστροφο παρατηρούμε ότι αν E, E' ελλειπτικές καμπύλες με την ίδια j συνάρτηση και με εξισώσεις

$$y^2 = x^3 + Ax + B$$

$$y'^2 = x'^3 + A'x' + B'$$

τότε

$$(4A)^3/(4A^3+27B^2) = (4A')^3/(4A'^3+27B'^2) \text{ συνεπώς } A^3B'^2 = A'^3B^2$$

Ψάχνουμε γιά ισομορφισμό της μορφής $(x,y) = (u^2x', u^3y')$ καί θεωρούμε τρείς περιπτώσεις:

$A = 0$ δηλαδή ($j = 0$) καί $B \neq 0$ (αφού $\Delta \neq 0$) καί παίρνουμε τελικά $u = (B/B')^{1/6}$

$B = 0$ δηλαδή ($j = 1728$) τότε $\mathrm{A} \neq 0, B' = 0$ καί $u = (A/A')^{1/4}$

$AB \neq 0$ δηλαδή ($j \neq 0, 1728$) τότε $\mathrm{A}'B' \neq 0$ οπότε παίρνουμε $u = (B/B')^{1/6} = (A/A')^{1/4}$

3. Αν $j_0 \neq 0, 1728$ τότε η καμπύλη:

$$\mathrm{E} : y^2 + xy = x^3 - \frac{36}{(j_0 - 1728)}x - \frac{1}{j_0 - 1728}$$

έχει $\Delta = \frac{j_0^2}{(j_0-1728)^3}$ καί $j = j_0$ ενώ γιά τις άλλες δυό περιπτώσεις απλά παρατηρούμε ότι οι
$\mathrm{E} : y^2 + y = x^3$
$\mathrm{E} : y^2 = x^3 + x$
έχουν $\Delta = -27$, $j = 0$ καί $\Delta = -64$, $j = 1728$ αντίστοιχα.

Η μελέτη της j συνάρτησης απαντά στο πρόβλημα ισομορφίας ελλειπτικών καμπυλών στην αλγεβρική κλειστότητα του σώματος που δουλεύουμε. Γιά να απαντήσουμε στο ανάλογο πρόβλημα για σώματα μικρότερα της αλγεβρικής κλειστότητας χρειαζόμαστε την Galois συνομολογία $\mathrm{H}^1(Gal(\bar{K}/K), Aut_{\bar{K}}(E))$ [Hu, κεφ.7] αλλά προς το παρόν θα περιοριστούμε στο να ορίσουμε την έννοια της Hasse-invariant και μάλιστα στην ειδική περίπτωση που $j_0 \neq 0, 1728$. Οπως είδαμε πιό πριν αν δύο ελλειπτικές καμπύλες έχουν την ίδια j-ανναλοίωτο τότε :

$$\left(\frac{\mathrm{A}}{\mathrm{A}'}\right)^3 = \left(\frac{B}{B'}\right)^2$$

το οποίο σημαίνει ότι

$$\frac{\mathrm{A}}{\mathrm{A}'} = t^2 \ , \ \frac{B}{B'} = t^3$$

και ο μετασχηματισμός

$$\begin{aligned} x &\longmapsto tx \\ y &\longmapsto t^{3/2}y \end{aligned}$$

που ορίζεται στο $\mathrm{K}(t^{1/2})$ είναι ο ζητούμενος ισομορφισμός. Δηλαδή δυό ελλειπτικές καμπύλες με την ίδια j-αναλλοίωτο γίνονται ισόμορφες σε μια τετραγωνική, το πολύ, επέκταση του σώματος ορισμού τους. Ο έλεγχος γιά το αν υπάρχει ισομορφία στα πλαίσια του αρχικού σώματος ελέγχεται με το αν οι Hasse συναρτήσεις των δύο ελλειπτικών καμπύλων που ορίζονται ώς:

$$\delta_E := -\tfrac{1}{2}A/B mod K^{*2}$$

είναι ίσες ή όχι. Ο παράγων $-\frac{1}{2}$ εισάγεται για ιστορικούς λόγους. Πράγματι απο τους παραπάνω τύπους έχω:

$$\mathrm{A}/B = A'/tB' \Leftrightarrow -At/2B = -A'/2B'$$

συνεπώς $\delta_E = \delta_{E'}$ ανν $t \in K^{*2}$.

2.3 Η αλγεβρική δομή των ιδιόμορφων κυβικών καμπυλών

Στην περίπτωση που η διακρίνουσα μηδενίζεται έχουμε ιδιόμορφη κυβική καμπύλη. Στην προηγούμενη παράγραφο διαχωρίσαμε δυό περιπτώσεις ιδιομορφίας και μάλιστα δώσαμε κριτήρια για το πότε συμβαίνει κάθε μία. Εδώ θα αναλύσουμε την αλγεβρίκη συμπεριφορά κάθε περίπτωσης.Στην περίπτωση των μη ιδιόμορφων κυβικών καμπύλων (ελλειπτικές) ορίζουμε όπως είδαμε νόμο ομάδας πάνω στα σημεία της καμπύλης μέσω του κανόνα χορδής-εφαπτομένης. Ανάλογη εργασία θα κάνουμε και εδώ. Υποθέτουμε, γιά να διευκολύνουμε τους υπολογισμούς ότι η ελλειπτική καμπύλη είναι της μορφής:

$$\mathrm{Y}^2 = \mathrm{X}^3 + \mathrm{AX} + \mathrm{B}$$

- Πρώτη περίπτωση: ιδιομορφία τύπου ακίδας (cusp form). Εχουμε, από το προηγούμενο γενικό κριτήριο ότι $c_4 = B = 0$ συνεπώς λόγω μηδενισμού της $\Delta = 4A^3 + 27B^2$ θα έχουμε ότι και $\mathrm{A} = 0$ οπότε έχουμε την καμπύλη $C : Y^2Z = X^3$ με ιδιόμορφο σημείο το $(0, 0)$. Κάθε γραμμή που δεν περνά από την αρχή των αξόνων γράφεται ως: $\mathrm{Z} = lX + mY$ και συναντά την C στα σημεία που επαληθεύουν την εξίσωση: $\mathrm{X}^3 - \mathrm{Y}^2(lX + mY) = 0$. Αν τα τρία σημεία τομής είναι τα (x_j, y_j, z_j), $j = 1, 2, 3$ τότε έχουμε $u_1 + u_2 + u_3 = 0$ όπου $u_j := x_j/y_j$. Αρα ορίζουμε δομή ομάδας στα σημεία της καμπύλης βάσει αυτού του κανόνα και εύκολα διαπιστώνουμε ότι η δομή αυτή κάνει το σύνολο των μη ιδιόμορφων σημείων της ελλειπτικής καμπύλης ισόμορφο με την προσθετική ομάδα του σώματος ορισμού της E.

- δεύτερη περίπτωση: ιδιομορφία τύπου κόμβου (node form). Αν δεν μηδενίζονται και τα δυό A, B τότε υπάρχει μετασχηματισμός

  $$\mathrm{X} \longmapsto X + \text{σταθερά}$$

  τέτοιος ώστε

  $$\mathrm{Y}^2\mathrm{Z} = \mathrm{X}^2(\mathrm{X} + \lambda Z) \;\; \lambda \neq 0$$

  $$\text{άρα } (\mathrm{Y}^2 - \lambda \mathrm{X}^2)Z = X^3$$

  όπου $\pm\lambda$ είναι οι κλίσεις των δυό εφαπτομένων στο $(0, 0)$.

Αν το λ είναι τετράγωνο τότε $U := Y + \gamma X, V := Y - \gamma X,\ \gamma := \sqrt{\lambda}$ και έχουμε $8\gamma^3 UVZ = (U - V)^3$. Κάθε γραμμή που δεν περνά από την αρχή των αξόνων γράφεται $Z = lU + mV$ και τέμνει την C στο $8\gamma^3 UV(lU + mV) - (U - V)^3 = 0$. Αν τα σημεία τομής είναι $(u_j, v_j, z_j), j = 1, 2, 3$ τότε έχουμε $(\frac{u_1}{v_1})(\frac{u_2}{v_2})(\frac{u_3}{v_3}) = 1$. Συνεπώς η ομάδα είναι ισόμορφη με την πολλαπλασιαστική ομάδα του σωματός ορισμού της E. Αν το λ δεν είναι τετράγωνο τότε επισυνάπτουμε την τετραγωνική του ρίζα και στο μεγαλύτερο σώμα κάνουμε την ίδια δουλειά. Ανάλογα με το αν λ είναι η όχι τετράγωνο ονομάζουμε την περίπτωση σε διαχωρισμένη και μη διαχωρισμένη πολλαπλασιαστική ιδιομορφία (singularity of split/non-split multiplicative type) αντίστοιχα.

2.4 Ελλειπτικές καμπύλες ορισμένες πάνω σε τοπικά σώματα

Στην παρούσα παράγραφο θα μελετήσουμε την ομάδα των ρητών σημείων μιάς ελλειπτικής καμπύλης ορισμένης πάνω σε σώμα το οποίο είναι πλήρες ως προς μιά διακριτή εκτίμηση. Θα ξεκινήσουμε με απλές παρατηρήσεις για τις εξισώσεις Weierstrass και την αναγωγή (reduction) modπ. Στα επόμενα θα συμβολίζουμε με:

K : τοπικό σώμα πλήρες ως προς την διακριτή εκτίμηση v
$\mathcal{R}$: ο δακτύλιος των ακεραίων του K δηλαδή $x \in K : v(x) \geq 0$
$\mathcal{R}^*$: η ομάδα των μονάδων, δηλαδή $x \in \mathcal{R} : v(x) = 0$
$\mathcal{M}$: το μέγιστο ιδεώδες του $\mathcal{R}$ δηλάδη $x \in \mathrm{K} : v(x) > 0$
π : τοπική συντεταγμένη του $\mathcal{R}, \mathcal{M} = \pi\mathcal{R}$
k : το σώμα πηλίκων $k = \mathcal{R}/\mathcal{M}$
γιά την v υποθέτουμε ότι είναι κανονικοποιημένη, δηλαδή $v(\pi) = 1$.

2.4.1 Ελλάχιστες εξισώσεις του Weierstrass

Εστω E/K ελλειπτική καμπύλη και έστω

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

μια εξίσωση του Weierstrass αυτής. Αντικαθιστώντας $(x, y) \longmapsto (u^{-2}x, u^{-3}y)$ αλλάζουμε τα $a_i \longmapsto u^i a_i$ και διαλέγοντας το u να διαιρείται από μεγάλη δύναμη του π, μπορούμε να βρούμε Weierstrass εξίσωση με $a_i \in \mathcal{R}$. Τότε η διακρίνουσα Δ ως αλγεβρικός συνδυασμός των $a_i \in \mathcal{R}$ θα είναι με εκτίμηση $v(\Delta) \geq 0$ και αφού v διακριτή γυρεύουμε μοντέλο με $v(\Delta)$ όσο το δυνατόν μικρότερο.

Ορισμός 2.9 *Εστω E/K ελλειπτική καμπύλη. Μιά εξίσωση του Weierstrass θα λέγεται ελάχιστη της Ε προς την θέση v ανν $v(\Delta)$ είναι ελαχίστη υπό την προυπόθεση ότι $a_1, ..., a_6 \in \mathcal{R}$*

<u>Παρατήρηση:</u>
Πως μπορούμε να ελέγξουμε αν μια δεδομένη εξίσωση του Weierstrass είναι ελάχιστη; Καταρχήν όλα τα a_i πρέπει να ανήκουν στο $\mathcal{R}$ και ειδικότερα η $\Delta \in \mathcal{R}$. Αν η εξίσωση δεν είναι ελάχιστη τότε υπάρχει αλλαγή συντεταγμένων που δίνει διακρίνουσα $\Delta' = u^{12}\Delta \in \mathcal{R}$. Αρα η $v(\Delta)$ μπορεί να αλλαχθεί μόνο σε "βήματα" του 12 συνεπώς αν $a_i \in \mathcal{R}$ και $v(\Delta) < 12$ τότε η εξίσωση είναι

ελάχιστη. Ομοίως αφού $c_4' = u^4 c_4$ και $c_6' = u^6 c_6$ έχουμε ότι αν $a_i \in \mathcal{R}$ και $v(c_4) < 4$ ή $v(c_6) < 6$ τότε η εξίσωση είναι ελάχιστη.

Παράδειγμα: Θεωρούμε την ελλειπτική καμπύλη:

$$\mathrm{E} : y^2 + xy + y = x^3 + x^2 + 22x - 9$$

ορισμένη στο $\mathbb{Q}_p$. Εχουμε $\Delta = -2^{15} \cdot 5^2, c_4 = -5 \cdot 2 \cdot 11$ συνεπώς είναι ελάχιστη εξίσωση για κάθε πρώτο του $\mathbb{Z}$.

2.4.2 Αναγωγή modulo π

Θα μελετήσουμε την αναγωγή modulo π κατά την οποία θεωρούμε την φυσική προβολή:

$$\mathcal{R} \longrightarrow k = \mathcal{R}/\pi\mathcal{R}$$

$$t \longmapsto \tilde{t}$$

Γιά δεδομένη ελάχιστη εξίσωση του Weierstrass για την E/K θεωρούμε όλους τους συντελεστές mod π και παίρνουμε μια (πιθανόν ιδιόμορφη) κυβική καμπύλη πάνω από το k την:

$$\tilde{E}/k : y^2 + \tilde{a}_1 xy + \tilde{a}_3 y = x^3 + \tilde{a}_2 x^2 + \tilde{a}_4 x + \tilde{a}_6$$

Η καμπύλη αυτή λέγεται η ανηγμένη της αρχικής modπ. Η $\tilde{E}$, αφού ξεκίνησα με ελάχιστη εξίσωση για το E, είναι μοναδική κατά προσέγγιση των συνήθων μετασχηματισμών εξισώσεων υπέρ το k.

2.4.3 Καλή και κακή αναγωγή

Εστω Ε/Κ ελλειπτική καμπύλη. Η ανηγμένη εξίσωση $\tilde{E}$/Κ μπορεί να παρουσιάσει ιδιομορφίες.

Ορισμός 2.10

- *Θα λέμε ότι η Ε έχει καλή ή stable αναγωγή πάνω από το* Κ *ανν η* $\tilde{E}$ *είναι μη ιδιόμορφη.*
- *Θα λέμε ότι η Ε έχει πολλαπλασιαστική ή semistable αναγωγή πάνω από το* Κ *ανν η* $\tilde{E}$ *έχει ιδιομορφία πολλαπλασιαστικού τύπου (node form). Σε αυτή την περίπτωση η αναγωγή θα λέγεται διαχωρισμένη, μη διαχωρισμένη μορφή ανάλογα με το αν οι κλίσεις των εφαπτομένων ευθειών στον κόμβο ανήκουν στο* k *ή όχι.*
- *Θα λέμε ότι η Ε έχει προσθετική η unstable αναγωγή πάνω από το* Κ *ανν η* $\tilde{E}$ *έχει ιδιομορφία προσθετικού τύπου (cusp form).*

Παράδειγμα:
Εστω $p \geq 5$ πρώτος αριθμός και θεωρούμε τις ακόλουθες ελλειπτικές καμπύλες στο $\mathbb{Q}_p$:
$E_1 : y^2 = x^3 + px^2 + 1$ προφανώς έχει καλή αναγωγή mod $p\mathbb{Z}_p$
$E_2 : y^2 = x^3 + x^2 + p$ προφανώς έχει split πολλαπλασιαστική αναγωγή mod $p\mathbb{Z}_p$
$E_3 : y^2 = x^3 + p$ προφανώς έχει κακή αναγωγή mod $p\mathbb{Z}_p$
Ομως η E_3 έχει καλή αναγωγή στο $\mathbb{Q}_p(\sqrt[6]{p})$ αφού τότε το δεδομένο μοντέλο της E_3 στο $\mathbb{Q}_p(\sqrt[6]{p})$

δεν είναι ελάχιστο. Πράγματι με την παραπάνω επέκταση αυξάνουμε τους ακεραίους και με τους μετασχηματισμούς της εξίσωσης του Weierstrass μπορούμε να επιτύχουμε μικρότερη διακρίνουσα. Ετσι ενώ αρχικά είχαμε:

$$v_p(\Delta) = v_p(27p^2) = 2$$

κάνοντας τον μετασχηματισμό $x = \sqrt[3]{p}x', \ y = \sqrt[2]{p}y'$ βρίσκουμε ότι η E_3 πάνω από το σώμα $\mathbb{Q}_p(\sqrt[6]{p})$ έχει την εξίσωση:

$$y'^2 = x'^3 + 1$$

της οποίας η διακρίνουσα είναι $\Delta = 1$ και προφανώς $v(\Delta) = 0$. Καταλήξαμε λοιπόν στο συμπέρασμα ότι η ιδιότητα της κακής αναγωγής μεταβάλλεται όταν θεωρούμε την E σε διαφορετικά σώματα.

Ορισμός 2.11 E/K *ελλειπτική καμπύλη. Η E έχει δυνάμει (potential) καλή αναγωγή πάνω από το K ανν υπάρχει πεπερασμένη επέκταση K$'/K$ ώστε η E να έχει καλή αναγωγή στο K'.*

Θεώρημα 2.12 *(ημιευσταθούς αναγωγής) Αν E/K είναι μία ελλειπτική καμπύλη τότε:*

1. *Αν K$'/K$ είναι μιά μη διακλαδιζομένη πεπερασμένη επέκταση του K, τότε ο τύπος αναγωγής της E υπέρ το K (καλή,πολλαπλασιαστική, προσθετική) διατηρείται και στο K'*

2. *Εστω K'/K πεπερασμένη επέκταση. Αν η E έχει καλή η πολλαπλασιαστική αναγωγή πάνω από το K, τότε έχει τον ιδίου τύπου αναγωγή και στο K'.*

3. *Υπάρχει πάντοτε πεπερασμένη επέκταση K'/K τέτοια ώστε η E να έχει καλή ή διαχωρίσιμη πολλαπλασιαστική αναγωγή υπέρ το K'.*

4. *Η E έχει δυνάμει καλή αναγωγή ανν η j-αναλλοίωτη της είναι $\mathcal{R}$-ακεραία.*

Απόδειξη:

1. Υποθέτουμε οτι char$(k) \geq 5$ (Η περίπτωση char(k)=2,3 είναι ιδιαίτερα περίπλοκη και για αυτό παραλείπεται. Οποιος ενδιαφέρεται σχετικά μπορεί να δεί το άρθρο του J.Tate [Ta]. Επομένως η E έχει ελάχιστη εξίσωση του Weierstrass της μορφής:

   $$E : y^2 = x^3 + Ax + B$$

   Εστω $\mathcal{R}'$ ο δακτύλιος ακεραίων του K' και v' η εκτίμηση του K' που εκτείνει την v και $x = (u')^2x', y = (u')^3y'$ ο μετασχηματισμός που δίνει ελάχιστη εξίσωση της E υπέρ το K'. Αφού η K'/K είναι μη διακλαδιζομένη, μπορούμε να βρούμε $u \in K$ τέτοιο ώστε $(u/u') \in (\mathcal{R}')^*$. Πράγματι αν $u' = \Pi^l s$, όπου $s \in (\mathcal{R}')^*$ τότε λόγω της μη διακλάδωσης έχουμε την σχέση των δυό τοπικών μεταβλητών π και Π: $\pi\mathcal{R}' = \Pi\mathcal{R}'$ οπότε αρκεί να θέσουμε $u = \pi^l$ οπότε προφανώς έχουμε $(u/u') = s \in (\mathcal{R}')^*$. Συνεπώς ο μετασχηματισμός $x = u^2x', y = u^3y'$

δίνει επίσης ελάχιστη εξίσωση της E υπέρ το K′, αφού $v'(u^{-12}\Delta) = v'(u'^{-12}\Delta)$. Η νέα εξίσωση έχει συντελεστές στο $\mathcal{R}$ και συνεπώς από το ελάχιστο του αρχικού μοντέλου στο K έχουμε $v(u) = 0$. Τελικά βλέπουμε ότι $v(\Delta) = v(\Delta')$ και $v(c_4) = v(c_4')$ και συνεπώς έχουμε την ίδια συμπεριφορά ως προς την αναγωγή.

2. Εστω μια ελάχιστη Weierstrass εξίσωση γιά την E υπέρ το K με αντίστοιχα Δ και c_4, $\mathcal{R}'$ ο δακτύλιος των ακεραίων του K', v' η εκτίμηση του K' που εκτείνει την v και έστω

$$\begin{aligned} x &= u^2x' + r \\ y &= u^3y' + su^2x' + t \end{aligned}$$

η αλλαγή μεταβλητών που δίνει μια ελάχιστη εξίσωση του Weierstrass της E υπέρ το K'. Γιά την καινούργια εξίσωση τα Δ' και c_4' ικανοποιούν:

$$\begin{aligned} 0 &\leq v'(\Delta') = v'(u^{-12}\Delta) \\ 0 &\leq v'(c_4') = v'(u^{-4}c_4) \end{aligned}$$

επειδή $u \in \mathcal{R}$ έχουμε

$$0 \leq v'(u) \leq min\left\{\frac{1}{12}v'(\Delta), \frac{1}{4}v'(c_4)\right\}$$

Ομως για καλή (αντίστοιχα πολλαπλασιαστική) αναγωγή έχουμε $v(\Delta) = 0$ (αντίστοιχα $v(c_4) = 0$) άρα σε κάθε περίπτωση $v'(u) = 0$ άρα $v'(\Delta') = v'(\Delta)$ και $v'(c_4') = v'(c_4)$.

3. Υποθέτουμε ότι char$k \neq 2$ και εκτείνουμε το K έτσι ώστε η E να έχει εξίσωση του Weierstrass στην κανονική μορφή Legendre:

$$E : y^2 = x(x-1)(x-\lambda), \;\; \lambda \neq 0, 1$$

τότε

$$c_4 = 16(\lambda^2 - \lambda + 1)$$

$$\Delta = 16\lambda^2(\lambda - 1)^2$$

Ξεχωρίζουμε τρείς περιπτώσεις:

- $\lambda \in \mathcal{R}$, $\lambda \neq 0, 1 \; mod \; \mathcal{M}$ τότε $\Delta \in \mathcal{R}^*$, άρα η καμπύλη έχει καλή αναγωγή.
- $\lambda \in \mathcal{R}, \lambda = 0$ ή $1 mod \mathcal{M}$ τότε $\Delta \in \mathcal{M}, c_4 \in \mathcal{R}^*$ και συνεπώς η E έχει διαχωρισμένη πολλαπλασιαστική αναγωγή.
- $\lambda \notin \mathcal{R}$. Διαλέγουμε ακαίρεο $r \geq 1$ τέτοιο ώστε $\pi^r\lambda \in \mathcal{R}^*$. Τότε η αλλαγή μεταβλητών: $x = \pi^{-r}x', y = \pi^{-\frac{3r}{2}}y'$ (Αν χρειαστεί επεκτείνουμε το K στο K($\pi^{-\frac{3r}{2}}$)) δίνει:

  $$E : (y')^2 = x'(x' - \pi^r)(x' - \pi^r\lambda)$$

  γιά την E με ακεραίους συντελεστές $\Delta' \in \mathcal{M}, c_4' \in \mathcal{R}^*$ συνεπώς η καμπύλη έχει διαχωρισμένη πολλαπλασιαστική αναγωγή.

4. Οπως προηγουμένως υποθέτουμε οτι $\mathrm{char}(k) \neq 2$ και εκτείνουμε το K έτσι ώστε η E να έχει Weierstrass εξίσωση στην μορφή Legendre:

$$E : y^2 = x(x-1)(x-\lambda),\ \lambda \neq 0,1$$

Εξ υποθέσεως $j = j(E) \in \mathcal{R}$ και το λ σχετίζεται με την j μέσω της:

$$(1-\lambda(1-\lambda))^3 - j\lambda^2(1-\lambda)^2 = 0$$

Το j ομώς είναι ακέραιος και το λ ικανοποιεί μιά εξίσωση με συντελεστές ακεραίους αρα $\lambda \in \mathcal{R}$. Απο την άλλη $\lambda \neq 0, 1 mod \mathcal{M}$, άρα η δεδομένη εξίσωση του Legendre έχει καλή αναγωγή.

Αντιστρόφως, υποθέτουμε ότι η E έχει δυναμεί καλή αναγωγή. Εσ

τω K'/K πεπερασμένη επέκταση όπου η E/K' έχει καλή αναγωγή και $\mathcal{R}'$ ο αντίστοιχος δακτύλιος ακεραίων, Δ', c_4' οι σταθερές της E/K', αφού η E έχει καλή αναγωγή στο K', έχουμε ότι $\Delta' \in (\mathcal{R}')^*$ και συνεπώς

$$j(E) = (c_4')^3/\Delta' \in \mathcal{R}'$$

Ομως η E είναι ορισμένη υπέρ το K, άρα $j(E) \in K$, οπότε $j(E) \in \mathcal{R}' \cap K = \mathcal{R}$.

2.5 π-αδικά φίλτρα

Σκοπός αυτής της παραγράφου είναι η μελέτη του πυρήνα της αναγωγής, δηλαδή της ομάδας των σημείων που modulo $\pi\mathcal{R}$ μηδενίζονται, όπου $\mathcal{R}$ ο δακτύλιος των ακεραίων του K. Θα περιοριστούμε στα τοπικά σώματα που είναι πεπερασμένες επεκτάσεις του σώματος των p-αδικών αριθμών $\mathbb{Q}_p$. Εσω K ένα τέτοιο σώμα και έσω μιά ελλειπτική καμπύλη $C : Y^2 = X^3 + AX + B$ ορισμένη υπέρ το σώμα K. Χωρίς περιορισμό της γενικότητας υποθέτουμε ότι $\mathrm{A}, \mathrm{B} \in \mathcal{R}$. Εσω $\mathcal{B} := \mathrm{E}/K$ η ομάδα τών K-σημείων της C. Εχουμε δεί ότι το σύνολο των μη ιδιόμορφων σημείων της ανηγμένης στο σώμα $k = \mathcal{R}/\pi\mathcal{R}$ καμπύλης αποτελεί σε κάθε περίπτωση ομάδα και θα την συμβολίζουμε με $\bar{\mathcal{B}}^{(0)}$ ένω με $\bar{\mathcal{B}}$ θα συμβολίζουμε όλα τα σημεία της ανηγμένης καμπύλης, ιδιόμορφα και μη. Θεωρούμε $\mathcal{B}^{(0)}$ το σύνολο των σημείων της $\mathcal{B}$ τα οποία $\mathrm{mod}\pi\mathcal{R}$ ανάγονται στα $\bar{\mathcal{B}}^{(0)}$. Η συνάρτηση $\mathcal{B}^{(0)} \longrightarrow \bar{\mathcal{B}}^{(0)}$ είναι, λόγω του λήμματος του Hensel [Cas, κεφ.10], επι.

Η αναγωγή είναι επι πλέον ομομορφισμός ομάδων $\mathcal{B}^{(0)} \longrightarrow \bar{\mathcal{B}}^{(0)}$. Πράγματι αν $a, b, c \in \mathcal{B}$ με $a + b + c = 0$, αυτό σημαίνει ότι τα a, b, c ανήκουν στην τομή της καμπύλης C με μιά ευθεία L. Τότε όμως $\bar{a}, \bar{b}, \bar{c}$ ανήκουν στην τομή της ανηγμένης καμπύλης και της ευθείας $\bar{C} \cap \bar{L}$, οπότε θα έχουν και εκεί άθροισμα μηδέν.

Συνοψίζοντας έχουμε ότι $\mathcal{B}^{(0)}$ υποομάδα της $\mathcal{B}$ και υπάρχει επιμορφισμός ομάδων $\mathcal{B}^{(0)} \longrightarrow \bar{\mathcal{B}}^{(0)}$. Ο πυρήνας της αναγωγής είναι το σύνολο τών σημείων που απεικονίζονται στο $\bar{o}$, δηλαδή σε μη ομογενείς συντεταγμένες το o μαζί με τα $(x,y) \in \mathcal{B}$ με $x \notin \mathcal{R}, y \notin \mathcal{R}$, όπου με o ,$\bar{o}$ συμβολίζουμε τα ουδέτερα στοιχεία των ομάδων $\mathcal{B}^{(0)}$ και $\bar{\mathcal{B}}^{(0)}$ αντίστοιχα.

Αν $(x,y) \in \mathcal{B}$ και $x,y \notin \mathcal{R}$ τότε $|y|^2 = |x|^3$ (ultrametric ανισότητα) και έτσι $|x| = \pi^{2n}, |y| = \pi^{3n}$ γιά κάποιο $n \geq 1$. Αυτό το n θα το ονομάζουμε επίπεδο αναγωγής του (x,y). Αν (x,y), δεν ανήκει στον πυρήνα ή $(x,y) = o$ τότε το επίπεδο θα είναι εξ ορισμού 0 ή ∞ αντίστοιχα. Εστω $\mathrm{N} \geq 1$. Θεωρούμε τον μετασχηματισμό:

$$X_N = \pi^{2N} X, Y_N = \pi^{3N} Y, Z_N = Z.$$

Η εξίσωση της καμπύλης μετασχηματίζεται στην :

$$C_N : Y_N^2 Z_N = X_N^3 + \pi^{4N} A X_N Z_N^2 + \pi^{6N} B Z_N^3$$

Αν ξανακάνουμε αναγωγή $\mathrm{mod}\pi\mathcal{R}$ καταλήγουμε στην καμπύλη:

$$\bar{C}_N : Y_N^2 Z_N = X_N^3$$

Παρατηρούμε ότι ένα σημείο $(x,y) \in \mathcal{B}$ απεικονίζεται στο ιδιόμορφο σημείο $(0,0)$ αν το επιπεδό του είναι $< \mathrm{N}$ και είναι στον πυρήνα της αναγωγής της C_N αν το επίπεδο του είναι $> \mathrm{N}$. Τέλος η προσθετική ομάδα των μη ιδιόμορφων σημείων της $\bar{C}_N$ είναι η προσθετική ομάδα του $k = \mathcal{R}/\pi\mathcal{R}$. Εχουμε λοιπόν αποδείξει την

Πρόταση 2.13 *Αν με $\mathcal{B}^{(N)}$ συμβολίζουμε το σύνολο των σημείων του $\mathcal{B}$ με επίπεδο $\geq N$ τότε τα $\mathcal{B}^{(N)}$ είναι ομάδες και ισχύει:*

$$\mathcal{B} \supset \mathcal{B}^{(0)} \supset \mathcal{B}^{(1)} \supset ..... \supset \mathcal{B}^{(N)} \supset .....$$

και μάλιστα τα πηλίκα $\mathcal{B}^{(\mathrm{N})}/\mathcal{B}^{(\mathrm{N}+1)}$ γιά $\mathrm{N} \geq 1$ είναι γινόμενα κυκλικών ομάδων τάξης p.

<u>Παρατήρηση:</u> Εστω $(x,y) \in \mathcal{B}$ σημείο πεπερασμένης τάξης πρώτης προς τον p. Τότε $x,y \in \mathcal{R}$. Αλλιώς το (x,y) θα ήταν σε κάποιο επίπεδο $n \geq 1$. Τότε $(x,y) \in \mathcal{B}^{(n)}, (x,y) \notin \mathcal{B}^{(n+1)}$ και συνεπώς θα απεικονίζεται σε μη μηδενικό στοιχείο της $\mathcal{B}^{(n)}/\mathcal{B}^{(n+1)}$ που όλα τα στοιχεία της είναι τάξης p. Με άλλα λόγια ο πυρήνας της αναγωγής $\mathcal{B}^{(1)}$ δεν έχει σημεία τάξης πρώτης προς τον p.

Πρόταση 2.14 *Αν η ανηγμένη καμπύλη $\bar{C}$ είναι μη ιδιόμορφη $(m, char(k)) = 1$,τότε έχουμε την εμφύτευση: $C(\mathrm{K})[m] \hookrightarrow \tilde{C}(k)$.*

<u>Απόδειξη:</u>

Σε κάθε περίπτωση έχουμε την μικρή ακριβή ακολουθία:

$$0 \longrightarrow \mathcal{B}^{(1)} \longrightarrow \mathcal{B}^{(0)} \longrightarrow \bar{\mathcal{B}}^{(0)} \longrightarrow 0$$

όμως $\bar{\mathcal{B}}^{(0)} = \bar{\mathcal{B}}$ και $\mathcal{B}^{(0)} = \mathcal{B}$ συνεπώς η παραπάνω ακολουθία γράφεται:

$$0 \longrightarrow \mathcal{B}^{(1)} \longrightarrow \mathcal{B} \longrightarrow \bar{\mathcal{B}} \longrightarrow 0$$

δηλαδή με άλλα λόγια:

$$\mathcal{B} \cong \frac{\bar{\mathcal{B}}}{\mathcal{B}^{(1)}}$$

Σύμφωνα όμως με την προηγούμενη παρατήρηση η $\mathcal{B}^{(1)}$ δεν έχει στοιχεία τάξης m, από όπου λαμβάνουμε και την ζητούμενη εμφύτευση: $C(\mathrm{K})[m] \hookrightarrow \tilde{C}(k)$.

2.6 Καθολικά ελάχισια μοντέλα Weierstrass

Εστω E/K ελλειπτική καμπύλη. Τότε γιά κάθε v μη αρχιμήδεια εκτίμηση μπορούμε να βρούμε εξίσωση του Weierstrass γιά την E ,

$$Y_v^2 + a_{1,v}X_vY_v + a_{3,v}Y_v = X_v^3 + a_{2,v}X_v^2 + a_{4,v}X_v + a_{6,v}$$

που είναι ελάχιστη εξίσωση για την Ε στην θέση v. Εστω Δ_v η διακρίνουσα αυτής της εξίσωσης.

Ορισμός 2.15 *Η ελάχιστη διακρίνουσα της Ε/Κ είναι το ακέραιο ιδεώδες του Κ που δίνεται από :*

$$\mathcal{D}_{E/K} := \prod_v p_v^{ord_v(\Delta_v)}$$

όπου p_v το πρώτο ιδεώδες του R που αντιστοιχεί στην εκτίμηση v και το v διατρέχει όλες τις μη αρχιμήδειες εκτιμήσεις του R.

Συνεπώς η $\mathcal{D}_{E/K}$ καταγράφει την εκτίμηση της ελάχιστης διακρίνουσας του Ε σε κάθε μη αρχιμήδεια εκτίμηση και είναι ένα μέτρο του πόσο περίπλοκη είναι αριθμητικά η ελλειπτική καμπύλη Ε.

Το ερώτημα που τίθεται είναι κατά πόσο μπορούμε να βρούμε ελάχιστο μοντέλο εξίσωσης του Weierstrass, ταυτόχρονα γιά όλες τις μη-αρχιμήδειες εκτιμήσεις. Εστω

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

μιά εξίσωση του Weierstrass γιά την Ε/Κ με διακρίνουσα έστω Δ. Τότε γιά κάθε v μη αρχιμήδεια εκτίμηση μπορούμε να βρούμε μετασχηματισμό

$$X = u_v^2X_v + r_v, \;\; Y = u_v^3Y_v + s_vu_v^2X_v + t_v$$

ο οποίος να δίνει την ελάχιστη τοπική εξίσωση του Weierstrass. Οι δυό διακρίνουσες σχετίζονται μέσω της:

$$\Delta = u_v^{12}\Delta_v$$

οπότε αν ορίσουμε ιδεώδες, εξαρτώμενο απο το Δ, από την σχέση:

$$A_\Delta := \prod_v p_v^{-ord_v(u_v)}$$

τότε έχουμε

$$\mathcal{D}_{E/K} = \Delta A_\Delta^{12}$$

Λήμμα 2.16 *Με τόν παραπάνω συμβολισμό, η κλάση ιδεωδών του* K *που αντισοιχεί στο* A_Δ *είναι ανεξάρτητη της* Δ.

<u>Απόδειξη:</u> Θεωρούμε μια άλλη εξίσωση του Weierstrass με διακρίνουσα Δ'. Τότε $\Delta = u^{12}\Delta'$ όπου $u \in K^*$, οπότε

$$(\Delta')A_{\Delta'}^{12} = \mathcal{D}_{E/K} = (\Delta)A_\Delta^{12} = (\Delta')[(u)A_\Delta]^{12}$$

συνεπώς ισχύει:

$$A'_\Delta = (u)A_\Delta$$

δηλαδή τα ιδεώδη: A'_Δ, A_Δ ανήκουν στην ίδια κλάση ιδεωδών του K.

Ορισμός 2.17 *Η κλάση ιδεωδών του* A_Δ *θα λέγεται κλάση του Weierstrass της* E/K *και συμβολίζεται με* $A_{E/K}$.

Ορισμός 2.18 *Μία εξίσωση του Weierstrass*

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

της ελλειπτικής καμπύλης E/K *τέτοια ώστε* $a_1, a_2, a_3, a_4, a_6 \in R$ *της οποίας η διακρίνουσα* Δ *παράγει το ιδεώδες* $\mathcal{D}_{E/K} = (\Delta)$, *θα λέγεται καθολική εξίσωση του Weierstrass.*

Πρόταση 2.19 *Υπάρχει καθολική ελάχιστη εξίσωση του Weierstrass γιά την* E/K *ανν* $A_{E/K}$*=(1).*

Απόδειξη: Ας υποθέσουμε ότι η E/K έχει μια καθολικά ελάχιστη εξίσωση έστω με διακρίνουσα Δ. Τότε $\mathcal{D}_{E/K} = (\Delta)$ οπότε

$$12 ord_v(A_\Delta) = ord_v(\mathcal{D}_{E/K}) - ord_v(\Delta) = 0$$

άρα καιʼανάγκη $\mathrm{A}_\Delta = (1)$ συνεπώς η κλάση του $\mathrm{A}_{E/K} = (1)$. Αντιστρόφως, υποθέτουμε ότι $A_{E/K} = (1)$. Διαλέγουμε μία εξίσωση του Weierstrass γιά την E/K με συντελεστές $a_i \in R$ και διακρίνουσα Δ. Οπως προηγουμένως, γιά κάθε μη-αρχιμήδεια εκτίμηση v θεωρούμε τον μετασχηματισμό

$$X = u_v^2 X_v + r_v, \;\; Y = u_v^3 Y_v + s_v u_v^2 X_v + t_v$$

ο οποίος μας δίνει τοπικά (ως προς v) ελάχιστη εξίσωση. Εστω $a_{i,v}$ οι συντελεστές αυτής της εξίσωσης και Δ_v η διακρίνουσα της. Μπορούμε να υποθέσουμε ότι γιά όλες εκτός από πεπερασμένο πλήθος εκτιμήσεων v έχουμε $u_v = 1, r_v = s_v = t_v = 0$ και έστω S το σύνολο αυτό. Επιπλέον όλα τα u_v, r_v, s_v, t_v είναι v-ακέραια. Εξ ορισμού $\mathrm{A}_{E/K} = 1$ σημαίνει ότι το ιδεώδες

$$\prod_v p_v^{ord_v(u_v)}$$

είναι κύριο με γεννήτορα $u \in K^*$. Τότε όμως $ord_v(u) = ord_v(u_v)$ γιά όλες τις μη αρχιμήδειες εκτιμήσεις. Από το θεώρημα υπολοίπων του κινέζου έχουμε ότι $\exists\ r, s, t \in R$ τέτοια ώστε για τις πεπερασμένες στο πλήθος εκτιμήσεις του S να έχουμε:

$$ord_v(r - r_v), ord_v(s - s_v), ord_v(t - t_v) > max_{i=1,2,3,4,6}\{ord_v(u_v^i a_{i,v})\}$$

Τώρα θεωρούμε την εξίσωση του Weierstrass γιά την E/K που δίνεται από την αλλαγή συντεταγμένων:

$$X = u^2 X' + r, \;\; Y = u^3 Y' + s u_v^2 X' + t$$

η οποία έχει συντελεστές a_i' και διακρίνουσα Δ'. Επειδή $\Delta = u^{12}\Delta'$, έχουμε:

$$ord_v(\Delta') = ord_v(u^{-12}\Delta) = ord_v(\left(\frac{u_v}{u}\right)^{12}\Delta_v) = ord_v(\Delta_v).$$

Η εξίσωση του Weierstrass της E/K που προκύπτει με τον τελευταίο μετασχηματισμό είναι μιά καθολική εξίσωση του Weierstrass γιά την E/K. Αυτό που απομένει να δείξουμε είναι το ότι τα a_i' είναι v-ακέραια $\forall v \in S$ το οποίο ισχύει αφού τα a_i' είναι πολυώνυμα των $r, s, t, a_1, ..., a_6$. Πράγμαιι έτσι γιά παράδειγμα έχουμε:

$$ord_v(u^2 a_2') = ord_v(a_2 - sa_1 + 3r + s^2) = ord_v[u_v^2 a_{2,v} - (s - s_v)(a_1 + s + s_v) + 3(r - r_v)] = ord_v(u_v^2 a_{2,v})$$

όπου η τελευταία γραμμή προκύπτει από την προηγούμενη λόγω εκλογής των r, s και την μη αρχιμήδεια φύση της v. Επιπλέον ισχύει $ord_v(u) = ord_v(u_v)$ και $ord_v(a_{2,v}) \geq 0$ από τα οποία προκύπτει το ζητούμενο αποτέλεσμα.

Πόρισμα 2.20 *Αν ο αριθμός κλάσεων $h_K = 1$ τότε κάθε ελλειπτική καμπύλη έχει καθολική εξίσωση του Weierstrass.*

2.7 Η αλγεβρική δομή της ομάδας $E(K)$

Θα κλείσουμε το κεφάλαιο αυτό παραθέτοντας μερικά πολύ σημαντικά θεωρήματα γιά την δομή της ομάδας των ρητών σημείων μιας ελλειπτικής καμπύλης.

Θεώρημα 2.21 *(Mordell-Weil) Η ομάδα $E(K)$ όπου K αλγεβρικό σώμα αριθμών είναι πεπερασμένα παραγόμενη αβελιανή ομάδα δηλαδή:*

$$E(K) = E_{tor}(K) \times \mathbb{Z}^r.$$

Απόδειξη: [Av4] Ο αριθμός r ονομάζεται τάξη (rank) της ελλειπτικής καμπύλης και είναι πολύ δύσκολο να υπολογιστεί. Γιά την υποομάδα στρέψης ισχύει το περίφημο:

Θεώρημα 2.22 *(Mazur) Αν $E/\mathbb{Q}$ η ομάδα των ρητών σημείων μιάς ελλειπτικής καμπύλης τότε η ομάδα στρέψης $E_{tor}(\mathbb{Q})$ είναι μία από τις παρακάτω 15 ομάδες:*

$$\begin{array}{ll} \frac{\mathbb{Z}}{N\mathbb{Z}} & \text{με } 1 \leq N \leq 10 \text{ ή } \mathrm{N} = 12 \\ \frac{\mathbb{Z}}{2\mathbb{Z}} \times \frac{\mathbb{Z}}{2N\mathbb{Z}} & \text{με } 1 \leq N \leq 4 \end{array}$$

Ολες οι παραπάνω ομάδες είναι δυνατόν να προκύψουν ως ομάδες στρέψης κάποιας ελλειπτικής καμπύλης ορισμένης υπέρ το $\mathbb{Q}$.

Απόδειξη: [Maz1],[Maz2]

3 Modular καμπύλες και μορφές

3.1 L-σειρές ελλειπτικών καμπύλων

Σκοπός αυτής της παραγράφου είναι ο ορισμός και η μελέτη του αναλόγου των L-σειρών αλγεβρικών σωμάτων αριθμών στα σώματα συναρτήσεων αλγεβρικών πολλαπλοτήτων και συγκεκριμένα ελλειπτικών καμπύλων. Θα χρειαστούμε λίγα στοιχεία της δομής του δακτυλίου ενδομορφισμών, $End(E)$ της ελλειπτικής μας καμπύλης.

3.1.1 Ισογένειες

Εστω $T = \mathbb{C}/L$, $T' = \mathbb{C}/L'$ δυό ελλειπτικές καμπύλες, ορισμένες υπέρ το $\mathbb{C}$. Μιά ισογένεια μεταξύ τους θα είναι κάθε μη μηδενικός αναλυτικός ισομορφισμός $\lambda : T \longrightarrow T'$. Η έννοια της ισογένειας ταυτίζεται με την ύπαρξη μιγαδικού αριθμού λ τέτοιου ώστε: $\lambda \cdot L \subset L'$. Ο πυρήνας του λ υπολογίζεται $ker(\lambda) \simeq \lambda^{-1}L'/L \simeq L'/(\lambda L)$ και είναι πεπερασμένη υποομάδα βαθμού $n = [L' : \lambda L]$. Παρατηρούμε ότι ισχύει:

$$nL' \subset \lambda L \subset L'$$

δηλαδή ορίζεται η δυική ισογένεια:

$$n/\lambda : T' = \mathbb{C}/L' \longrightarrow \mathbb{C}/L = T$$

την οποία θα συμβολίζουμε με $\hat{\lambda}$. Επιπλέον διαπιστώνουμε ότι $\lambda \circ \hat{\lambda} = n$ δηλαδή η σύνθεση αντιστοιχεί σε πολλαπλασιασμό με τον φυσικό n.

Οπως παρατηρούμε η ισογένεια λ επάγει μιά εμφύτευση στα σώματα ελλειπτικών συναρτήσεων των T, T' δηλαδή $\lambda^* : Ell(L') \longrightarrow Ell(L)$ η οποία είναι επέκταση Galois με ομάδα Galois την $\lambda^{-1}L'/L = ker(\lambda)$ και επιπλέον ισχύει :

$$[Ell(L) : Ell(L')] = \sharp(\lambda^{-1}L'/L) = [L' : \lambda L]$$

Η παραπάνω παρατήρηση μας δίνει την δυνατότητα να ορίσουμε ισογένειες στην γενική περίπτωση όπου οι ελλειπτικές καμπύλες ορίζονται πάνω από οποιοδήποτε σώμα.

Ορισμός 3.1 *Εστω E, E' δυό ελλειπτικές καμπύλες ορισμένες στο σώμα k. Μιά ισογένεια $\lambda : E \longrightarrow E'$ είναι ένας μορφισμός υπέρ τον k με $\lambda(0) = 0$. Ορίζουμε σαν βαθμό της ισογένειας τον βαθμό της επέκτασης των αντιστοίχων σωμάτων ελλειπτικών συναρτήσεων: $deg(\lambda) = [k(E) : k(E')]$. Ο βαθμός της παραπάνω επέκτασης είναι το γινόμενο των βαθμών διαχωρισιμότητας και πλήρους αδιαχωρισιμότητας δηλαδή:*

$$deg(\lambda) = [k(E) : k(E')]_s[k(E) : k(E')]_i = deg(\lambda)_s \cdot deg(\lambda)_i.$$

Γιά να ορίσουμε την δυική ισογένεια στην περίπτωση του γενικού σώματος θα μελετήσουμε την δράση της λ στην όμαδα των διαιρετών:

Ορισμός 3.2 *Μιά ισογένεια $\lambda : E \longrightarrow E'$ ορίζει ένα μορφισμό ομάδων*

$$\lambda : Div(E) \longrightarrow Div(E')$$

ως εξής: $\lambda(\sum n_p P) := \sum n_p \lambda(P)$ και το παρακάτω διάγραμμα είναι μεταθετικό:

$$\begin{array}{ccc} Div_0(E) & \xrightarrow{\lambda} & Div_0(E') \\ \downarrow s & & s \downarrow \\ E(k) & \xrightarrow{\lambda} & E'(k) \end{array}$$

όπου Div_0 η ομάδα των διαιρετών βαθμού 0 και s η συνάρτηση που στέλνει ένα διαιρέτη βαθμού 0 στην ελλειπτική καμπύλη ως εξής: $s(\sum n_P P) = \sum n_P P \in E(k)$, ο πυρήνας της s είναι η ομάδα των κυρίων διαιρετών.

Επιπλέον λ ορίζει την $\lambda^{-1} : Div_0(E') \longrightarrow Div_0(E)$ ως εξής:

$$\lambda^{-1}(\sum n_P P) := \sum n_P \lambda^{-1}(P),$$

όπου $\lambda^{-1}(P) := m(Q_1 + ... + Q_r)$ γιά $\{Q_1, ..., Q_r\} = \lambda^{-1}(P)$ οι αντίστροφες εικόνες συνολοθεωρητικά και $mr = deg(\lambda)$. Αυτή η κατασκευή επάγει την δυική ισογένεια η οποία ορίζεται έτσι ώστε το παρακάτω διάγραμμα να είναι μεταθετικό:

$$\begin{array}{ccc} Div_0(E') & \xrightarrow{\lambda^{-1}} & Div_0(E) \\ \downarrow s & & s \downarrow \\ E'(k) & \xrightarrow{\hat{\lambda}} & E(k) \end{array}$$

Γιά ισογένειες σε οποιοδήποτε σώμα ισχύει το παρακάτω:

Θεώρημα 3.3 *Η συνάρτηση $\lambda \longrightarrow \hat{\lambda}$ είναι μορφισμός ομάδων $Hom(E, E') \longrightarrow Hom(E', E)$ που επιπλέον ικανοποιεί: $\hat{\hat{\lambda}} = \lambda$, $deg(\lambda) = deg(\hat{\lambda})$, $\hat{\lambda} \cdot \lambda = n$ στον $End(E)$ και $\lambda \cdot \hat{\lambda} = n$ στον $End(E')$. Η ενέλιξη $\lambda \longmapsto \hat{\lambda}$ του δακτυλίου $End(E)$ ικανοποιεί $\hat{n} = n$ όπου $deg(n) = n^2$. Η συνάρτηση βαθμού*

$$deg : Hom(E, E') \longrightarrow \mathbb{Z}$$

είναι θετική τετραγωνική μορφή δηλαδή

- $deg(\lambda) \geq 0$ *και* $deg(\lambda) = 0$ *ανν* $\lambda = 0$
- $deg(m\lambda) = m^2 deg(\lambda)$
- $deg(\lambda + \mu) = deg(\lambda) + (\hat{\lambda}\mu + \hat{\mu}\lambda) + deg(\mu)$

Θα περιορίσουμε την μελέτη μας τώρα στον δακτύλιο $End(E) = Hom(E, E)$ ο οποίος δεν έχει μηδενοδιαιρέτες αφού αν $\mu\lambda = 0$ τότε $deg(\mu\lambda) = deg(\mu) \cdot deg(\lambda)$ συνεπώς $deg(\lambda) = 0 \Rightarrow \lambda = 0$ ή $deg(\mu) = 0 \Rightarrow \mu = 0$. Στην ειδική περίπτωση που η ελλειπτική καμπύλη είναι ορισμένη στο $\mathbb{C}$ τότε έχουμε ότι ο δακτύλιος των ενδομορφισμών είναι το $\{\lambda \in \mathbb{C} : \lambda L \subset L\}$ συνεπώς υποδακτύλιος του $\mathbb{C}$, οπότε η μη ύπαρξη μηδενοδιεραιτων είναι προφανής.

Ορισμός 3.4 *Ορίζουμε το ίχνος ενός ενδομορφισμού $\lambda \in End(E)$, $tr(\lambda) := \lambda + \hat{\lambda}$ και το χαρακτηριστικό του πολυώνυμο το $r_\lambda := t^2 - tr(\lambda)t + deg(\lambda)$.*

Παρατηρούμε ότι η συνθήκη της τετραγωνικότητας του βαθμού εκφράζεται και ως $deg(\lambda + \mu) = deg(\lambda) + tr(\hat{\lambda}\mu) + deg(\mu)$.

Πρόταση 3.5 *Το ίχνος του ενδομορφισμού λ στον $End(E)$ ανήκει στον υποδακτύλιο $\mathbb{Z}$ του $End(E)$ και το $r_\lambda \in \mathbb{Z}[t]$. Επιπλέον $r_\lambda(\lambda) = 0$.*

Απόδειξη: υπολογίζουμε ότι $deg(1+\lambda) = (1+\lambda)(1+\hat{\lambda}) = 1+tr(\lambda)+\lambda\hat{\lambda}$ και αφού $deg(\lambda) \in \mathbb{Z}$ έχουμε το ζητούμενο αποτέλεσμα. Τέλος παρατηρούμε ότι $r_\lambda(\lambda) = \lambda^2 - (\lambda + \hat{\lambda})\lambda + \lambda\hat{\lambda} = 0$.

Δηλαδή δείξαμε ότι γιά κάθε ελλειπτική καμπύλη υπεράνω οποιοδήποτε σώματος κάθε στοιχείο του δακτυλίου $End(E)$ ικανοποιει μιά τετραγωνική εξίσωση υπέρ τον υποδακτυλίο $\mathbb{Z}$.

Ορισμός 3.6 *Μιά ελλειπτική καμπύλη έχει μιγαδικό πολλαπλασιασμό ανν $\mathbb{Z} \neq End(E)$.*

3.1.2 Ζήτα συναρτήσεις ελλειπτικών καμπύλων σε πεπερασμένα σώματα

Εστω $E : y^2 = x^3 - Ax - B$ ελλειπτική καμπύλη με $A, B \in \mathbb{Z}$. Θεωρούμε την ελλειπτική καμπύλη στο σώμα $\mathbb{F}_q$, όπου $q = p^n$, $p \in \mathbb{P}$, δηλαδή $E_q : y^2 = x^3 - \bar{A}x - \bar{B}$ ορίζει ελλειπτική καμπύλη στο $\mathbb{F}_q$, ανν p δεν διαιρεί το Δ. Σε ότι ακολουθεί θα θεωρούμε μόνο τέτοιους πρώτους. Εστω N_{q^m} ο αριθμός των σημείων της $E_q(\mathbb{F}_{q^m})$. Ορίζουμε την συνάρτηση:

$$Z(E_p, u) := exp\left(\sum_{m=1}^{\infty} N_{q^m}\frac{u^m}{m}\right)$$

την όποια την θεωρούμε είτε ως τυπική δυναμοσειρά είτε ως συνάρτηση μιγαδικής μεταβλητής με ακτίνα σύγκλισης q^{-2}. Πράγματι για τον υπολογισμό της ακτίνας σύγκλισης παρατηρούμε ότι

$$N_{q^s} \leq \frac{q^{3s} - 1}{q^s - 1} < (2+1)q^{2s} \Rightarrow |u| \leq q^{-2}$$

Εστω k η αλγεβρική κλειστότητα του $\mathbb{F}_q$.

Ορισμός 3.7 *Εστω $K = \mathbb{F}_q$, $q = p^s$, όπου $p \in \mathbb{P}(\mathbb{Z})$. Εστω $C(K)$ αλγεβρική καμπύλη ορισμένη υπέρ το K, ορίζουμε την καμπύλη $C^{(q)}(K)$ περιγράφοντας το ομογενές ιδεώδες της ως: $I(C^{(q)})$ είναι το ιδεώδες που γεννάται από τα $\{f^{(q)} : f \in I(C)\}$, όπου $f^{(q)}$ είναι το πολυώνυμο που ορίζεται υψώνωντας κάθε συντελεστή του στην $q^{\text{στή}}$ δύναμη. Επιπλέον ορίζουμε τον αυτομορφισμό του Frobenius:*

$$\Phi : C \longrightarrow C^{(q)}$$

$$\Phi([x_0, ..., x_n]) = [x_0^q, ..., x_n^q].$$

Η παραπάνω συνάρτηση είναι καλά ορισμένη, πράγματι αν $P = [x_0, ..., x_n] \in C$, πρέπει να δείξουμε ότι $\Phi(P)$ είναι ρίζα κάθε γεννήτορα $f^{(q)}$ του $I(C^{(q)})$. Πράγματι

$$f^{(q)}(\Phi(P)) = f^{(q)}(x_0^q, ..., x_n^q) = [f(x_0, ..., x_n)]^q = 0.$$

Θεώρημα 3.8 *Γιά τον αυτομορφισμό του Frobenius Φ ισχύει ότι :*

- $\Phi^* K(C^{(q)}) = K(C)^q := \{f^q : f \in K(C)\}$
- Φ *είναι πλήρως μη-διαχωρίσιμος*
- $deg\Phi = q$

Απόδειξη:

- Το σώμα $K(C)$ είναι πηλίκα ομογενών πολυωνύμων του ιδίου βαθμού και $\Phi^* K(C^{(q)})$ είναι το υπόσωμα του που αποτελείται από τα:

  $$\Phi^*(f/g) = f(x_0^q, ..., x_n^q)/g(x_0^q, ..., x_n^q),$$

  από την άλλη το σώμα $K(C)^q$ αποτελείται από τα πηλίκα

  $$f(x_0, ..., x_n)^q/g(x_0, ..., x_n)^q$$

  όμως το K είναι τέλειο οπότε όπως είδαμε στην απόδειξη του θεωρήματος (1.24) κάθε στοιχείο του K είναι μία q δύναμη, άρα

  $$(\mathrm{K}[x_0, ..., x_n])^q = K[x_0^q, ..., x_n^q]$$

  από όπου προκύπτει άμεσα και ο ισχυρισμός του θεωρήματος.
- Προφανώς λόγω του προηγούμενου.
- Εσιω t τοπική συντεταγμένη σε κάποιο ομαλό σημείο $P \in C$, οπότε λόγω του θεωρήματος 1.24 έχουμε ότι $K(C)$ διαχωρίσιμη αλγεβρική επέκταση υπέρ το $K(t)$, σχηματίζουμε λοιπόν το ακόλουθο διάγραμμα επεκτάσεων σωμάτων:

K(C)

q(t)

διαχωρίσιμη K(C) πλήρως

μη διαχωρίσιμη

q

K(t) K(C)

Συνεπώς $K(C) = K(C)^q(t)$ άρα $deg\Phi = [K(C)^q(t) : K(C)^q]$ έχουμε ότι $t^q \in K(C)^q$. Γιά να δείξουμε ότι $deg\Phi = q$ αρκεί να δείξουμε ότι $t^{q/p} \notin K(C)^q$. Το τελευταίο ισχύει αφού αν $t^{q/p} = f^q$ με $f \in K(C)$ τότε $q/p = ord_P(t^{q/p}) = q\ ord_P(f)$ το οποίο είναι προφανώς αδύνατο.

Περιοριζόμαστε τώρα στην περίπτωση ελλειπτικών καμπύλων, γιά τον

$$\Phi : E \longrightarrow E$$

$$\Phi(x, y) = (x^q, y^q).$$

ισχυεί ότι ο $\Phi \in End(E)$, έχει βαθμό q και είναι πλήρως μη-διαχωρίσιμος. Επιπλέον το σημείο $(x, y) \in E(\mathbb{F}_q)$ ανν $\Phi(x, y) = (x, y)$ δηλαδή ανν $(x, y) \in ker(1_E - \Phi)$. Αφού το διαφορικό της $1_E - \Phi$είναιίσομε1_E ο ενδομορφισμός $1_E - \Phi \in End(E)$ είναι διαχωρίσιμος[Si,σελ.35]. Συνεπώς

$$\mathrm{N}_1 = \sharp E(\mathbb{F}_q) = deg(1 - \Phi) = \deg(\Phi) - tr(\Phi) + 1 = 1 + q - tr(\Phi)$$

Ομως,από το θεώρημα 3.3 έχουμε: $m^2 - mntr(\Phi) + n^2 q = deg(n - m\Phi) \geq 0 \quad \forall \ \ m, n$. Επωμένως $tr(\Phi)^2 - 4deg(\Phi) \leq 0$ ή $|tr(\Phi)| \leq 2\sqrt{q}$. Αν $\alpha, \bar{\alpha}$ οι δυό συζυγείς μιγαδικές ρίζες του πολυωνύμου $1 - a_p T + qT^2$, όπου $a_p := tr(\Phi)$, τότε $|\alpha| = |\bar{\alpha}| = q^{1/2}$. Αποδείξαμε επομένως το θεώρημα:

Θεώρημα 3.9 *(Υπόθεση Riemann γιά ελλειπτικές καμπύλες). Εστω E μιά ελλειπτική καμπύλη ορισμένη σε ένα πεπερασμένο σώμα $\mathbb{F}_q$, και έστω $N_m := \sharp E(\mathbb{F}_{q^m})$. Τότε γιά όλα τα $m \geq 1$ έχουμε*

$$|1 + q^m - N_m| \leq 2 \cdot q^{m/2}.$$

Θεώρημα 3.10 *Εστω E μιά ελλειπτική καμπύλη ορισμένη σε ένα πεπερασμένο σώμα $\mathbb{F}_q$. Το χαρακτηριστικό πολυώνυμο του αυτομορφισμού του Frobenius της E είναι:*

$$f_E(T) = deg(1 - \Phi T) = 1 - tr(\Phi)T + qT^2 \in \mathbb{Z}[T]$$

και η ζήτα συνάρτηση αυτής είναι η ρητή συνάρτηση :

$$Z(E_q, q^{-s}) = \frac{f_E(q^{-s})}{(1 - q^{-s})(1 - q^{1-s})} = \frac{1 - tr(\Phi)q^{-s} + q^{1-2s}}{(1 - q^{-s})(1 - q^{1-s})}.$$

Απόδειξη: Γνωρίζουμε ότι $N_m = 1 + q^m - Tr(\Phi^m) = 1 + q^m - \alpha^m - \bar{\alpha}^m$ όπου α και $\bar{\alpha}$ είναι οι δυό φανταστικές συζυγείς ρίζες του χαρακτηριστικού πολυωνύμου $deg(1 - \Phi T)$. Κάνοντας χρήση της παραπάνω σχέσης υπολογίζουμε τον λογάριθμο της $Z(E_q, q^{-s})$:

$$\begin{aligned} \log Z(E_q, q^{-s}) &= \textstyle\sum_{m=1}^{\infty}(1 + q^m - \alpha^m - \bar{\alpha}^m)q^{-ms}/m \\ &= 1/m(\textstyle\sum_{m=1}^{\infty} q^{-ms} + \sum_{m=1}^{\infty} q^{-m(s-1)} - \sum_{m=1}^{\infty}(\alpha q^{-s})^m - \sum_{m=1}^{\infty}(\bar{\alpha} q^{-s})^m) \\ &= -\log(1 - q^{-s}) - \log(1 - q^{1-s}) + \log[(1 - \alpha q^{-s})(1 - \bar{\alpha} q^{-s})]. \end{aligned}$$

οπότε το εκθετικό της παραπάνω έκφρασης είναι η $Z(E_p, q^{-s})$ και εύκολα βλέπουμε ότι :

$$Z(E_q, q^{-s}) = \frac{1 - (\alpha + \bar{\alpha})q^{-s} + q^{1-2s}}{(1 - q^{-s})(1 - q^{1-s})} = \frac{f_E(q^{-s})}{(1 - q^{-s})(1 - q^{1-s})}.$$

Παρατήρηση: Η ζήτα συνάρτηση έχει πόλους στα $s = 0$ και $s = 1$. Η υπόθεση Riemann

$$|1 + q^m - N_m| \leq 2 \cdot q^{m/2}$$

είναι ισοδύναμη με το ότι οι ρίζες της $f_E(T)$ είναι μιγαδικές συζυγείς η μιά της άλλης, και ότι έχουν απόλυτη τιμή ίση με $1/\sqrt{q}$ δηλαδή η $\zeta_E(s)$ έχει ρίζες μόνο πάνω στην ευθεία $Re(s) = 1/2$, όπου $\zeta_E(s) := Z(E_q, q^{-s})$

Επιπλέον αν στην $f_E(q^{-s}) = 1 - tr(\Phi)q^{-s} + q^{1-2s}$ αντικαταστήσουμε το s με το $1 - s$ τότε καταλήγουμε στην :

$$f_E(q^{-(1-s)})1 - tr(\Phi)q^{s-1} + q^{2s-1} = q^{2s-1}(1 - tr(\Phi)q^{-s} + q^{1-2s}) = q^{2s-1} f_E(q^{-s}).$$

Απο την παραπάνω συναρτησιακή εξίσωση γιά το f_E και το αναλλοίωτο του παρονομαστή υπό τον μετασχηματισμό $s \longrightarrow s - 1$ έχουμε την επόμενη:

Πρόταση 3.11 *Η ζήτα συνάρτηση $\zeta_E(s)$ της E στο πεπερασμένο σώμα $\mathbb{F}_q$ ικανοποιεί την παρακάτω συναρτησιακή εξίσωση:*

$$\zeta_E(1 - s) = q^{2s-1}\zeta_E(s).$$

Παρατήρηση: Εχουμε ότι : $N_p = p + 1 - a_p \Rightarrow N_{p^m} = p^m + 1 - \alpha^m - \bar{\alpha}^m$. Συνεπώς ο υπολογισμός του N_p καθορίζει το a_p, δηλαδή αρκεί να γνωρίζουμε το πλήθος των σημείων $mod\ p$ γιά να γνωρίζουμε το πλήθος των σημείων $mod\ p^m$ γιά όλα τα $m \geq 1$.

Οπως παρατήρησε ο E.Artin ο παραπάνω ορισμός είναι ανάλογος του ορισμού L-σειρών αλγεβρικών σωμάτων αριθμών:[Av2] Θεωρούμε την ακεραία περιοχή των πολυωνύμων μιάς μεταβλητής με συντελεστές από το σώμα $\mathbb{F}_p$ και το σώμα πηλίκων αυτής $\mathbb{F}_p(X)$. Επιπλέον θεωρούμε την αλγεβρική επέκταση του, $K := \mathbb{F}_p(X)(\sqrt{x^3 - Ax - B})$ και έστω D η ακεραία θήκη του $\mathbb{F}_p[X]$ στο K, δηλαδή τα στοιχεία του K που ικανοποιούν μονικά πολυώνυμα με συντελεστές στο $\mathbb{F}_p[X]$. Ο D είναι δακτύλιος του Dedekind και κάθε μη μηδενικό ιδεώδες είναι πεπερασμένου δείκτη στον D. Αν $I \subset D$ είναι μη μηδενικό ιδεώδες ορίζουμε νόρμα του $N(I) = |D/I|$. Οπως έχουμε ήδη παρατηρήσει τα μέγιστα ιδεώδη αντιστοιχούν ένα προς ένα με τους πρώτους διαιρέτες. Ας θεωρήσουμε την αλγεβρική κλειστότητα k του πεπερασμένου σώματος $\mathbb{F}_p$ και έστω ένα σημείο $P \in E(k)$. Το σημείο αυτό προφανώς θα ορίζεται σε κάποια επέκταση $\mathbb{F}_{p^n}$ του $\mathbb{F}_p$ και έστω $deg(P) = n$ ο βαθμός της ελάχιστης επέκτασης που το P ορίζεται. Αν σ ο γεννήτορας της κυκλικής ομάδας Galois $Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)$ τότε το σημείο

$$\mathcal{P} := P + P^{\sigma} + ... + P^{\sigma^{n-1}}$$

είναι πρώτος διαιρέτης ορισμένος στο σώμα $\mathbb{F}_p$ και επιπλέον όλοι οι πρώτοι διαιρέτες θα είναι αυτής της μορφής και η νόρμα τους θα ισούται με $N\mathcal{P} = p^n$. Σε αντίθεση με τον ορισμό της ομάδας διαιρετών θα συμβολίζουμε ένα θετικό διαιρέτη πάνω από το $\mathbb{F}_p$ πολλαπλασιαστικά, δηλαδή

$$\mathcal{A} = \mathcal{P}_1^{n(1)}....\mathcal{P}_r^{n(r)}$$

όπου $n(i)$ φυσικοί αριθμοί και $\mathcal{P}_i$ πρώτοι διαιρέτες ορισμένοι υπέρ το $\mathbb{F}_p$. Τότε η νόρμα του $\mathcal{A}$ ορίζεται ώς:

$$N\mathcal{A} = (\mathrm{N}\mathcal{P}_1)^{n(1)}.....(N\mathcal{P}_r)^{n(r)}$$

Ορισμός 3.12 *Αν E ελλειπτική καμπύλη ορισμένη στο $\mathbb{F}_p$ τότε ορίζουμε την συνάρτηση:*

$$\zeta'_E(s) := \sum_{\text{θετικοί } \mathcal{A}} (N\mathcal{A})^{-s} = \prod_{\text{πρώτοι } \mathcal{P}} \frac{1}{(1-(N\mathcal{P})^{-s})}$$

Πρόταση 3.13 *Ισχύει: $\zeta_E(s) = \zeta'_E(s)$.*

<u>Απόδειξη:</u> Εστω ότι A_m συμβολίζει τον αριθμό των θετικών διαιρετών ορισμένων στο $E(\mathbb{F}_p)$ με νόρμα p^m και έστω ότι με P_m συμβολίζουμε τον αριθμό των πρώτων διαιρετών ορισμένων στο $E(\mathbb{F}_p)$ με νόρμα p^m έχουμε ότι:

$$Z_E(u) = \sum_{m=0}^{\infty} A_m u^m = \prod_{m=0}^{\infty} (1-u^m)^{-P_m}$$

όπου $\mathrm{Z}_{\mathbf{E}}(q^{-s}) = \zeta'_E(s)$. Αν N_m είναι το πλήθος των σημείων στην $E(\mathbb{F}_{p^m})$ τότε από την περιγραφή των πρώτων διαιρετών του $\mathbb{F}_p(E)$, έχουμε ότι :

$$N_m = \sum_{d|m} dP_d$$

υπολογίζουμε την

$$\frac{d}{du}\log Z_E(u) = \frac{1}{u}\sum_{d=1}^{\infty}\frac{dP_d u^d}{1-u^d} = \frac{1}{u}\sum_{d,d'} dP_d u^{dd'} = \frac{1}{u}\sum_{m=1}^{\infty} N_m u^m$$

και ολοκληρώνοντιας και πέρνοντιας το εκθετικό της παραπάνω έκφρασης καταλήγουμε στο ότι

$$Z_E(u) = Z(E_p, u)$$

το οποίο δίνει το ζητούμενο αποτέλεσμα.

Ορίσαμε το $\zeta(E_p, s)$ γιά πρώτους p που δεν διαιρούν το Δ. Γιά πρώτους αριθμούς διαιρέτες του Δ ορίζουμε :

$$f_E(T) = \left\{ \begin{array}{ll} 1 - T & \text{αν έχω ιδιομορφία τύπου διαχωρισμένου κόμβου} \\ 1 + \mathrm{T} & \text{αν έχω ιδιομορφία τύπου μη διαχωρισμένου κόμβου} \\ 1 & \text{αν έχω ιδιομορφία τύπου ακίδας.} \end{array} \right\}$$

Από τις τοπικές ζ συναρτήσεις ορίζουμε την καθολική ζ συνάρτηση ως το γινόμενο όλων των τοπικών:

$$\zeta(E, s) = \prod_{p \in \mathbb{P}(\mathbb{Z})} \zeta(E_p, s)$$

Από το ορισμό βλέπουμε ότι:

$$\zeta(E, s) = \zeta(s)\zeta(s-1)L(E, s)^{-1}$$

όπου

$$L(E, s) = \prod_{p \not| \Delta} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \prod_{p | \Delta} \frac{1}{1 - \epsilon p^{-s}},$$

όπου $\epsilon = 1, -1, 0$ αντίστοιχα, με την περίπτωση της $f_E(T)$. Το παραπάνω απειρογινόμενο θα το ονομάζουμε L-σειρά της ελλειπτικής καμπύλης E. Από τον τύπο $|\alpha| = p^{1/2}$ έχουμε την σύγκλιση της $L(E, s)$ γιά $Res > 3/2$. Πράγμαι η σειρά :

$$\sum_{p \in \mathbb{P}} |\alpha p^{-s}| \leq \sum_{p \in \mathbb{P}} p^{1/2} p^{-s} < \sum_{n=1}^{\infty} \frac{1}{n^{s-1/2}}$$

η οποία συγκλίνει ανν $Res > 3/2$ και η σύγκλιση του παραπάνω αθροίσματος μας δίνει την σύγκλιση του απειρογινομένου που ορίζει την L-σειρά.

<u>Παρατήρηση:</u> Τα κυριότερα προβλήμαια που τίθενται σχετικά με μιά L-σειρά είναι αυτά της αναλυτικής επέκτασης και συναρτησιακής εξίσωσης καθώς και το πρόβλημα της εύρεσης ριζών και τιμών σε δεδομένα σημεία. Γιά το πρόβλημα των ριζών η υπόθεση Riemann δίνει την απάντηση η οποία στην περίπτωση των L-σειρών προβολικών αλγεβρικών πολλαπλοτήτων αποδείχθηκε από τον P.Deligne το 1973. Το πρόβλημα της αναλυτικής επέκτασης L-σειρών ονομάζεται γιά ιστορικούς λόγους νόμος αντιστροφής. Γιά μιά σύνδεση των L-σειρών ελλειπτικών καμπύλων με μιγαδικό πολλαπλασιασμό και τον κυβικό και διτετραγωνικό νόμο αντιστροφής παραπέμπουμε στον [I-R, κεφ.18], ενώ γιά μιά "φιλοσοφικού" επιπέδου συζήτηση γιά τις L-σειρές στον [Lg]. Γιά την περίπτωση πάντως των L-σειρών ελλειπτικών καμπύλων ο νόμος αντιστροφής εκφράζεται από την εικασία Taniyama-Shimura την οποία θα διατυπώσουμε σε επόμενη παράγραφο.

Οπως παρατηρήσαμε στην παράγραφο 2.7 η εύρεση του $rank E(\mathbb{Q})$ είναι ένα πολύ δύσκολο πρόβλημα. Μία απάντηση δίνουν οι παρακάτω εικασίες:

Εικασία 3.14 *Η L-σειρά $L(E, s)$ κάθε ελλειπτικής καμπύλης $E/\mathbb{Q}$ επεκτείνεται αναλυτικά σε όλο το μιγαδικό επίπεδο.*

Εικασία 3.15 *(Birch και Swinnerton-Dyer) Υποθέτοντας την αλήθεια της εικασίας 3.14, ο rank$E(\mathbb{Q})$ ισούτε με την τάξη της ρίζας της $L(E,s)$ στο 1.*

Σχετικά με την εικασία των Birch και Swinnerton-Dyer έχουν αποδειχθεί τα παρακάτω:[Ko]

Θεώρημα 3.16 *(Coates Wiles 1977) Αν η E έχει μιγαδικό πολλαπλασιασμό και $L(E,1) \neq 0$ τότε η $E(\mathbb{Q})$ είναι πεπερασμένη.*

Θεώρημα 3.17 *(Gross-Zagier 1986) Αν η E είναι modular και η $L(E,s)$ έχει απλή ρίζα στο $s=1$ τότε η $E(\mathbb{Q})$ είναι άπειρη. Ο ορισμός της modular ελλειπτικής καμπύλης θα δοθεί σε επόμενο κεφάλαιο.*

3.2 Οι επιφάνειες Riemann $X_0(N)$

Θα ξεκινήσουμε με την ταξινόμιση των στοιχείων της $GL_2^+(\mathbb{R})$ ανάλογα με την δράση τους στο υπερβολικό επίπεδο $\mathbb{H}$.

Ορισμός 3.18 *Αν $\sigma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2^+(\mathbb{R})$ τότε το σ δρα στο $\mathbb{H}$ ως εξής:*

$$\sigma(z) = \frac{az+b}{cz+d} \quad \forall \;\; z \in \mathbb{H}$$

επιπλέον γιά την τιμή ∞ ορίζουμε το $\sigma(\infty) = \lim_{x \longrightarrow \infty} \sigma(ix)$

Η κλάση των μετασχηματισμών αυτών διατηρεί τον προσανατολισμό και δρα στο πάνω μιγαδικό επίπεδο $\mathbb{H}$ αφού:

$$Im\frac{az+b}{cz+d} = (ad-cb)\frac{Imz}{|cz+d|^2}$$

<u>Παρατήρηση:</u> Η παραπάνω δράση δεν είναι πιστή. Προς τούτο θεωρούμε την ομάδα $PGL_2^+(\mathbb{R}) := GL_2^+(\mathbb{R})/ZGL_2^+(\mathbb{R})$ ή οποία δρα πιστά στο $\mathbb{H}$. (Με $ZGL_2^+(\mathbb{R})$ συμβολίζουμε το κέντρο της $GL_2^+(\mathbb{R})$ δηλαδή τους μετασχηματισμούς της μορφής $\lambda \cdot 1_2,\ \lambda \in \mathbb{R}^*$.)

Τα στοιχεία της $GL_2^+(\mathbb{R})$ χωρίζονται σε υπερβολικά, ελλειπτικά και παραβολικά ανάλογα με την τιμή της διακρίνουσας του χαρακτηριστικού πολυωνύμου του στοιχείου, δηλαδή $D = trA^2 - 4detA$. Ενα στοιχείο θα λέγεται υπερβολικό αν $D > 0$, παραβολικό αν $D = 0$ και ελλειπτικό αν $D < 0$. Γιά τις ανάγκες μας θα περιοριστούμε σε υποομάδες της $SL_2(\mathbb{Z})$ και συγκεκριμένα στις:

$$\Gamma_0(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad \in SL_2(\mathbb{Z})/c \equiv 0 mod N. \right\}$$

$$\Gamma(N) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \quad \in SL_2(\mathbb{Z})/\begin{bmatrix} a & b \\ c & d \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} mod N \right\}$$

Προφανώς έχουμε τους εγκλεισμούς:

$$\Gamma(N) \subseteq \Gamma_0(N) \subseteq SL_2(\mathbb{Z})$$

<u>Παρατήρηση:</u> Αφού γιά $\gamma \in SL_2(\mathbb{Z})$, $det(\gamma) = 1$ έχουμε την παρακάτω συνθήκη: το $\gamma \neq \pm 1_2$ είναι υπερβολικό αν $|tr(\gamma)| < 2$, παραβολικό αν $tr(\gamma) = \pm 2$ και ελλειπτικό αν $|tr(\gamma)| > 2$.

Ορισμός 3.19 *Τα σημεία του υπερβολικού επιπέδου $\mathbb{H} \cup \mathbb{R} \cup \infty$ που παραμένουν αναλλοίωτα υπό κάποιο ελλειπτικό στοιχείο της $\Gamma_0(N)$ ονομάζονται ελλειπτικά, ένω αυτά που παραμένουν αναλλοίωτα από κάποιο παραβολικό στοιχείο ονομάζονται παραβολικά ή $cusp$ σημεία, ως προς την υποομάδα $\Gamma_0(N)$.*

Παρατηρούμε ότι το γ_1 και το $\gamma^{-1}\gamma_1\gamma \quad \forall \gamma \in SL_2(\mathbb{Z})$ έχουν την ίδια διακρίνουσα D. Συνεπώς αν $z \in \mathbb{H} \cup \mathbb{R} \cup \infty$ είναι παραβολικό (αντίστοιχα ελλειπτικό σημείο) τότε κάθε $\gamma \in SL_2(\mathbb{Z})$ μεταφέρει το z σε παραβολικό (αντίστοιχα ελλειπτικό σημείο), ως προς την υποομάδα $\gamma^{-1}\Gamma_0(N)\gamma$.

Τα παραβολικά σημεία του $\mathbb{H} \cup \mathbb{R} \cup \infty$, ως προς την $SL_2(\mathbb{Z})$ είναι τα $\{\infty\} \cup \mathbb{Q}$. Πράγματι παρατηρούμε ότι

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \infty = \frac{\infty + 1}{1} = \infty$$

δηλαδή το ∞ είναι παραβολικό σημείο και επιπλέον $SL_2(\mathbb{Z})(\infty) = \mathbb{Q} \cup \{\infty\}$.

Γιά τα ελλειπτικά σημεία z έχουμε ότι η ομάδα ισοτροπίας τους δηλαδή η ομάδα $\Gamma_0(N)_z := \{\gamma \in \Gamma_0(N)/\gamma z = z\}$ είναι πεπερασμένη κυκλική. Πράγματι έσιω $\tau \in SL_2(\mathbb{R})$ τέτοιο ώστε $\tau(i) = z$, παρατηρούμε ότι $\Gamma_0(N)_z = \tau SO(2)\tau^{-1} \cap \Gamma_0(N)$ αφού η ομάδα ισοτροπίας του i είναι η $SO(2) \cap \Gamma_0(N)$ όπου $SO(2) := \{\alpha \in SL_2(\mathbb{R})/ \quad \alpha^t\alpha = 1_2\}$. Ομως $\Gamma_0(N)$ διακριτή και $SO(2)$ συμπαγής άρα η τομή είναι διακριτή ομάδα. Επιπλέον έχουμε ότι $SO(2) \cong \mathbb{R}/\mathbb{Z} \cong S^1$ και όλες οι διακριτές υποομάδες του είναι πεπερασμένες κυκλικές.

Γιά τα παραβολικά σημεία της $\Gamma_0(N)$ έχουμε ότι η ομάδα ισοτροπίας είναι άπειρη κυκλική. Πράγματι γιά $s \in \mathbb{R} \cup \infty$ ορίζουμε τα :

$$\begin{aligned} F(s) &:= \{\alpha \in SL_2(\mathbb{R})/\alpha(s) = s\} \\ P(s) &:= \{\alpha \in F(s)/\alpha \quad \text{παραβολικό} \quad \text{ή} \quad \pm 1_2\} \end{aligned}$$

και υπολογίζουμε εύκολα:

$$\begin{aligned} F(\infty) &= \left\{ \begin{bmatrix} a & b \\ 0 & a^{-1} \end{bmatrix} /a \in \mathbb{R}^*, b \in \mathbb{R} \cup \infty \right\} \\ P(\infty) &= \left\{ \pm \begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix} /h \in \mathbb{R} \right\} \simeq \mathbb{R} \times \{\pm 1_2\} \end{aligned}$$

Συνεπώς αν s παραβολικό σημείο υπάρχει $\gamma \in SL_2(\mathbb{Z})$ τέτοιο ώστε

$$P(s) = \gamma^{-1}P(\infty)\gamma \simeq \mathbb{R} \times \{\pm 1_2\}$$

Η ομάδα $P(s)\cap\Gamma_0(N))/(\Gamma_0(N)\cap\{\pm 1_2\})$ είναι ισόμορφη με μιά μη τετριμμένη διακριτή υποομάδα του $\mathbb{R}$ και συνεπώς με το $\mathbb{Z}$. Συνεπώς αρκεί να δείξουμε ότι $\Gamma_0(N)\cap P(s)$ είναι ισόμορφη με την $\Gamma_0(N)_s$ δηλαδή αρκεί να δείξουμε ότι τα στοιχεία της $\Gamma_0(N)_s$ είναι $\pm 1_2$ ή παραβολικά. Χωρίς περιορισμό της γενικότητας ας υποθέσουμε ότι $s=\infty$. Εστω

$$\sigma = \begin{bmatrix} \pm 1 & h \\ 0 & \pm 1 \end{bmatrix}$$

γεννήτορας της ομάδας $P(s)\cap\Gamma_0(N)$. Αν η $\Gamma_0(N)_s$ περιέχει υπερβολικό στοιχείο

$$\tau = \begin{bmatrix} a & b \\ 0 & a^{-1} \end{bmatrix}$$

(χωρίς περιορισμό της γενικότητας $|\alpha|<1$) τότε το στοιχείο

$$\tau\sigma\tau^{-1} = \sigma = \begin{bmatrix} \pm 1 & a^2 h \\ 0 & \pm 1 \end{bmatrix} \in P(s)\cap\Gamma_0(N).$$

Ομως αυτό δεν γίνεται αφού $|a^2h|<|h|$ συνεπώς $\Gamma_0(N)\cap\{\pm 1_2\}=\Gamma_0(N)_s$.

Ορισμός 3.20 *(Θεμελιώδης περιοχή αντιπροσώπων) Εστω Γ διακριτή υποομάδα της ομάδας $SL_2(\mathbb{Z})$. Ενα ανοιχτό υποσύνολο R_Γ του $\mathbb{H}$ θα λέγεται θεμελιώδης περιοχή της Γ αν πληρεί τις παρακάτω ιδιότητες:*

- *Διαφορετικά σημεία του R_Γ δεν είναι ισοδύναμα ως προς την δράση της Γ,*
- *Αν $\tau\in\mathbb{H}\ \ \exists\ \tau'\in\bar{R}_\Gamma$ τέτοιο ώστε $\tau'\sim\tau$ ως προς την δράση της Γ.*

Στην περίπτωση που $\Gamma=SL_2(\mathbb{Z})$ τότε σαν θεμελιώδη περιοχή $R_{SL_2(\mathbb{Z})}$ μπορούμε να θεωρήσουμε τα $\tau\in\mathbb{H}$ που ικανοποιούν τις ανισότητες

$$|\tau|>1 \quad , \quad |\tau+\bar{\tau}|<1$$

[Ap, σελ 32]

Θα εφοδιάσουμε το πηλικοσύνολο $\Gamma_0(N)\backslash\mathbb{H}$ με την δομή επιφάνειας Riemann. Ορίζουμε $\mathbb{H}^*:=\mathbb{H}\cup\mathbb{Q}\cup\{\infty\}$. Στον χώρο $\mathbb{H}^*$ προσαρτούμε την παρακάτω τοπολογία: βασικά ανοιχτά σημείου του $\mathbb{H}$ είναι ανοιχτοί δίσκοι εξολοκλήρου εντός του $\mathbb{H}$, ενώ στο ∞ βασικά ανοιχτά είναι σύνολα της μορφής $\{z\in\mathbb{H}\quad /Im(z)>r\}\bigcup\{\infty\}$ (μεταφέρουμε την τοπολογία του $0\in\mathbb{C}$ μέσω της συνάρτησης $e^{-2\pi i z}$), τέλος στα ρητά σημεία x μεταφέρουμε την τοπολογία του ∞ μέσω του στοιχείου της $SL_2(\mathbb{Z})$ που απεικονίζει το ∞ στο x οπότε βασική οικογένεια ανοιχτών είναι οι εφαπτόμενοι δίσκοι στο x που βρίσκονται εντός του $\mathbb{H}$.

Ο πηλικοχώρος $X_0(N):=\Gamma_0(N)\backslash\mathbb{H}^*$ είναι Hausdorff και συμπαγής [Sh,κεφ 1]. Επιπλέον παρατηρούμε ότι η φυσική προβολή $\pi:\mathbb{H}^*\longrightarrow X_0(N)$ είναι ανοιχτή συνάρτηση. Πράγματι αν V ανοιχτό στον $\mathbb{H}^*$ τότε :

$$\pi^{-1}(\pi(V)) = \bigcup_{\gamma\in\Gamma_0(N)} \gamma(V)$$

ανοιχτό.

Γιά να εισάγουμε σύστημα χαρτών $\{(U_z,\phi_z)/z \in \mathbb{H}^*\}$ στον $X_0(N)$ και θεωρούμε τις παρακάτω περιπτώσεις:

(a) $z_0 \in \mathbb{H}$ διαλέγουμε περιοχή V_z, όπως είδαμε προηγουμένως, και $U_{z_0} = \pi(V_{z_0})$ είναι ανοιχτό του $X_0(N)$.

- Αν η ομάδα ισοτροπίας $\Gamma_0(N)_{z_0} = \{\pm 1_2\}$, τότε ο $\pi : V_{z_0} \longrightarrow U_{z_0}$ είναι ομοιομορφισμός, και αν ϕ_{z_0} ο αντίστροφός του, τότε $(U_{z_0}\phi_{z_0})$ είναι ο ζητούμενος χάρτης του σημείου z_0.
- Αν η ομάδα ισοτροπίας $\Gamma_0(N)_{z_0} \neq \{\pm 1_2\}$, θα είναι πεπερασμένης τάξης και το στοιχείο z_0 θα είναι ελλειπτικό δηλαδή $\Gamma_0(N)_{z_0}$ κυκλική και μάλιστα τάξης $2n$ (εύκολα μπορούμε να δούμε ότι το n είναι 2 ή 3). Εστω

$$\lambda : \mathbb{H} \longrightarrow \{z \in \mathbb{C}/|z| \leq 1\}$$

ορισμένη ως: $\lambda(z) = (z - z_0)/(z - \bar{z}_0)$. Τότε $\phi_{z_0} : U_{z_0} \longrightarrow \mathbb{C}$ ορίζεται από $\phi_{z_0}(\pi(z_{z_0})) = \lambda(z_{z_0})^n$ και (U_{z_0}, ϕ_{z_0}) είναι ο ζητούμενος χάρτης.

(b) Η περίπτωση του παραβολικού στοιχείου: Γνωρίζουμε ότι η ομάδα $SL_2(\mathbb{Z})$ δρά μεταβατικά στα παραβολικά σημεία, έστω λοιπόν $\beta \in SL_2(\mathbb{Z})$ με $\beta(z_0) = \infty$. Εχουμε ότι

$$\beta\Gamma_0(N)_{z_0}\beta^{-1} = \left\{\pm \begin{bmatrix} 1 & mh \\ 0 & 1 \end{bmatrix} /m \in \mathbb{Z}\right\}$$

όπου h ορίζεται σαν το πλάτος ή ο δείκτης διακλάδωσης του z_0. Θεωρούμε τον παρακάτω χάρτη $\Gamma_0(N)_{z_0}\backslash U_{z_0}, \phi$ όπου

$$\phi : \Gamma_0(N)_{z_0}\backslash U_{z_0} \longrightarrow \mathbb{C}$$

$$z \longmapsto e^{2\pi i\beta(z)/h}$$

Αποδυκνείεται ότι οι παραπάνω χάρτες είναι συμβατοί μεταξύ τους και συνεπώς ορίζουν μιγαδική δομή στο $X_0(N) = \Gamma_0(N)\backslash\mathbb{H}^*$.

Παρατήρηση: Τα ελλειπτικά σημεία είναι τα σημεία διακλάδωσης της προβολής

$$\pi : \mathbb{H}^* \longrightarrow X_0(N).$$

3.3 Αυτόμορφες συναρτήσεις και μορφές

Ορισμός 3.21 *Θα ονομάζουμε αυτόμορφη κάθε συνάρτηση*

$$f : \mathbb{H} \longrightarrow \mathbb{C}$$

που είναι $\Gamma_0(N)$ περιοδική, δηλαδή κάθε συνάρτηση που γράφεται ώς σύνθεση $f = g \circ \pi$, όπου π η φυσική προβολή $\mathbb{H}^* \longrightarrow \Gamma_0(N)\backslash\mathbb{H}^*$ και g μερόμορφη συνάρτηση της επιφάνειας Riemann $X_0(N)$.

Μια περισσότερο γενική έννοια από αύτην της αυτόμορφης συνάρτησης είναι της αυτόμορφης μορφής. Εστω $\sigma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in GL_2(\mathbb{R})$ και $z \in \mathbb{C}$ θέτουμε

$$j(\sigma, z) = cz + d$$

τότε αποδεικνύουμε εύκολα ότι

$$j(\sigma\tau, z) = j(\sigma, \tau(z)) \cdot j(\tau, z),$$
$$\frac{d}{dz}\sigma(z) = det(\sigma) \cdot j(\sigma, z)^{-2}$$

Για κάθε ακέραιο $k, \sigma \in GL_2^+(\mathbb{R})$ και κάθε συνάρτηση f ορισμένη στο $\mathbb{H}$ γράφουμε:

$$f|[\sigma]_k := det(\sigma)^{k/2} \cdot f(\sigma(z)) \cdot j(\sigma, z)^{-k}.$$

Τέλος διαπιστώνουμε ότι:

$$f|[\sigma\tau]_k = (f|[\sigma]_k)|[\tau]_k.$$

<u>Παρατήρηση:</u> Παρά το ότι και οι δυό μετασχηματισμοί $\sigma, -\sigma$ δρουν στο $\mathbb{H}$ με τον ίδιο τρόπο αντίθετα στην δράση επί συναρτήσεων γιά k περριτό έχουμε:

$$j(-\sigma, z)^k = -j(\sigma, z)^k \quad \text{και συνεπώς}$$

$$f|[-\sigma]_k = -f|[\sigma]_k.$$

Αντίθετα γιά k άρτιο οι δράσεις των $[\sigma]_k, [-\sigma]_k$ ταυτίζονται.

Ορισμός 3.22 *Εστω k ακέραιος. Μιά συνάρτηση $f : \mathbb{H} \longrightarrow \mathbb{C}$ θα λέγεται αυτόμορφη μορφή βάρους k ως προς την ομάδα $\Gamma_0(N)$, αν η f πληρεί τις παρακάτω συνθήκες:*

- *f είναι μερόμορφη στο $\mathbb{H}$,*
- *$f|[\gamma]_k = f$ γιά όλα τα $\gamma \in \Gamma_0(N)$,*
- *f είναι μερόμορφη σε κάθε παραβολικό σημείο της $\Gamma_0(N)$.*

Το ακριβές νόημα της παραπάνω συνθήκης είναι το εξής: Εστω z ένα παραβολικό σημείο της $\Gamma_0(N)$ και έστω $\rho \in SL_2(\mathbb{Z})$ τέτοιο ώστε $\rho(z) = \infty$. Θέτοντας $\Gamma_0(N)_z = \{\gamma \in \Gamma_0(N) | \gamma(z) = z\}$ έχουμε :

$$\rho\Gamma_0(N)_z\rho^{-1} \cdot \{\pm 1\} = \left\{ \pm \begin{bmatrix} 1 & h \\ 0 & 1 \end{bmatrix}^m / m \in \mathbb{Z} \right\}$$

γιά κάποιο θετικό ακέραιο h. Συνεπώς η $f|[\rho^{-1}]_k$ είναι αναλλοίωτη κάτω από τον μετασχηματισμό $z \longrightarrow z + h$ και λόγω περιοδικότητας υπάρχει μερόμορφη συνάρτηση $F(q)$ στην περιοχή $0 < |q| < r$ όπου r θετικός πραγματικός αριθμός τέτοιος ώστε:

$$f|[\rho^{-1}]_k = F(e^{2\pi i z/h})$$

Η τελευταία συνθήκη απαιτεί η F να είναι μερόμορφη συνάρτηση στο $q = 0$.
<u>Παρατήρηση:</u> Το $\{-1\} \in \Gamma_0(N)$, συνεπώς δεν έχουμε μη τετριμμένες αυτόμορφες μορφές περιττού βάρους. Πράγματι θα έπρεπε $f = f|[-1]_k = -f$ οπότε $f = 0$.

Ορισμός 3.23 *Το ανάπτυγμα της F ως δυναμοσειράς Laurent του $q = e^{2\pi iz/h}$, που έχει την παρακάτω μορφή:*

$$f|[\rho^{-1}]_k = \sum_{n\geq n_0} c_n e^{2\pi niz/h}$$

θα ονομάζεται ανάλυση Fourier της f στο z, ενώ οι συντελεστές c_n θα ονομάζονται συντελεστές Fourier της f.

Ορισμός 3.24 *Μιά αυτόμορφη μορφή f της $\Gamma_0(N)$ θα λέγεται ακέραια αν το ανάπτυγμα Fourier της σε κάθε παραβολικό σημείο ξεκινά από το μηδέν, ενώ αν ξεκινά από το ένα θα λέγεται παραβολική μορφή. Θα συμβολίζουμε τις ακέραιες μορφές βάρους k με $M_k(\Gamma_0(N)$ και τις παραβολικές με $S_k(\Gamma_0(N))$.*

Διαπιστώνουμε εύκολα ότι ο ελάχιστος όρος που ξεκινά η σειρά Fourier είναι ανεξάρτητος του αντιπροσώπου του παραβολικού σημείου που επιλέγουμε στην κλάση ισοδυναμίας που ορίζει η δράση της ομάδας $\Gamma_0(N)$.

Οπως είδαμε προηγουμένως οι αυτόμορφες συναρτήσεις αποτελούν το σώμα των μερόμορφων συναρτήσεων της επιφάνειας Riemann $X_0(N)$. Για τις αυτόμορφες μορφές βάρους 2 ισχύει η παρακάτω

Πρόταση 3.25 *Υπάρχει αμφιμονοσήμαντη αντιστοιχία μεταξύ των ολόμορφων 1-μορφών της επιφάνειας Riemann $X_0(N)$ και των παραβολικών μορφών βάρους 2.*

Απόδειξη: Θεώρουμε την φυσική προβολή $\pi : \mathbb{H}^* \longrightarrow \Gamma_0(N)\backslash\mathbb{H}^* = X_0(N)$ και έστω ω ολόμορφη 1-μορφή της $X_0(N)$. Θεωρούμε την 1-ολόμορφη διαφορική μορφή του καθολικού καλύμματος $\mathbb{H}$, $\pi^*\omega = \omega \circ \pi$. Η $\pi^*\omega$ γράφεται ώς $\pi^*\omega = f(z)dz$. Επιπλέον παρατηρούμε ότι η $\pi^*\omega$ είναι αναλλοίωτη ως προς την δράση της $\Gamma_0(N)$.

$$f(z)dz = \pi^*\omega = \pi^*\omega \circ \gamma = f(\gamma z)d\gamma z = f(\gamma z)j(\gamma, z)^{-2}dz$$

συνεπώς $f|[\gamma]_2 = f$. Θεωρούμε τον πίνακα $T^m = \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix}$ όπου m είναι ο δείκτης διακλάδωσης της $\Gamma_0(N)$ στο ∞. Αφου η $\pi^*\omega$ είναι αναλλοίωτη από τον T^m έχουμε

$$f(z) = f_\infty(q^{1/m}) = \sum a_n q^{n/m} = \sum a_n e^{2\pi niz/m}$$

όπου f_∞ δυναμοσειρά ως προς την μεταβλητή $q^{1/m} = e^{2\pi iz/m}$ και

$$d(q^{1/m}) = q^{1/m}\frac{2\pi i}{m}dz.$$

Αρα

$$f(z)dz = f_\infty(q^{1/m})\frac{md(q^{1/m})}{2\pi iq^{1/m}}$$

όπου $q^{1/m}$ τοπική παράμετρος στο ∞. Συνεπώς $\pi^*\omega$ ολόμορφο στο ∞ ανν f_∞ έχει ρίζα στο ∞ δηλαδή είναι δυναμοσειρά της μορφής

$$f_\infty(q^{1/m}) = \sum_{n=1}^{\infty} a_n q^{n/m}$$

Εστω z ένα παραβολικό σημείο της $\Gamma_0(N)$ και $\alpha \in SL_2(\mathbb{Z})$ τέτοιο ώστε $\alpha(z) = \infty$ τότε η $\pi^*\omega \circ \alpha^{-1}$ είναι ολόμορφη στο ∞ και μπορεί να γραφεί ως

$$\pi^*\omega \circ \alpha^{-1}(z) = h(z)dz$$

γιά κάποια ολόμορφη h ορισμένη στο $\mathbb{H}$. Κάνοντας την ίδια ανάλυση όπως προηγουμένως διαπιστώνουμε την ανάγκη μηδενισμού της h σε κάθε παραβολικό σημείο.

Εστω $f \in S_k(\Gamma_0(N))$ μιά παραβολική (cusp) μορφή και έστω $f(\tau) = \sum_{n=1}^{\infty} c_n q^n$ το ανάπτυγμα της στο παραβολικό σημείο ∞, $q = e^{2\pi i\tau}, Im(\tau) > 0$. Η L-σειρά της f ορίζεται σαν η σειρά Dirichlet:

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

και εύκολα πιστοποιούμε ότι (μετασχηματισμός Mellin)

$$\int_0^\infty f(i\sigma)\sigma^s \frac{d\sigma}{\sigma} = (2\pi)^{-s}\Gamma(s)L(s,f)$$

γιά όλες τις τιμές του σ που το ολοκλήρωμα ορίζεται.

Λήμμα 3.26 *Εστω $f \in S_k(\Gamma_0(N))$ με q ανάπτυγμα στο ∞, $f(\tau) = \sum_{n=1}^{\infty} c_n q^n$. Τότε:*

- *η συνάρτηση $h(\tau) := |f(\tau)|\sigma^{k/2}$ είναι φραγμένη στο $\mathbb{H}$ και αναλλοίωτη υπό την δράση της $\Gamma_0(N)$,*
- *Υπάρχει σταθερά M τέτοια ώστε $|c_n| \le Mn^{k/2}$, $forall\ n \in \mathbb{N}$.*

Απόδειξη:

- Ορίζουμε την συνάρτηση $h(\tau) = h(\rho + i\sigma) = |f(\tau)|\sigma^{k/2}$ όπου $\tau = \rho + i\sigma$. Γνωρίζουμε ότι $Im(\gamma(\tau)) = Im(\tau)|j(\gamma,\tau)|^{-2}$ γιά όλα τα $\gamma \in SL_2(\mathbb{Z})$. Επιπλέον $\forall\ \gamma \in \Gamma_0(N)$ ισχύει ότι: $h(\gamma\tau) = f(\gamma\tau)Im(\gamma\tau) = j(\gamma,\tau)^2 f(\gamma\tau)Im(\tau)\cdot j(\gamma,\tau)^{-2}$, δηλαδή η h είναι αναλλοίωτη ως προς την δράση της $\Gamma_0(N)$. Αν s είναι ένα παραβολικό σημείο της $\Gamma_0(N)$ υπάρχει $\beta \in SL_2(\mathbb{Z})$ τέτοιο ώστε $\beta(\sigma) = \infty$ και τοπική συντεταγμένη $q = e^{2\pi i\tau/h}$ έτσι ώστε:

  $$f|[\beta^{-1}]_k = \Phi(q),$$

  όπου Φ ολόμορφη συνάρτηση στο $0 < |q| < r$ με $r > 0$. Εχουμε λοιπόν:

  $$h(\beta^{-1}(\tau)) = \Phi(q)(Im\beta^{-1}\tau)^{k/2}$$

  και αφού η f είναι παραβολική μορφή έχουμε $\Phi(q) \to 0$ καθώς $q \to 0$. Συνεπώς $h(w) \to 0$ καθώς $w \to s$, ως προς την τοπολογια της $\mathbb{H}^*$. Δηλαδή η h είναι συνεχής συνάρτηση ορισμένη στην συμπαγή επιφάνεια Riemann $\Gamma_0(N)\backslash\mathbb{H}^*$, συνεπώς είναι φραγμένη.

- οι συντελεστές c_n υπολογίζονται από τον τύπο :

$$c_n = \frac{1}{2\pi i}\int_{|q|=r} f(q)q^{-n-1}dq \text{ γιά μικρό } r>0$$

$$\text{αν } Im(\tau)=\sigma=\frac{h}{2\pi n} \text{ τότε } |e^{2\pi i\tau/h}|=e^{-1/n}$$

και επιπλέον ισχύει: $|f(q)|\leq M\sigma^{-k/2}$ αρκεί $r=e^{-1/n}$. Συνεπώς έχουμε την εκτίμηση

$$|c_n|\leq Mn^{k/2}.$$

Θεωρούμε το στοιχείο $a_N := \begin{bmatrix} 0 & -1 \\ N & 0 \end{bmatrix}$ αν $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ τότε

$$a_N\gamma a_{\mathrm{N}}^{-1} = \begin{bmatrix} d & -c/N \\ -Nb & a \end{bmatrix}.$$

Συνεπώς $a_N\Gamma_0(N)a_N^{-1}\subseteq\Gamma_0(N)$. Γιά $f\in M_k(\Gamma_0(N))$, θεωρούμε την συνάρτηση

$$w_N(f)=f|[a_N]_k$$

και γιά $\gamma\in\Gamma_0(N)$ έχουμε ότι

$$(f|[a_N]_k)|[\gamma]_k = (f|[a_N\gamma a_N^{-1}]_k)|[a_N]_k = f|[a_N]_k$$

δηλαδή η $w_N(f)$ είναι αυτόμορφη $\Gamma_0(N)$ μορφή ιδίου βάρους και επιπέδου με την f.

Πρόταση 3.27 *Η συνάρτηση w_N απεικονίζει το $M_k(\Gamma_0(N))$ και το $S_k(\Gamma_0(N))$ στους εαυτούς τους.*

Απόδειξη: Εστω $f\in M_k(\Gamma_0(N))$. Αυτό σημαίνει ότι γιά κάθε $\beta\in SL_2(\mathbb{Z})$ η συνάρτηση $f|[\beta^{-1}]_k$ έχει ολόμορφο q_N ανάπτυγμα στο ∞ ,όπου $q_N=e^{2\pi i\tau/N}$. Θα πρέπει να δείξουμε ότι το ίδιο ισχύει και γιά την $w_N(f)=f|[\alpha_N]_k$, δηλαδή ότι η

$$f|[\alpha_N]_k|[\beta^{-1}]_k$$

έχει ολόμορφο q_N ανάπτυγμα γιά όλα τα $\beta\in SL_2(\mathbb{Z})$. Εύκολα παρατηρούμε ότι υπάρχει $\gamma\in SL_2(\mathbb{Z})$ τέτοιο ώστε :

$$\alpha_N\cdot\beta^{-1}=\gamma^{-1}\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

με $a\cdot d=N$ και $0\leq b<d$. Οπότε το ανάπτυγμα γράφεται ώς:

$$f|[\alpha_N]_k|[\beta^{-1}]_k = (N^{-1/2}d)^{-k}\sum_{n=0}^{\infty} c_n e^{2\pi inb/Nd}e^{2\pi ina^2\tau/N^2}$$

αφού έχουμε

$$f|[\gamma^{-1}]_k(\tau)=\sum_{n=0}^{\infty}c_n e^{2\pi in\tau/N}.$$

Συνεπώς έχουμε απλά πολλαπλασιασμό των συντελεστών με ρίζες της μονάδας που δεν επηρεάζουν τον ελάχιστο μη μηδενικό όρο στο ανάπτυγμα Fourier.

Παρατηρούμε ότι $(\frac{1}{\sqrt{N}}a_N)^2 = -I$ συνεπώς η w_N είναι μιά ενέλιξη στους χώρους $M_k(\Gamma_0(N))$ και $S_k(\Gamma_0(N))$. Οι παραπάνω χώροι συνεπώς διαχωρίζονται ως τα αθροίσματα των ιδιόχωρων των ιδιοτιμών $+1$ και -1. Στην περίπτωση του $S_k(\Gamma_0(N))$ θα συμβολίζουμε τους παραπάνω ιδιόχωρους με $S_k^{\pm}(\Gamma_0(N))$.

Θεώρημα 3.28 *(Hecke) Εστω $f \in S_k(\Gamma_0(N))$ μιά παραβολική μορφή σε ένα από τους ιδιόχωρους $S_k^{\epsilon}(\Gamma_0(N))$ της w_N, όπου $\epsilon = \pm 1$. Τότε η L-σειρά $L(s,f)$ ορίζεται αρχικά γιά $Re(s) > k/2+1$ και επεκτείνεται σε ακεραία συνάρτηση του $\mathbb{C}$. Επιπλέον η συνάρτηση:*

$$\Lambda(s,f) := N^{s/2}(2\pi)^{-s}\Gamma(s)L(s,f)$$

ικανοποιεί την συναρτησιακή εξίσωση:

$$\Lambda(s,f) = \epsilon(-1)^{k/2}\Lambda(k-s,f).$$

<u>Απόδειξη:</u> από το λήμμα 3.26 έχουμε την αρχική εκτίμηση της σύγκλισης γιά $Re(s) > k/2+1$. Αφού $w_N f = \epsilon f$ ο νόμος αντιστροφής της f υπό την δράση της w_N είναι :

$$f\left(\frac{i}{N\sigma}\right) = \epsilon N^{k/2} i^k \sigma^k f(i\sigma).$$

Από την σχέση του μετασχηματισμού Mellin έχουμε ότι:

$$\Lambda(s,f) = N^{s/2}\int_0^{\infty} f(i\sigma)\sigma^{s-1}d\sigma. \qquad \text{(α)}$$

Λόγω των εκτιμήσεων του λήμματος 3.26 έχουμε ότι το ολοκλήρωμα:

$$\int_{1/\sqrt{N}}^{\infty} f(i\sigma)\sigma^{s-1}d\sigma$$

συγλίνει για όλα τα $s \in \mathbb{C}$ και ορίζει μιά ακέραια συνάρτηση. Ξαναγράφουμε την (α) γιά $Re(s) > k/2+1$ ως:

$$\Lambda(s,f) = N^{s/2}\int_0^{1/\sqrt{N}} f(i\sigma)\sigma^{s-1}d\sigma + N^{s/2}\int_{1/\sqrt{N}}^{\infty} f(i\sigma)\sigma^{s-1}d\sigma.$$

Στον πρώτο όρο αντικαθιστούμε το σ με $(N\sigma)^{-1}$ και στην συνέχεια χρησιμοποιούμε τον τύπο μετασχηματισμού της f ύπο την δράση της w_N. Το αποτέλεσμα είναι:

$$\Lambda(s,f) = \epsilon N^{\frac{1}{2}(k-s)} i^k \int_{1/\sqrt{N}}^{\infty} f(i\sigma)\sigma^{k-s-1}d\sigma + N^{s/2}\int_{1/\sqrt{N}}^{\infty} f(i\sigma)\sigma^{s-1}d\sigma.$$

Συνεπώς λόγω της προηγούμενης παρατήρησης γιά την σύγκλιση του ολοκληρώματος ο παραπάνω όρος ορίζεται και είναι ακέραιος γιά όλα τα $s \in \mathbb{C}$. Αφού η $\Gamma(s)$ δεν είναι πουθενά 0, έπεται ότι η $L(s,f)$ είναι τελικά ακέραια. Τέλος αντικαθιστώντας το s με $k-s$ και πολλαπλασιάζοντας με $\epsilon i^k = \epsilon(-1)^{k/2}$ έχουμε ότι

$$\epsilon(-1)^{k/2}\Lambda(k-s,f) = N^{\frac{1}{2}s}\int_{1/\sqrt{N}}^{\infty} f(i\sigma)\sigma^{s-1}d\sigma + \epsilon N^{\frac{1}{2}(k-s)} i^k \int_{1/\sqrt{N}}^{\infty} f(i\sigma)\sigma^{k-s-1}d\sigma.$$

η οποία μας δίνει και το ζητούμενο αποτέλεσμα.

3.4 Τελεστές του Hecke και L-σειρές των Hecke ιδιομορφών.

Ορισμός 3.29 *Θα ονομάζουμε αυτόμορφα ζεύγη (modular pairs) τα ζεύγη της μορφής* (Λ, C) *όπου* Λ *είναι ένα δικτυωτό του* $\mathbb{C}$ *και* C *μιά κυκλική υποομάδα του* $\mathbb{C}/\Lambda$ *τάξης ακριβώς* N.

Αν Λ είναι ένα δικτυωτό θα συμβολίζουμε με P_Λ την φυσική προβολή του $\mathbb{C}$ στο $\mathbb{C}/\Lambda$. Σε ένα αυτόμορφο ζεύγος (Λ, C) και ένα μη μηδενικό μιγαδικό αριθμό α θα αντισοιχούμε ένα άλλο αυτόμορφο ζεύγος $(\alpha\Lambda, \alpha C)$ ως εξής: η κυκλική υποομάδα αC δίνεται από:

$$\alpha C = P_{\alpha\Lambda}(\alpha P_\Lambda^{-1}(C)).$$

Μια συνάρτηση μιγαδικής μεταβλητής $\tilde{f}$ ορισμένη στα αυτόμορφα ζεύγη θα λέγεται ομογενής βαθμού $-k$ αν

$$\tilde{f}(\alpha\Lambda, \alpha C) = \alpha^{-k}\tilde{f}(\Lambda, C) \quad \text{γιά} \quad \alpha \in \mathbb{C}^*$$

Σε κάθε τέτοια συνάρτηση $\tilde{f}$ αντισοιχούμε μιά συνάρτηση f στο $\mathbb{H}$ που ορίζεται ως:

$$f(\tau) := \tilde{f}(\Lambda_\tau, P_{\Lambda_\tau}(\frac{1}{N}\mathbb{Z})).$$

Επαληθεύουμε ότι ικανοποιεί την σχέση:

$$f(\gamma\tau) = j(\gamma,\tau)^k f(\tau) \quad \text{γιά κάθε} \quad \gamma \in \Gamma_0(N).$$

Πράγματι αφού $\Lambda_{\gamma\tau} = j(\gamma,\tau)^{-1}\Lambda_\tau$ έχουμε:

$$\begin{aligned}
&f(\gamma\tau) = \tilde{f}(\Lambda_{\gamma\tau}, P_{\Lambda_{\gamma\tau}}(\tfrac{1}{N}\mathbb{Z})) = \tilde{f}(j(\gamma,\tau)^{-1}\Lambda_\tau, P_{j(\gamma,\tau)^{-1}\Lambda_\tau}(\tfrac{1}{N}\mathbb{Z})) = \\
&= j(\gamma,\tau)^k\tilde{f}(\Lambda_\tau, j(\gamma,\tau)P_{j(\gamma,\tau)^{-1}\Lambda_\tau}(\tfrac{1}{N}\mathbb{Z})) = \\
&= j(\gamma,\tau)^k\tilde{f}(\Lambda_\tau, P_{\Lambda_\tau}j(\gamma,\tau)P^{-1}_{j(\gamma,\tau)^{-1}\Lambda_\tau}P_{j(\gamma,\tau)^{-1}\Lambda_\tau}(\tfrac{1}{\mathrm{N}}\mathbb{Z}))) = \\
&= j(\gamma,\tau)^k\tilde{f}(\Lambda_\tau, P_{\Lambda_\tau}(j(\gamma,\tau)(\tfrac{1}{N}\mathbb{Z} + j(\gamma,\tau)^{-1}\Lambda_\tau))) = \\
&= j(\gamma,\tau)^k\tilde{f}(\Lambda_\tau, P_{\Lambda_\tau}(j(\gamma,\tau)\tfrac{1}{N}\mathbb{Z} + \Lambda_\tau)).
\end{aligned}$$

Αντιστρόφως υποθέτουμε ότι f είναι $\Gamma_0(N)$ αυτόμορφη συνάρτηση από το $\mathbb{H}$ στο $\mathbb{C}$ θα ορίσουμε ομογενή συνάρτηση $\tilde{f}$ βαθμού $-k$ στα αυτόμορφα ζεύγη. Εστω ότι δίνεται το (Λ, C). Τότε το Λ είναι υποδικτυωτό δείκτη N στην $P_\Lambda^{-1}(C)$ με την $P_\Lambda^{-1}(C)/\Lambda$ κυκλική. Συνεπώς μπορούμε να βρούμε μιά $\mathbb{Z}$ βάση $\{\omega_1, \omega_2\}$ του Λ τέτοια ώστε $\{\frac{1}{N}\omega_1, \omega_2\}$ να είναι μιά $\mathbb{Z}$ βάση του $P_\Lambda^{-1}(C)$. Επιπλέον μπορούμε να υποθέσουμε ότι $Im(\omega_2/\omega_1) > 0$. Σε αυτή την βάση ορίζουμε

$$\tilde{f}(\Lambda, C) = \omega_1^{-k}f(\omega_2/\omega_1).$$

Γιά να δούμε ότι η $\tilde{f}(\Lambda, C)$ είναι καλώς ορισμένη, έστω $\{\omega_1', \omega_2'\}$ μιά άλλη βάση του Λ τέτοια ώστε $\{\frac{1}{N}\omega_1', \omega_2'\}$ είναι βάση του $P_\Lambda^{-1}(C)$ και $Im(\omega_2'/\omega_1') > 0)$. Αν γράψουμε

$$\begin{pmatrix} \omega_2' \\ \omega_1' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_2 \\ \omega_1 \end{pmatrix}$$

τότε το $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$. Αφού $\{\frac{1}{N}\omega_1, \omega_2\}$ και $\{\frac{1}{N}\omega_1', \omega_2'\}$ είναι δυό βάσεις γιά το $P_\Lambda^{-1}(C)$ η ισότητα

$$\begin{pmatrix} \omega_2' \\ \frac{1}{N}\omega_1' \end{pmatrix} = \begin{pmatrix} a & Nb \\ \frac{1}{N}c & d \end{pmatrix} \begin{pmatrix} \omega_2 \\ \frac{1}{N}\omega_1 \end{pmatrix}$$

εξαναγκάζει τον πίνακα αλλαγής να είναι ακέραιος και συνεπώς ανήκει στην $\Gamma_0(N)$. Συνεπώς έχουμε:

$$\omega_1'^{-k} f(\omega_2'/\omega_1') = \omega_1'^{-k} f(\gamma(\omega_2/\omega_1)) = \omega_1'^{-k} j(\gamma, \omega_2/\omega_1)^k f(\omega_2/\omega_1) = \omega_1^{-k} f(\omega_2/\omega_1)$$

δηλαδή η $\tilde{f}$ είναι καλά ορισμένη.

Τέλος ας ελέγξουμε την ομογένεια της $\tilde{f}$. Αν $\{\omega_1, \omega_2\}$ είναι μιά διατεταγμένη βάση του δικτυωτού Λ τότε $\{\alpha\omega_1, \alpha\omega_2\}$ είναι μιά διατεταγμένη βάση γιά το $\alpha\Lambda$ συνεπώς

$$\tilde{f}(\alpha\Lambda, \alpha C) = (\alpha\omega_1)^{-k} f((\alpha\omega_2)/(\alpha\omega_1)) = \alpha^{-k}\tilde{f}(\Lambda, C).$$

Οι δυό κατασκευές $\tilde{f} \longrightarrow f$ και $f \longrightarrow \tilde{f}$ είναι αντίστροφες η μία της άλλης και συνεπώς υπάρχει μιά αμφιμονοσήμαντη αντιστοιχία μεταξύ ομογενών συναρτήσεων $\tilde{f}$ βαθμού $-k$ των αυτομόρφων ζεύγων και των αυτομόρφων συναρτήσεων του $\mathbb{H}$ βάρους k ως προς την $\Gamma_0(N)$.

Ορισμός 3.30 *Εστω $\mathcal{L}$ η ελεύθερη αβελιανή ομάδα με γεννήτορες τα αυτόμορφα ζεύγη (Λ, C). Γιά κάθε $n \in N$ ορίζουμε τον n-οστό τελεστή του Hecke*

$$T(n) : \mathcal{L} \longrightarrow \mathcal{L}$$

$$T(n)(\Lambda, C) = \sum (\Lambda', C')$$

όπου το άθροισμα λαμβάνεται πάνω σε όλα τα δικτυωτά Λ' με δείκτη $[\Lambda : \Lambda'] = n$ και πάνω σε όλες τις κυκλικές ομάδες C' που παράγονται από την εικόνα της C μέσω της φυσικής προβολής $\mathbb{C}/n\Lambda \longrightarrow \mathbb{C}/\Lambda'$. Προφανώς το παραπάνω άθροισμα είναι πεπερασμένο. Ορίζουμε τέλος τελεστές Hecke στις συναρτήσεις $\tilde{f}$ των ομογενών βαθμού k αυτόμορφων ζευγών ως:

$$(T_k(n)\tilde{f})(\Lambda, C) = n^{k-1} \sum \tilde{f}(\Lambda', C')$$

όπου το άθροισμα διατρέχει ακριβώς τα δικτυωτά και τις υποομάδες του πρώτου μέρους του ορισμού.

Είναι σαφές ότι η $T_k(n)\tilde{f}$ είναι συνάρτηση ορισμένη στα αυτόμορφα ζεύγη, ομογενής και μάλιστα βαθμού $-k$. Στην συνέχεια θα μελετήσουμε τον επαγώμενο τελεστή στις συναρτήσεις μεταβλητής $\tau \in \mathbb{H}$ και θα δούμε ότι μεταφέρει αυτόμορφες ως προς την $\Gamma_0(N)$ μορφές σε αυτόμορφες μορφές και παραβολικές μορφές σε παραβολικές μορφές. Και αυτόν τον τελεστή θα τον καλούμε επίσης τελεστή του Hecke.

Ας μελετήσουμε όμως την σχέση των αυτομόρφων ζευγών (Λ, C) και (Λ', C') κάνοντας χρήση πινάκων. Θα συμβολίζουμε με $M(n)$ το σύνολο των 2×2 πινάκων με συντελεστές ακεραίους και ορίζουσα n. Επιλέγουμε μιά βάση $\{\omega_1, \omega_2\}$ του Λ τέτοια ώστε $\{\frac{1}{N}\omega_1, \omega_2\}$ να είναι μιά βάση του $P_\Lambda^{-1}(C)$ και $Im(\omega_2/\omega_1) > 0$ και έσωι $\{\omega_1', \omega_2'\}$ μιά παρόμοια βάση γιά το Λ'. Τότε μπορούμε να γράψουμε

$$\begin{pmatrix} \omega_2' \\ \omega_1' \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} \omega_2 \\ \omega_1 \end{pmatrix}$$

όπου ο πίνακας $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ ανήκει στο $M(n)$. Οι αντίστροφες εικόνες των nC και C' δίνονται από

$$\begin{aligned} P_{n\Lambda}^{-1}(nC) &= \tfrac{n}{N}\mathbb{Z}\omega_1 + n\mathbb{Z}\omega_2 \\ P_{\Lambda'}^{-1}(C') &= \tfrac{1}{N}\mathbb{Z}\omega_1' + \mathbb{Z}\omega_2' \end{aligned}$$

Επειδή

$$\frac{n}{N}\omega_1 = \frac{1}{N}(a)(c\omega_2 + d\omega_1) - \left(\frac{c}{N}\right)(a\omega_2 + b\omega_1) = \frac{1}{N}(a)\omega_1' - \left(\frac{c}{N}\right)\omega_2'$$

και

$$n\omega_2 = (-bn)(c\omega_2 + d\omega_1) + (nd)(a\omega_2 + b\omega_1) = \frac{1}{N}(-bnN)\omega_1' + (nd)\omega_2'$$

και το C απεικονίζεται στο C' ανν c/N είναι ακέραιος. Ας υποθέσουμε ότι αύτο ισχύει. Γιά να απεικονίζεται το nC επί του C', το $\frac{n}{N}\omega_1$ πρέπει να έχει ακριβώς τάξη N κατά προσέγγιση Λ'. Η τάξη είναι τουλάχιστον $m \geq 1$ τέτοια ώστε

$$\frac{nm}{N}\omega_1 = r\omega_1' + s\omega_2'$$

γιά κάποιους ακέραιους r, s. Με αντιστροφή των προηγούμενων σχέσεων αντικαθιστούμε το $\omega_1 = \frac{1}{n}(-c\omega_2' + a\omega_1')$ και ξαναγράφουμε την συνθήκη ως:

$$\frac{m}{N}(-c\omega_2' + a\omega_1') = r\omega_1' + s\omega_2'.$$

Αφού $N|c$ η συνθήκη είναι ακριβώς $ma/N = r$. Η τάξη είναι συνεπώς $\mathrm{N}/(a, N)$ και η τάξη είναι ακριβώς N ανν $(a, N) = 1$. Τελικά καταλήξαμε στο συμπέρασμα ότι $\{\omega_1', \omega_2'\}$ και $\{\omega_1, \omega_2\}$ σχετίζονται με ένα πίνακα του συνόλου

$$M(n, N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(n) | c \equiv 0 mod N \quad \text{και} \;\; (a, N) = 1 \right\}$$

Θα μπορούσαμε φυσικά να διαλέξουμε μιά άλλη βάση γιά το Λ' αλλά αυτή σε κάθε περίπτωση σχετίζεται με το $\{\omega_1', \omega_2'\}$ μέσω στοιχείου της $\Gamma_0(N)$. Συνεπώς τα αυτόμορφα ζεύγη (Λ', C') στο άθροισμα παραμετρίζονται από της κλάσεις $\Gamma_0(N)\backslash M(n, N)$.

Πρόταση 3.31 *Εστω $\{a_i\}$ ένα πλήρες σύστημα αντιπροσώπων των κλάσεων $\Gamma_0(N)a$ της $\Gamma_0(N)$ στον $M(n, N)$. Αν f ανήκει στην $M_k(\Gamma_0(N))$, τότε $T_k(n)f$ δίνεται ως συνάρτηση του τ από την σχέση:*

$$T_k(n)f = n^{\frac{k}{2}-1} \sum_i f|[a_i]_k$$

συνεπώς η $T_k(n)f$ είναι επίσης αυτόμορφη μορφή βάρους k και επιπέδου N.

Απόδειξη: άμεση από τον ορισμό των τελεστών του Hecke.

Πόρισμα 3.32 *Ο τελεστής Hecke $T_k(n)$ απεικονίζει το $M_k(\Gamma_0(N))$ και το $S_k(\Gamma_0(N))$ στον εαυτό τους.*

Απόδειξη: Αν $f \in M_k(\Gamma_0(N))$ και $\beta \in SL_2(\mathbb{Z})$ εφαρμόζοντας ένα παρόμοιο επιχείρημα με αυτό της πρότασης 3.27 βλέπουμε ότι $(f|[a_i]_k)|[\beta^{-1}]|_k(\tau)$ έχει ολόμορφο q_{nN} ανάπτυγμα στο ∞. Συνεπώς το ίδιο ισχύει και γιά τον $(T_k(n)f)|[\beta^{-1}]_k(\tau)$. Ομως η $T_k(n)f$ είναι αυτόμορφη μορφή της $\Gamma_0(N)$ και συνεπώς $(T_k(n)f)|[\beta^{-1}]_k(\tau)$ είναι περιοδική με περίοδο N. Δηλαδή οι όροι του q_{nN} αναπτύγματος που ο δείκτης τους δεν είναι πολλαπλάσιο του n μηδενίζονται και το $T_k(n)f$ είναι ολόμορφο στο παραβολικό σημείο $\beta^{-1}(\infty)$. Ομοίως αποδεικνύεται ότι οι τελεστές του Hecke $T_k(n)$ απεικονίζουν τον $S_k(\Gamma_0(N))$ στον εαυτό του.

Λήμμα 3.33 *Οι πίνακες $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ με $ad = n, d > 0, (a, N) = 1$ και $0 \le b \le d$ είναι ένα πλήρες σύστημα αντιπροσώπων γιά τις δεξιές κλάσεις του $\Gamma_0(N)$ στο $M(n, N)$.*

Απόδειξη: Εστω ότι δίνεται $\begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}$. Διαλέγουμε τους σχετικά πρώτους αριθμούς x, y με $N|x$ και $xa' + yc' = 0$ και στην συνέχεια τους σχετικά πρώτους αριθμούς u, v με $uy + v(-x) = 1$. Τότε $\begin{pmatrix} u & v \\ x & y \end{pmatrix} \in \Gamma_0(N)$ και:

$$\begin{pmatrix} u & v \\ x & y \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} = \begin{pmatrix} a'' & b'' \\ 0 & d'' \end{pmatrix}$$

Μπορούμε επιπλέον να υποθέσουμε ότι $a'' > 0$ και $d'' > 0$, αν όχι πολλαπλασιάζουμε με -1_2. Διαλέγουμε ακαιρέους q, r με $b'' = d''q + r$ και $0 \le r < d''$. Τότε

$$\begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a'' & b'' \\ 0 & d'' \end{pmatrix} = \begin{pmatrix} a'' & r \\ 0 & d'' \end{pmatrix}$$

ο οποίος είναι και ο αντιπρόσωπος της πλευρικής υποομάδας που ψάχνουμε.

Ας υποθέσουμε τώρα ότι δυό στοιχεία που περιγράφει το λήμμα ανήκουν στην ίδια πλευρική υποομάδα, δηλαδή

$$\begin{pmatrix} u & v \\ x & y \end{pmatrix} \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} a' & b' \\ 0 & d' \end{pmatrix}$$

με $uy - vx = 1$. Θα πρέπει $x = 0$, $u = y = 1$ και $v = 0$.

Πρόταση 3.34 *Εστω $f \in M_k(\Gamma_0(N))$ με q ανάπτυγμα $f(\tau) = \sum_{n=0}^{\infty} c_n q^n$. Τότε η $T_k(m)f$ έχει q ανάπτυγμα:*

$$T_k(m)f(\tau) = \sum_{n=0}^{\infty} b_n q^n$$

όπου

$$b_n = \left\{ \begin{array}{ll} c_0 \sum_{\substack{a|m,\, a>0 \\ (a,\,N)=1}} a^{k-1} & \text{αν } n=0 \\ c_m & \text{αν } n=1 \\ \sum_{\substack{a|(n,\,m) \\ (a,\,N)=1}} a^{k-1} c_{nm/a^2} & \text{αν } n>1 \end{array} \right\}$$

<u>Απόδειξη:</u> Υποθέτουμε ότι $(a, N) = 1$ και έχουμε:

$$T_k(m)f = m^{k/2-1} \sum_i f|[\alpha_i]_k$$

και υπολογίσαμε ένα πλήρες σύστημα αντιπροσώπων έστω α ένας τέτοιος,

$$\alpha = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \qquad \begin{array}{l} ad = m \\ (a, N) = 1 \end{array}$$

συνεπώς έχουμε:

$$f|[\alpha]_k(\tau) = f\left(\frac{a\tau + b}{d}\right) d^{-k} m^{k/2} = \sum_{n=0}^{\infty} c_n e^{2\pi i n(a\tau+b)/d} d^{-k} m^{k/2}$$

άρα:

$$T_k(m)f(\tau) = m^{k-1} \sum_{n=0}^{\infty} \sum_{a,b,d} d^{-k} c_n e^{2\pi i n(a\tau+b)/d}$$

όπου το άθροισμα λαμβάνεται ώς προς τα a, d, b με $ad = m, d > 0, (a, N) = 1$. Παρατηρούμε ότι το άθροισμα

$$\sum_{b=0}^{d-1} e^{2\pi i n b/d} = \left\{ \begin{array}{ll} d & \text{αν } d|n \\ 0 & \text{αλλιώς} \end{array} \right\}$$

Αρκεί λοιπόν στα αθροίσματα να θεωρήσουμε μόνο τα n της μορφής $n = ld$, οπότε έχουμε:

$$T_k(m)f(\tau) = m^{k-1} \sum_{l=0}^{\infty} \sum_{ad=m, d>0} c_{ld} d^{-k+1} q^{la} = \sum_{l=0}^{\infty} \sum_{a|m, a>0} c_{lm/a} a^{k-1} q^{la}.$$

Ο συντελεστής του q^0 είναι αυτός που προκύπτει όταν θέσουμε $l = 0$ και ισούται με $c_0 = \sum_{a|m,a>0} a^{k-1}$. Ο συντελεστής του q^1 προκύπτει όταν θέσουμε $l = a = 1$ και είναι c_m. Γιά τους συντελεστές των q^n, $n \geq 2$ οι συντελεστές υπολογίζονται από τις τριάδες:(l, d, a) με $la = n$ και $a|m$. Ο συντελεστής $c_{lm/a} = c_{nm/a^2}$ με $a|n$ και $a|m$. Συνεπώς ο συντελεστής του q^n σε αυτή την περίπτωση είναι $\sum_{a|(n,m)} c_{nm/a^2} a^{k-1}$.

Στην συνέχεια θα μελετήσουμε την αλληλεπίδραση των τελεστών Hecke. Θέτουμε $R(n)(\Lambda, C) = (n\Lambda, nC)$.

Λήμμα 3.35

- *Γιά δύναμη πρώτου p^r με $r \geq 1$ τέτοια ώστε $p \not| N$ ισχύει:*

$$\mathrm{T}(p^r)T(p) = T(p^{r+1}) + pR(p)T(p^{r-1})$$

- *Γιά δύναμη πρώτου* p^r *με* $r \geq 1$ *τέτοιο ώστε* $p|N$ *ισχύει:*

$$T(p^r) = T(p)^r$$

- *T(m)T(n)=T(mn) αν* m, n *είναι μετάξυ τους πρώτοι.*

Γιά την απόδειξη του παραπάνω λήμματος, χρειάζεται να ελέγξουμε τις πολλαπλότητες των δικτυωτών που εμφανίζονται σε κάθε μέλος και να δείξουμε ότι είναι ίσες [Kn,σελ. 278]

Θεώρημα 3.36 *(Hecke) Στον χώρο* $M_k(\Gamma_0(N))$ *ισχύει για τους αντίστοιχους τελεστές Hecke:*

- *Γιά πρώτη δύναμη* p^r *με* $r \geq 1$ *τέτοιο ώστε* $p \not| N$ *ισχύει:*

$$T_k(p^r)T_k(p) = T_k(p^{r+1}) + p^{k-1}T_k(p^{r-1}).$$

  Επομένως $T_k(p^r)$ *είναι πολυώνυμο στα* $T_k(p)$ *με ακέραιους συντελεστες.*

- *Γιά πρώτη δύναμη* p^r *με* $r \geq 1$ *και* $p|N$ *έχουμε*

$$T_k(p^r) = T_k(p)^r$$

- $T_k(m)T_k(n) = T_k(mn)$ *αν* m, n *είναι πρώτοι μεταξύ τους.*
- *Η άλγεβρα που γεννάται από τα* $T_k(n)$ *γιά* $n = 1, 2, 3...$ *γεννάται μόνο από τα* $T_k(p)$ *όπου* p *πρώτος και είναι μεταθετική.*

Απόδειξη: άμεση συνέπεια του προηγουμένου λήμματος.

Ορισμός 3.37 *(εσωτερικό γινόμενο του Petersson) Στον* $S_k(\Gamma_0(N))$ *ορίζουμε το εσωτερικό γινόμενο :*

$$< f, h > := \int_{R_N} f(\tau)\overline{h(\tau)}\sigma^k \frac{d\rho d\sigma}{\sigma^2}$$

όπου R_N *είναι μιά θεμελιώδης περιοχή της* $\Gamma_0(N)$.

Το παραπάνω γινόμενο δεν εξαρτάται από την επιλογή της θεμελιώδους περιοχής, αφού εύκολα παρατηρούμε ότι το μέτρο

$$\frac{d\rho d\sigma}{\sigma^2}$$

παραμένει αναλλοίωτο από τους μετασχηματισμούς της $\Gamma_0(N)$.

Θεώρημα 3.38 *Οι τελεστές του Hecke* $T_k(n)$ *με* $(n, N) = 1$, *στον χώρο των παραβολικών μορφών* $S_k(\Gamma_0(N))$ *είναι αυτοσυζυγείς ως προς το εσωτερικό γινόμενο Petersson.*

Απόδειξη: Από τους τύπους πολλαπλασιασμού των τελεστών του Hecke παρατηρούμε ότι αρκεί να δείξουμε το θεώρημα γιά ένα πρώτο αριθμό p. Θέλουμε ουσιαστικά να δείξουμε ότι αν $f, h \in S_k(\Gamma_0(N))$ τότε ισχύει:

$$\int_R T_k(p)f(\tau)\overline{h(\tau)}\sigma^k \frac{d\rho d\sigma}{\sigma^2} = \int_R f(\tau)\overline{T_k(p)h(\tau)}\sigma^k \frac{d\rho d\sigma}{\sigma^2}.$$

Λόγω της ανεξαρτησίας τού ορισμού του γινομένου Petersson από την θεμελιώδη περιοχή, αρκεί να δείξουμε ότι

$$\int_{\tilde{R}} T_k(p)f(\tau)\overline{h(\tau)}\sigma^k \frac{d\rho d\sigma}{\sigma^2} = \int_{\tilde{R}} f(\tau)\overline{T_k(p)h(\tau)}\sigma^k \frac{d\rho d\sigma}{\sigma^2},$$

όπου $\tilde{R}$ είναι μιά θεμελιώδης περιοχή της ομάδας $\Gamma(pN)$. Πράγματι, θα εμφανιστούν οι προηγούμενοι παράγοντες πολλαπλασιασμένοι με $[\Gamma_0(N):\Gamma(pN)]$. Στό λήμμα 3.33 έχουμε υπολογίσει ένα πλήρες σύστημα αντιπροσώπων γιά τις κλάσεις του $\Gamma_0(N)$ στο $M(p,N)$. Γιά κάθε τέτοιο a_i υπάρχουν στοιχεία $\gamma_i, \gamma_i' \in \Gamma_0(N)$ τέτοια ώστε, αν $a_i' = pa_i^{-1}$, τότε $a_i' = \gamma_i a_i \gamma_i'$. Πράγματι αν υποθέσουμε ότι $p \not| N$ τότε γιά το στοιχείο $a_i = \begin{pmatrix} 1 & b \\ 0 & p \end{pmatrix}$, διαλέγουμε ακεραίους x, y τέτοιοι ώστε $p^2x - Ny = 1 + pbN$. Τότε από την σχέση

$$\begin{pmatrix} p & -b \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} px - bN & y \\ N & p \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & p \end{pmatrix} \begin{pmatrix} x & xb + y + pb \\ N & Nb + p^2 \end{pmatrix}^{-1}$$

βλέπουμε το ζητούμενο. Γιά το στοιχείο της μορφής: $a_i = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$ απλά αντιστρέφουμε την προηγούμενη σχέση. Αφού $f[\gamma_i'^{-1}]_k = f$ και $h[\gamma_i]_k = h$, έχουμε ότι:

$$\int_{\tilde{R}} f(\tau)\overline{h[a_i]_k(\tau)}\sigma^k \frac{d\rho d\sigma}{\sigma^2} = \int_{\gamma_i'\tilde{R}} f(\tau)\overline{h[\gamma_i a_i \gamma_i']_k(\tau)}\sigma^k \frac{d\rho d\sigma}{\sigma^2} =$$

$$= \int_{\tilde{R}} f(\tau)\overline{h[\gamma_i a_i \gamma_i']_k(\tau)}\sigma^k \frac{d\rho d\sigma}{\sigma^2} = \int_{\tilde{R}} f(\tau)\overline{h[a_i']_k(\tau)}\sigma^k \frac{d\rho d\sigma}{\sigma^2}.$$

Συνεπώς λόγω της Πρότασης 3.31 αρκεί να δείξουμε ότι γιά κάθε $a = a_i$ ισχύει:

$$\int_{\tilde{R}} f(\tau)[a]_k\overline{h(\tau)}\sigma^k \frac{d\rho d\sigma}{\sigma^2} = \int_{\tilde{R}} f(\tau)\overline{h[a']_k(\tau)}\sigma^k \frac{d\rho d\sigma}{\sigma^2}.$$

Θα αλλάξουμε μεταβλητές στο αριστερό μέλος αντικαθιστώντας το $a\tau$ με τ'. Επιπλέον παρατηρούμε ότι $a^* = n^{-1/2}a$ έχει ορίζουσα 1 και ικανοποιεί την

$$f[a]_k = f[a^*]_k$$

οπότε έχουμε:

$$f[a]_k(\tau)\overline{h(\tau)}\sigma^k = f[a^*]_k(\tau)\overline{h(\tau)}Im(\tau)^k =$$

$$= f(a^*\tau)\overline{h(a^{*-1}(a^*\tau))}j(a^*,\tau)^{-k}Im(\tau)^k = f(a^*\tau)\overline{h(a^{*-1}(a^*\tau))j(a^*,\tau)^k}\left(\frac{Im(\tau)}{|j(a^*,\tau)|^2}\right)^k =$$

$$= f(a^*\tau)\overline{h(a^{*-1}(a^*\tau))}j(a^{*-1}, a^*\tau)^{-k} Im(a^*\tau)^k = f(\tau'\overline{h[a']_k(\tau')} Im(\tau)^k.$$

Επιστρέφοντας στην σχέση των ολοκληρωμάτων έχουμε:

$$\int_{\tilde{R}} f[a]_k(\tau)\overline{h(\tau)}\sigma^k \frac{d\rho d\sigma}{\sigma^2} = \int_{a\tilde{R}} f(\tau)\overline{h[a']_k(\tau)}\sigma^k \frac{d\rho d\sigma}{\sigma^2}. \quad (b)$$

Γιά την f ισχύει ότι

$$f(\gamma\tau) = j(\gamma, \tau)^k f(\tau) \quad \text{γιά όλα τα } \gamma \in a\Gamma(pN)a^{-1}$$

αφού $a\Gamma(pN)a^{-1} \subseteq \Gamma_0(N)$. Επιπλέον ισχύει ότι

$$h[a']_k(\gamma\tau) = j(\gamma, \tau)^k h[a']_k(\tau) \quad \text{γιά όλα τα } \gamma \in a\Gamma(pN)a^{-1},$$

αφού $a'(a\Gamma(pN)a^{-1})a'^{-1} = \Gamma(pN) \subseteq \Gamma_0(N)$. Η ολοκληρωτέα ποσότητα στο δεξιό μέλος της (b) είναι αναλλοίωτη ως προς την δράση της $a\Gamma(pN)a^{-1}$. Το $a\tilde{R}$ είναι μιά θεμελιώδης περιοχή γιά την ομάδα $a\Gamma(p)a^{-1}$ συνεπώς μπορούμε να την αλλάξουμε με μιά οποιαδήποτε άλλη:

$$\int_{\tilde{R}} f[a]_k(\tau)\overline{h(\tau)}\sigma^k \frac{d\rho d\sigma}{\sigma^2} = \frac{1}{[a\Gamma(pN)a^{-1} : \Gamma(pN) \bigcap a\Gamma(pN)a^{-1}]} \int_{(a\tilde{R})'} f(\tau)\overline{h[a']_k(\tau)}\sigma^k \frac{d\rho d\sigma}{\sigma^2}.$$

Παρόμοια για το άλλο ολοκλήρωμα έχουμε ότι

$$f(\gamma\tau) = j(\gamma, \tau)^k f(\tau) \ \text{ γιά } \ \gamma \in \Gamma(pN)$$

και επιπλέον ισχύει:

$$h[a']_k(\gamma\tau) = j(\gamma, \tau)^k h[a']_k(\tau), \quad \gamma \in \Gamma(pN)$$

αφού $a'\Gamma(pN)a'^{-1} \subseteq \Gamma_0(N)$. Συνεπώς το ολοκλήρωμα είναι αναλλοίωτο ως προς την δράση της $\Gamma(pN)$, και μπορούμε να αντικαταστήσουμε την $\tilde{R}$ με οποιαδήποτε άλλη θεμελιώδη περιοχή θέλουμε. Συνεπώς έχουμε ότι:

$$\int_{\tilde{R}} f(\tau)\overline{h[a']_k(\tau)}\sigma^k \frac{d\rho d\sigma}{\sigma^2} = \frac{1}{[\Gamma(pN) : \Gamma(pN) \bigcap a\Gamma(pN)a^{-1}]} \int_{\tilde{R}} f(\tau)\overline{h[a']_k(\tau)}\sigma^k \frac{d\rho d\sigma}{\sigma^2}.$$

Οι δυό δείκτες που εμφανίζονται είναι ίσοι και επιπλέον το εσωτερικό των ολοκληρωμάτων είναι αναλλοίωτο ως προς την δράση της ομάδας $\Gamma(pN) \bigcap a\Gamma(pN)a^{-1}$. Από την άλλη τα $\tilde{R}'$ και $(a\tilde{R})'$ είναι δυό θεμελιώδεις περιοχές γιά το ολοκλήρωμα από όπου έχουμε την ισότητα των ολοκληρωμάτων και του θεωρήματος.

Αφού οι τελεστές του Hecke μετατίθενται έχουμε ότι ο $S_k(\Gamma_0(N))$ διασπάται σε ορθογώνιο άθροισμα ταυτόχρονων ιδιόχωρων των τελεστών $T_k(n)$ με $(n, N) = 1$. Τα ταυτόχρονα ιδιοδιανύσματα όλων των $T_k(n)$ με $(n, N) = 1$ θα ονομάζονται ιδιομορφές, ιδιομορφές του ιδίου ιδιοχώρου θα ονομάζονται ισοδύναμες.

Πρόταση 3.39 *Η ενέλιξη w_N της $S_k(\Gamma_0(N))$ είναι αυτοσυζυγής και μετατίθεται με όλα τα $T_k(n)$ τέτοια ώστε $(n, N) = 1$*

Απόδειξη: Εχουμε $w_N(f) = f|[\alpha_N]_k$. Ξαναεφαρμόζουμε το επιχείρημα του προηγούμενου θεωρήματος γιά $a = a_N$, με $\tilde{R}$ να είναι μιά θεμελιώδης περιοχή της $\Gamma(N^2)$. Εχουμε και $[a'_N] = [a_N]$ οπότε πράγματι η ενέλιξη w_N είναι αυτοσυζυγής.

Γιά να δείξουμε ότι $w_N T_k(n) = T_k(n) w_N$, υποθέτουμε χωρίς περιορισμό της γενικότητας ότι n είναι ένας πρώτος αριθμός p με $p \not| N$. Από το Λήμμα 3.33 έχουμε ότι οι αντιπρώσωποι είναι της μορφής

$$\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}, \quad \begin{pmatrix} 1 & b \\ 0 & p \end{pmatrix} \quad \text{με } 1 \leq b \leq p-1.$$

Αρκεί λοιπόν να ελέγξουμε ότι :

$$\sum_i f[a_N a_i]_k = \sum_i f[a_i a_N]_k.$$

Γιά τους δύο πρώτους πίνακες το παραπάνω είναι προφανές αφού

$$a_N \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} a_N \quad \text{και} \quad a_n \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} a_N.$$

Γιά τους άλλους πίνακες θα δείξουμε ότι ο πίνακας με b μεταβάλει το δεξί μέλος του αθροίσματος όσο και ο πίνακας με e το αριστερό, όπου $1 \leq e \leq p-1$ και $e \equiv (-Nb)^{-1} mod\ p$. Πράγματι υπολογίζουμε ότι

$$\begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & p \end{pmatrix} = \begin{pmatrix} p & -e \\ -Nb & p^{-1}(1+ebN) \end{pmatrix} \begin{pmatrix} 1 & e \\ 0 & p \end{pmatrix} \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}.$$

Επιπλέον αν με γ συμβολίσουμε τον πρώτο πίνακα στο δεξί μέλος τότε $\gamma \in \Gamma_0(N)$ συνεπώς $f[\gamma]_k = f$ και τελικά έχουμε

$$f\left[a_N \begin{pmatrix} 1 & b \\ 0 & p \end{pmatrix}\right]_k = f\left[\begin{pmatrix} 1 & e \\ 0 & p \end{pmatrix} a_N\right]_k.$$

Συνεπώς η ανάλυση του $S_k(\Gamma_0(N))$ σε χώρους ισοδυνάμων ιδιομορφών είναι συμβατή με την ανάλυση του $S_k(\Gamma_0(N))$ σε $S_k^+(\Gamma_0(N))$ και $S_k^-(\Gamma_0(N))$.

Οι τελεστές του Hecke $T_k(n)$ με $(n, N) = 1$ αντιμεταιτίθενται με τους $T_k(n)$ και συνεπώς απεικονίζουν τους χώρους ισοδυνάμων ιδιομορφών στους εαυτούς τους. Σε κάθε τέτοιο χώρο θα βρίσκεται τουλάχιστον ένα ιδιοδιάνυσμα όλων των $T_k(n)$

Πρόταση 3.40 *Υποθέτουμε ότι $f \in S_k(\Gamma_0(N))$ είναι μιά ιδιομορφή, ταυτόχρονα γιά όλους τους $T_k(n)$, έστω με $T_k(n)f = \lambda(n)f$. Αν το q ανάπτυγμα της f στο ∞ είναι $f(\tau) = \sum_{n=1}^{\infty} c_n q^n$ τότε λόγω της πρότασης 3.34 έχουμε:*

$$c_n = \lambda(n) c_1.$$

Συνεπώς αν $f \neq 0$ τότε $c_1 \neq 0$ και οι ιδιοτιμές $\{\lambda(n)\}$ καθορίζουν την f κατά προσέγγιση βαθμωτού.

Υπό τις προϋποθέσεις της παραπάνω πρότασης μπορούμε να κανονικοποιήσουμε την f έτσι ώστε το q ανάπτυγμα $f(\tau) = \sum_{n=1}^{\infty} c_n q^n$ να έχει $c_1 = 1$. Τότε η τιμή c_n είναι ιδιοτιμή του $T_k(n)$. Επιπλέον ισχύει:

$$\begin{array}{ll} c_{p^r} c_p = c_{p^{r+1}} + p^{k-1} c_{p^{r-1}} & \text{γιά } p \text{ πρώτο, } p \not| N \\ c_{p^r} = (c_p)^r & \text{γιά } p \text{ πρώτο, } p | N \\ c_m c_n = c_{mn} & \text{αν } (m,n) = 1 \end{array}$$

Αρα η L-Σειρά $L(s,f) = \sum_{n=1}^{\infty} c_n n^{-s}$ αναλύεται σε γινόμενο Euler. Συγκεκριμένα ισχύει το παρακάτω

Θεώρημα 3.41 *(Hecke-Petersson) Ο χώρος $S_k(\Gamma_0(N))$ των παραβολικών μορφών είναι το ορθογώνιο άθροισμα των χώρων ισοδυνάμων ιδιομορφών. Κάθε χώρος ισοδυνάμων ιδιομορφών έχει ένα στοιχείο που είναι ταυτόχρονα ιδιομορφή γιά όλα τα $T_k(n)$. Κάθε ιδιομορφή $f \in S_k(\Gamma_0(N))$ που είναι ταυτόχρονα ιδιοδιάνυσμα γιά όλα τα $T_k(n)$ μπορεί να κανονικοποιηθεί έτσι ώστε το q ανάπτυγμα του $f(\tau) = \sum_{n=1}^{\infty} c_n q^n$ έχει $c_1 = 1$. Επιπλέον η L-σειρά $L(s,f)$ έχει ανάπτυγμα σε γινόμενο Euler:*

$$L(s,f) = \prod_{\substack{p \in \mathbb{P} \\ p | N}} \left[\frac{1}{1 - c_p p^{-s}} \right] \prod_{\substack{p \in \mathbb{P} \\ p \not| N}} \left[\frac{1}{1 - c_p p^{-s} + p^{k-1-2s}} \right]$$

το οποίο συγλίνει γιά $Re(s) > \frac{k}{2} + 1$.

3.5 Modular ελλειπτικές καμπύλες

Γιά να οδηγηθούμε στην απόδειξη του θεωρήματος Fermat θα πρέπει να συνδέσουμε την θεωρία L-σειρών ελλειπτικών καμπύλων με την θεωρία των L-σειρών των Hecke ιδιομορφών. Θα συμβολίζουμε με $J_0(N)$ την ιακωβιανή πολλαπλότητα της επιφάνειας Riemann $X_0(N)$.

Ορισμός 3.42 *Μιά ελλειπτική καμπύλη E υπέρ το $\mathbb{Q}$ θα λέγεται modular ελλειπτική καμπύλη οδηγού N αν η E είναι παράγοντας της $J_0(N)$ και το N είναι ελάχιστο.*

Η προβολή από το $J_0(N)$ στην E επάγει ένα μη τετριμμένο μορφισμό

$$\phi : X_0(N) \longrightarrow E.$$

Ο παραπάνω ορισμός, σύμφωνα με θεώρημα των Eichler-Schimura [Sh,Kn] είναι ισοδύναμος με την ύπαρξη κανονικοποιημένης Hecke ιδιομορφής f βάρους 2 τέτοιας ώστε

$$L(E,s) = L(f,s).$$

Εικασία Taniyama-Shimura:

Κάθε ελλειπτική καμπύλη υπέρ το $\mathbb{Q}$ είναι modular

Η αλήθεια της παραπάνω εικασίας είναι γνωστή για ελλειπτικές καμπύλες με μιγαδικό πολλαπλασιασμό, ενώ πρόσφατα (Οκτώβριος 1994) ο Wiles την απέδειξε γιά ημιευσταθείς ελλειπτικές καμπύλες. Είναι γνωστός αλγόριθμος ο οποίος "δούλεψε" κάθε φορά που εφαρμόστηκε σε συγκεκριμένη ελλειπτική καμπύλη και έδωσε την modular παραμετρικοποίηση. Θα τον εφαρμόσουμε σε ένα απλό σχετικά παράδειγμα [Za, σελ 225].

Παράδειγμα: Εστω η ελλειπτική καμπύλη $E/\mathbb{Q} := y(y-1) = (x+1)x(x-1)$. Εύκολα διαπιστώνουμε ότι έχει κακή αναγωγή μόνο γιά $p = 37$ και μάλιστα στην θέση αυτή η αναγωγή είναι πολλαπλασιαστικού τύπου. Ψάχνουμε γιά μορφισμό ορισμένο υπέρ το $\mathbb{Q}$

$$\phi : X_0(37) \longrightarrow E$$

$$\tau \longmapsto (\xi(\tau), \eta(\tau))$$

όπου οι συναρτήσεις μιγαδικής μεταβλητής ξ, η : από το $\mathbb{H}$ στο $\mathbb{C}$ πρέπει να ικανοποιούν:

- ξ, η παραμένουν αναλλοίωτες από την δράση της $\Gamma_0(N)$
- $\eta(\tau)^2 - \eta(\tau) = \xi(\tau)^3 - \xi(\tau)$
- $\eta, \xi \in \mathbb{Q}[q^{-1}][[q]]$

Ας υποθέσουμε ότι γνωρίζαμε την Hecke ιδιομορφή f ως πρός την $\Gamma_0(N)$ τότε θα πρέπει να ισχύει ότι

$$f\left(-\frac{1}{37\tau}\right) = \epsilon 37\tau^2 f(\tau)$$

όπου $\epsilon = \pm 1$. Υπολογίζουμε ότι $rank E(\mathbb{Q}) \geq 1$ συνεπώς λόγω του 3.15 το ϵ θα είναι καιʼανάγκην 1 (Στην πραγματικότητα $rank E(\mathbb{Q}) = 1$).

Αρα βλέπουμε πώς αν η f υπάρχει τότε

$$f \in S_2(\Gamma_0^*(37)) = S_2(\Gamma_0(37) \cup \Gamma_0(37)w),$$

όπου $w := \begin{pmatrix} 0 & -1 \\ 37 & 0 \end{pmatrix}$. Υπολογίζουμε, μέσω της 1.31, ότι το γένος της επιφάνειας Riemann $\mathrm{X}_0(37)$ είναι 2. Επιπλέον θεωρούμε την επιφάνεια πηλίκο $\mathrm{X}_0^*(37) = \mathrm{X}_0(37)/ < w >$, της οποίας το γένος είναι 1. Κοιτάζουμε στους πίνακες των Hecke ιδιομορφών βάρους 2 και επιπέδου 37 και βρίσκουμε μιά τέτοια ιδιομορφή:

$$f(\tau) = q - 2q^2 - 3q^3 + 2q^4 - 2q^5 + 6q^6 - q^7 + 0q^8 + 6q^9 + \ldots.$$

οι συναρτήσεις η, ξ αφού δεν είναι σταθερές θα έχουν πόλους, και οδηγούμενοι από την αλγεβρική τους σχέση δοκιμάζουμε:

$$\xi(\tau) = q^{-2} + Aq^{-1} + B + Cq + \ldots..$$
$$\eta(\tau) = q^{-3} + A'q^{-2} + B'q^{-1} + C' + \ldots.$$

Από την αντιστοιχία ολόμορφων διαφορικών και 2-cusp μορφών (πρόταση 3.25) έχουμε την σχέση

$$\phi^*\omega = \frac{1}{2\pi i} f(\tau) d\tau$$

όπου ω είναι το αναλλοίωτο διαφορικό της ελλειπτικής καμπύλης, $\omega = dx/(2y-1)$. Εχουμε λοιπόν άλλη μιά σχέση γιά τις η, ξ:

$$f(\tau) = \frac{1}{2\pi i} \frac{\xi'(\tau)}{2\eta(\tau) - 1},$$

από όπου υπολογίζουμε γιά παράδειγμα ότι $A = 2, A' = 3$ και συνεχίζοντας επαγωγικά μπορούμε να υπολογίσουμε όσους συντελεστές των ξ, η θέλουμε. Ετσι οι η, ξ θα πρέπει να έχουν την μορφή

$$\xi(\tau) = q^{-2} + 2q^{-1} + 5 + 9q + 18q^2 + 29q^3 + ...$$
$$\eta(\tau) = q^{-3} + 3q^{-2} + 9q^{-1} + 20 + 46q + 92q^2 + ...$$

Επιπλέον θα πρέπει να ισχύει ότι:

$$\xi(\tau) f(\tau)^2 \in M_4(\Gamma_0^*(37))$$
$$\eta(\tau) f(\tau)^3 \in M_6(\Gamma_0^*(37))$$

Υπολογίζουμε πάλι τους πρώτους συντελεστές των $\xi(\tau)f(\tau)^2,\ \eta(\tau)f(\tau)^3$ και διαλέγουμε στοιχεία $f_4(\tau), f_6(\tau)$ στους χώρους $M_4(\Gamma_0^*(37)), M_6(\Gamma_0^*(37))$ αντίστοιχα, ώστε οι πρώτοι t συντελεστές τους να ταυτίζονται με τους αντίστοιχους των $\xi(\tau)f(\tau)^2,\ \eta(\tau)f(\tau)^3$, όπου t είναι η μεγαλύτερη από τις διαστάσεις των $M_4(\Gamma_0^*(37)), M_6(\Gamma_0^*(37))$. Ορίζουμε τελικά τις συναρτήσεις:

$$\xi'(\tau) := \frac{f_4(\tau)}{f(\tau)^2}, \quad \eta'(\tau) := \frac{f_6(\tau)}{f(\tau)^3}$$

και πρέπει να ελέγξουμε τις προυποθέσεις που θέσαμε γιά τις η, ξ. Ο έλεγχος της ισότητας $\eta(\tau)^2 - \eta(\tau) = \xi(\tau)^3 - \xi(\tau)$ είναι ισοδύναμος με τον έλενγχο της $f_6^2 - f_6 f^3 = f_4^3 - f_4 f^4$. Και τα δύο μέλη ανήκουν στον $M_{12}(\Gamma_0(37))$ και επαληθεύουμε την ισότητα με έλεγχο πεπερασμένων συντελεστών, σε πλήθος όσο και η διάσταση του $M_{12}(\Gamma_0(37)) + 1$. Εντελώς όμοια ελέγχουμε και την συνθήκη $-2\pi i f = \xi'/(2\eta - 1)$. Δείξαμε το πως μπορεί να υπολογιστεί η modular παραμετρικοποίηση στο συγκεκριμένο παράδειγμα. Ο παραπάνω υπολογισμός γίνεται εύκολα στο πρόγραμμα θεωρίας αριθμών PARI(1.38). Απλά δίνουμε τις εντολές:

```
    logging on
? \serieslength=50
   series precision = 50 significant terms
? e=initell([0,0,-1,-1,0])
%1 = [0, 0, -1, -1, 0, 0, -2, 1, -1, 48, -216, 37, 110592/37,
[0.8375654352833230354448108990, 0.2695944364054445582629379513,
 -1.107159871688767593707748850]~, 2.993458646231959629832009979,
 2.451389381986790060854224831*i, -0.4713192779568114758825938970,
```

```
 -1.435456518668684318723208856*i, 7.338132740789576739070721003]
? taniyama(e)
%2 = [x^-2 + 2*x^-1 + 5 + 9*x + 18*x^2 + 29*x^3 + 51*x^4 + 82*x^5
 + 131*x^6 + 199*x^7 + 306*x^8 + 450*x^9 + 666*x^10 + 957*x^11 +
1375*x^12 + 1934*x^13 + 2719*x^14 + 3752*x^15 + 5174*x^16 + 7040*x^17
+ 9546*x^18 + 12812*x^19 + 17146*x^20 + 22735*x^21 + 30062*x^22 +
39450*x^23 + 51606*x^24 + 67087*x^25 + 86948*x^26 + 112053*x^27 +
143997*x^28 + 184158*x^29 + 234839*x^30 + 298198*x^31 + 377636*x^32 +
476387*x^33 + 599436*x^34 + 751672*x^35 + 940242*x^36 + 1172467*x^37 +
 1458650*x^38 + 1809476*x^39 + 2239760*x^40 + 2765095*x^41 +
3406462*x^42 + 4186448*x^43 + 5134805*x^44 + 6283800*x^45 + 7675390*x^46
+ 9355533*x^47 + 11382898*x^48 + O(x^49),

 -x^-3 - 3*x^-2 - 9*x^-1 - 20 - 46*x - 92*x^2 - 180*x^3 - 329*x^4 -
 593*x^5 - 1023*x^6 - 1736*x^7 - 2862*x^8 - 4655*x^9 - 7402*x^10 -
11633*x^11 - 17973*x^12 - 27469*x^13 - 41419*x^14 - 61865*x^15 -
91358*x^16 - 133803*x^17 - 194102*x^18 - 279474*x^19 - 399118*x^20 -
566184*x^21 - 797440*x^22 - 1116406*x^23 - 1553106*x^24 - 2148803*x^25
 - 2956292*x^26 - 4046961*x^27 - 5511931*x^28 - 7473009*x^29 -
10085277*x^30 - 13553543*x^31 - 18138208*x^32 - 24179673*x^33 -
32109300*x^34 - 42486439*x^35 - 56017618*x^36 - 73611740*x^37 -
96413598*x^38 - 125885577*x^39 - 163863312*x^40 - 212677758*x^41 -
275244944*x^42 - 355246439*x^43 - 457273699*x^44 - 587093438*x^45 -
751873850*x^46 - 960576291*x^47 + O(x^48)]
? \q
```

Η απάντηση δόθηκε σε πραγματικό χρόνο. Πρόκειται γιά τους 50 πρώτους όρους των σειρών η, ξ.

4 $X^n + Y^n = Z^n$

4.1 Από τον Kummer στον Frey

Σε αυτή την παράγραφο θα προσπαθήσουμε να δώσουμε, σε σύγχρονη πάντα γλώσσα την εξέλιξη των ιδεών που οδήγησαν πρόσφατα στην λύση της τελευταίας εικασίας του Fermat.

Ορισμός 4.1 *Η επέκταση L/K θα λέγεται μη-διακλαδιζομένη αν καμμία εκτίμηση του K αρχιμήδεια ή όχι δεν διακλαδίζεται.*

Θεώρημα 4.2 *(Hilbert) Εστω K ένα αλγεβρικό σώμα αριθμών. Υπάρχει πεπερασμένη αβελιανή και μη διακλαδιζομένη επέκταση του Galois $K^{(1)}/K$, μέγιστη ως προς αυτή την ιδιότητα.*

Το $K^{(1)}$ θα λέγεται σώμα κλάσεων του Hilbert (Hilbert class field). Γιά κάθε πρώτο (ακέραιο) ιδεώδες του K, ο αυτομορφισμός του Frobenius [Av1] ορίζεται ως:

$$\sigma_P = \left(\frac{K^{(1)}/K}{P} \right) \text{ από } \sigma_P(x) = x^{N(P)} mod\, Q$$

όπου Q ένα πρώτο ιδεώδες του $K^{(1)}$ που βρίσκεται πάνω από το P. Επεκτείνουμε πολλαπλασιαστικά στην ομάδα κλάσεων και έχουμε την συνάρτηση του Artin γιά την επέκταση $K^{(1)}/K$:

$$\phi_{K^{(1)}/K} : I_K \longrightarrow Gal(K^{(1)}/K)$$

Ισχύει ότι $\phi_{K^{(1)}/K}$ είναι επί και ότι $Ker\phi_{K^{(1)}/K} = H_K$. Ο ισομορφισμός $I_K/H_K \simeq Gal(K^{(1)}/K)$ λέγεται νόμος αντιστροφής του Artin. Οπου I_K, H_K οι ομάδες των ιδεωδών, κυρίων ιδεωδών του σώματος K.

Πρόταση 4.3 *Αν $P \in \mathbb{P}(K)$ τότε το P αναλύεται πλήρως στο $K^{(1)}$ ανν $(\frac{K^{(1)}/K}{P}) = 1$.*

Πράγματι τότε η επέκταση S/Q / R/P θα ήταν βάθμου 1 και δεν θα είχαμε αδράνεια.

Ενδιαφερόμαστε γιά την ύπαρξη μη-τετριμμένων λύσεων στην εξίσωση του Fermat

$$x^p + y^p = z^p, \quad p \text{ πρώτος διάφορος του } 2$$

Η ιδέα του Kummer ήταν να θεωρήσουμε το κυκλοτομικό σώμα

$$K = \mathbb{Q}(\zeta_p)$$

και να μελετήσουμε της μη-διακλαδιζόμενες αβελιανές επεκτάσεις του K των οποίων ο βαθμός επέκτασης υπέρ το K να είναι δύναμη του p. Στην αποκαλούμενη "κανονική περίπτωση" δηλαδή όταν $p \not| h_k$, δεν υπάρχει τέτοια επέκταση διότι θα έπρεπε, αν υπήρχε, έστω μία επέκταση να είχαμε $K \subsetneq L \subsetneq K^{(1)}$ δηλαδή θα έπρεπε $p | [K^{(1)} : K] = h_k$, άτοπο. Το παραπάνω αποτέλεσμα μεταφέρεται στην γλώσσα των παραστάσεων ως εξής:

Η μη-ύπαρξη μονοδιάστατης μη-διακλαδιζομένης παράστασης της ομάδας Galois $Gal(\bar{\mathbb{Q}}/\mathbb{Q}(\zeta_p))$,

$$\rho : Gal(\bar{\mathbb{Q}}/\mathbb{Q}(\zeta_p)) \longrightarrow GL_1(\mathbb{C})_p$$

συναπάγει την εικασία του Fermat γιά τον p.

Ο Frey αντί να θεωρήσει μονοδιάστατες παραστάσεις ομάδων Galois κυκλοτομικών σωμάτων προχώρησε στην αμέσως επομένη γενίκευση δηλαδή στις ελλειπτικές καμπύλες. Θεώρησε την διδιάσταιη παράσταση με ”μικρή” διακλάδωση:

$$\rho : Gal(\bar{\mathbb{Q}}/\mathbb{Q}(\zeta_p)) \longrightarrow Aut(E[p]) = GL_2(\mathbb{F}_p)$$

και υποθέτοντας την αλήθεια της εικασίας των Taniyama-Shimura έδωσε την μη ύπαρξη ακέραιων λύσεων της εξίσωσης Fermat. Γιά να εξηγήσουμε καλύτερα τα παραπάνω θα χρειαστεί να αναπτύξουμε μερικά εργαλεία στις επόμενες παραγράφους, γιά μία στοιχειώδη εισαγωγή στην θεωρία παραστάσεων δες [Αν2].

4.2 Καμπύλες του Tate

Θεώρημα 4.4 *(Tate) Εστω* K *μιά πεπερασμένη επέκταση του σώματος* $\mathbb{Q}_l$ *των l-αδικών αριθμών με Hasse αναλλοίωτο* $\delta_E \in K^{*2}$ *και υποθέτουμε ότι η* E *έχει αναγωγή πολλαπλασιαστικού τύπου modl. Τότε η ομάδα των* K*-ρητών σημείων της* $\mathrm{E}, \mathrm{E(K)}$ *είναι αναλυτικά-αλγεβρικά ισόμορφη με το πηλίκο* $\mathrm{K}^*/q^{\mathbb{Z}}$ *όπου* q *η l-αδική περίοδος της* E, $q \in \mathbb{Q}_l$ *και* $j_E = \frac{1}{q} + \sum_{i=0}^{\infty} a_i q^i$. *Οι συντελεστές* a_i *είναι ακριβώς οι ακέραιοι που εμφανίζονται στο ανάπτυγμα Fourier της κλασικής j-αναλλοιώτου πάνω από το* $\mathbb{C}$ *(με* $q = e^{2\pi i\tau}$*)*

Απόδειξη: Προσπαθούμε να ορίσουμε το ανάλογο των ελλειπτικών καμπύλων στο $\mathbb{C}$ σε πεπερασμένες επεκτάσεις l-αδικών σωμάτων. Αντί λοιπόν να θεωρήσουμε πηλίκα της μορφής $\mathbb{C}/\Lambda$ οπού Λ διακριτή προσθετική υποομάδα του $\mathbb{C}$, επιχειρούμε να κάνουμε το ίδιο για το K, όπου K πεπερασμένη επέκταση του $\mathbb{Q}_l$. Δυστυχώς τα p-αδικά σώματα αριθμών δεν έχουν διακριτές προσθετικές υποομάδες αφού αν L μια τέτοια και $w \in L$ τότε $p^n w \in L$ και $v(p^n w) \longrightarrow 0$ άρα το 0 είναι σημείο συσσώρευσης του L συνεπώς $L = 0$. Μελετώντας την κλασική περίπτωση βλέπουμε οτι η κανονικοποιημένη εκθετική συνάρτηση $exp(2\pi iz)$ είναι ισομορφισμός του $(\mathbb{C}, +) \longrightarrow (\mathbb{C}^*, \cdot)$ και επιπλέον μέσω αυτού το δικτυωτό $\Lambda = \mathbb{Z} \oplus \tau\mathbb{Z}$ απεικονίζεται στην πολλαπλασιαστική υποομάδα του $\mathbb{C}^*, q^{\mathbb{Z}}$ όπου $q = e^{2\pi i\tau}$ και συνεπώς η ελλειπτική καμπύλη $\mathrm{E}_\Lambda(\mathbb{C}) \cong \mathbb{C}/\Lambda \cong \mathbb{C}^*/q^{\mathbb{Z}}$. Το $\bar{\mathbb{Q}}_l$ έχει διακριτές υποομάδες $q^{\mathbb{Z}}$ και θα προσπαθήσουμε να ορίσουμε τον αναλυτικό ισομορφισμό, αρχικά τυπικά, οδηγούμενοι απο τους αντίστοιχους τύπους για τις ελλειπτικές καμπύλες ορισμένες υπέρ το $\mathbb{C}$. Ας ξεκινήσουμε πρώτα με μερικούς υπολογισμούς σχετικούς με την συνάρτηση Weierstrass ως προς το δικτυωτό $\mathbb{Z} \oplus \tau\mathbb{Z}$. Εξ ορισμού

$$\wp(z : \tau) = \frac{1}{z^2} + \sum_{(m,n)\neq(0,0)} \frac{1}{(z - m - n\tau)^2} - \sum_{(m,n)\neq(0,0)} \frac{1}{(m + n\tau)^2}$$

Ισχύει [Ah, σελ.188] ότι:

$$\frac{\pi^2}{(sin\pi z)^2} = \sum_{m\in\mathbb{Z}} (z-m)^{-2}.$$

Επομένως αν $n \neq 0$ έχουμε:

$$\sum_{(m,n)\neq(0,0)} \frac{1}{(z-m-n\tau)^2} - \sum_{(m,n)\neq(0,0)} \frac{1}{(m+n\tau)^2} = \left(\frac{\pi}{sin\pi(z-n\tau)}\right)^2 - \left(\frac{\pi}{sin\pi n\tau}\right)^2$$

και αν $n = 0$ ομοίως:

$$\frac{1}{z^2} + \sum_{m\neq 0} \frac{1}{(z-m)^2} - \sum_{m\neq 0} \frac{1}{m^2} = \sum_{m\in\mathbb{Z}} \frac{1}{(z-m)^2} - 2\sum_{m=1}^{\infty} \frac{1}{m^2} =$$

$$= \frac{\pi^2}{(sin\pi z)^2} - 2\zeta(2) = \frac{\pi^2}{(sin\pi z)^2} - \frac{\pi^2}{3}$$

οπότε τελικά έχουμε:

$$\wp(z:\tau) = \sum_{n\in\mathbb{Z}} \left(\frac{\pi}{sin\pi(z+n\tau)}\right)^2 - \sum_{n\neq 0} \left(\frac{\pi}{sin\pi n\tau}\right)^2 - \frac{\pi^2}{3}.$$

Εισάγουμε τις καινούργιες μεταβλητές:

$$X = e^{2\pi i z}, q = e^{2\pi i \tau}$$

και έχουμε:

$$\frac{\pi^2}{(sin\pi(z+n\tau))^2} = (2\pi i)^2 \frac{q^n X}{(1-q^n X)^2}.$$

Συνεπώς:

$$\wp(z:\tau) = (2\pi i)^2 \left[\sum_{n\in\mathbb{Z}} \frac{q^n X}{(1-q^n X)^2} + \frac{1}{12} - \sum_{n\neq 0} \frac{q^n}{(1-q^n)^2}\right] =: (2\pi i)^2 P(X)$$

όπου

$$P(X) := P(X;q) := \sum_{n\in\mathbb{Z}} \frac{q^n X}{(1-q^n X)^2} + \frac{1}{12} - 2\sum_{n\geq 1} \frac{q^n}{(1-q^n)^2}$$

Παρατηρούμε ότι ο τελευταίος όρος αυτής της σειράς μπορεί να εκφρασθεί λίγο διαφορετικά:

$$(1-q^n)^{-2} = 1 + 2q^n + 3q^{2n} + \ldots\ldots$$

άρα

$$\frac{q^n}{(1-q^n)^2} = q^n + 2q^{2n} + 3q^{3n} + \ldots.$$

$$\sum_{n\geq 1} \frac{q^n}{(1-q^n)^2} = \sum_{n\geq 1, m\geq 1} m q^{mn} = \sum_{m\geq 1} m \sum_{n\geq 1} q^{mn} = \sum_{m\geq 1} m \frac{q^m}{1-q^m} =: s_1(q)$$

όπου κάνουμε χρήση του γενικότερου συμβολισμού:

$$s_k(q) := \sum_{m\geq 1} m^k \frac{q^m}{1-q^m} = \sum_{N\geq 1} \sigma_k(N) q^N \quad (k \in \mathbb{N})$$

και με $\sigma_k(N)$ συμβολίζουμε το άθροισμα των k δυνάμεων των διαιρετών του N. Τελικά έχουμε:

$$P(X) = \sum_{n\in\mathbb{Z}} \frac{q^n X}{(1-q^n X)^2} + \frac{1}{12} - 2s_1(q)$$

Ορίζουμε τον διαφορικό τελεστή

$$D := X\frac{d}{dX} = (2\pi i)^{-1}\frac{d}{dz}, X = e^{2\pi i z}$$

και έχουμε: $\frac{d}{dz}\wp(z;\tau) = (2\pi i)^3 DP$ συνεπώς μπορούμε να βρούμε την διαφορική εξίσωση γιά την P.

$$(2\pi i)^6 (DP)^2 = (\wp')^2 = 4\wp^3 - g_2\wp - g_3 = 4(2\pi i)^6 P^3 - (2\pi i)^2 g_2 P - g_3$$

Εύκολα υπολογίζουμε ότι:

$$DP(X) = DP(X;q) = \sum_{n\geq 1} \frac{q^n X + q^{2n} X^2}{(1-q^n X)^3}.$$

Θέτουμε:

$$g_2' = (2\pi i)^{-4} g_2 = \frac{1 + 240 s_3(q)}{12}$$

$$g_3' = (2\pi i)^{-6} g_3 = -\frac{1 - 504 s_5(q)}{216}$$

επιπλέον ισχύει:

$$j = 12^3 \frac{g_2^3}{\Delta} = 12^3 \frac{g_2'^3}{\Delta'} = q^{-1} + \sum_{n \geq 0} c(n) q^n, \quad \Delta' = (2\pi)^{-12} \Delta$$

Το πλεονέκτημα αυτών των εκφράσεων είναι η απαλλαγή από το π και το ότι οι εξισώσεις του Tate έχουν νόημα και σε τοπικά σώματα αριθμών. Οι συναρτήσεις P, DP παραμετρίζουν την ελλειπτική καμπύλη

$$y^2 = 4x^3 - g_2' x - g_3'.$$

Θεωρούμε τώρα τον μετασχηματισμό:$X = x - \frac{1}{12}, Y = \frac{1}{2}y + \frac{1}{2}(x - \frac{1}{12})$ και τελικά έχουμε την καμπύλη στην μορφή Tate:

$$Y^2 - XY = X^3 - h_2 X - h_3$$

όπου εύκολα υπολογίζουμε ότι :

$$h_2 = 5 \sum_{n=1}^{\infty} \frac{n^3 q^n}{1 - q^n}, \quad h_3 = 1/12 \sum_{n=1}^{\infty} \frac{(5n^3 + 7n^5) q^n}{1 - q^n}$$

και

$$X(w) = \sum_{n \in \mathbb{Z}} \frac{q^n w}{(1 - q^n w)^2} - 2 \sum_{n=1}^{\infty} \frac{n q^n}{1 - q^n}$$

$$Y(w) = \sum_{n \in \mathbb{Z}} \frac{(q^n w)^2}{(1 - q^n w)^3} - \sum_{n=1}^{\infty} \frac{n q^n}{1 - q^n}$$

και έχουμε παραμέτρηση της καμπύλης του Tate. Μεταφέρουμε τώρα την όλη θεωρία σε τοπικά σώματα αριθμών πλήρη ως προς μια μη-αρχιμήδεια εκτίμηση. Αν q στοιχείο ενός τέτοιου σώματος με $0 < |q| < 1$, θεωρούμε τις παραπάνω σειρές ως συναρτήσεις του $w \in K$, $w \neq 0$. Λόγω ultrametric τριγωνικής ανισότητας βλέπουμε ότι αυτή η συνθήκη στο q είναι αναγκαία και ικανή για να συγκλίνουν οι παραπάνω σειρές γιά όλα τα w. Το ερώτημα που θα προσπαθήσουμε τώρα να απαντήσουμε είναι για ποιές τιμές j του K^* υπάρχει πολλαπλασιαστική ομάδα της μορφής $q^{\mathbb{Z}}$ του K^* τέτοια ώστε η απόλυτη αναλλοίωτος της καμπύλης $K^*/q^{\mathbb{Z}}$ να ισούτε με j. Ισχύει το παρακάτω:

Θεώρημα 4.5 *Γιά κάθε $j \in K^*$ τέτοιο ώστε $|j| > 1$ υπάρχει μοναδική καμπύλη του Tate με απόλυτη αναλλοίωτο j.*

Απόδειξη: Παρατηρούμε ότι αν

$$f(x) = \sum_{n \geq 0} c_n x^n$$

είναι μία τυπική σειρά με συντελεστές $c_n \in K : |c_n| \leq 1$ τότε η $x \longmapsto 1/x + f(x)$ ορίζει αμφιμονότιμη συνεχή συνάρτηση ανάμεσα στα $0 < |x| < 1$ και στο $|x| > 1$. Πράγματι η σειρά συγκλίνει γιά $|x| < 1$ αφού η μετρική προέρχεται από μη-αρχιμήδεια εκτίμηση. Αρα η $1/x + f(x)$ είναι καλά ορισμένη και συνεχής. Γιά το ένα προς ένα έχουμε:

$$\frac{1}{x} + f(x) = \frac{1}{y} + f(y) \Rightarrow \frac{y - x}{xy} = f(y) - f(x) = \sum_{n \geq 1} c_n (y^n - x^n) =$$

$$= \sum_{n\geq 1} c_n(y-x)(y^{n-1}+...+x^{n-1}).$$

Επειδή υποθέσαμε όμως ότι $|x|, |y| < 1$, έπεται ότι το άθροισμα $y^{n-1}+...+x^{n-1}$ ανήκει στον μοναδιαίο δίσκο, συνεπώς έχουμε:

$$\frac{|y-x|}{|xy|} < |y-x| \Rightarrow |y-x| = 0 \Rightarrow y = x.$$

Σταθεροποιούμε ένα $y \in K$ με $|y| > 1$ και ορίζουμε επαγωγικά ακολουθία $\{x_i\}_{i\geq 0}$ ώς εξής:

$$x_0 = 0,\ x_{i+1} = y^{-1}(1 + x_i f(\chi_i)).$$

Εχουμε επαγωγικά ότι $|x_i| < 1$, συνεπώς

$$x_{i+1} - x_i = y^{-1}(x_i f(x_i) - x_{i-1} f(x_{i-1})) = y^{-1}\sum_{n\geq 0} c_n (x_i - x_{i-1})(x_i^n + ... + x_{i-1}^n)$$

$$|x_{i+1} - x_i| \leq |y^i| \cdot |x_1 - x_0| = \left|\frac{1}{y}\right|^i \cdot |x_1|$$

και αφού $|1/y| < 1$ η ακολουθία $\{x_i\}_{i\geq 0}$ είναι Cauchy άρα συγλίνουσα. Οι πράξεις του τοπικού σώματος είναι συνεχείς συνεπώς το όριο της παραπάνω ακολουθίας ικανοποιεί την σχέση: $x = y^{-1}(1 + xf(x)) \Leftrightarrow y = x^{-1}(1 + xf(x))$, δηλαδή η συνάρτηση f είναι και επί.

Λήμμα 4.6 *Εστω K μιά πεπερασμένη επέκταση του σώματος $\mathbb{Q}_p$. Αν $x \in K$ με $|x| < 1$ τότε $1 + 4x$ είναι τετράγωνο στο K.*

Απόδειξη: Γνωρίζουμε ότι:

$$(1+4x)^{1/2} = 1 + \frac{1}{2}(4x) + \frac{1}{2}\left(-\frac{1}{2}\right)(4x)^2/2! + ...$$

όπου ο συντελεστής του x^k κατά προσέγγιση προσήμου δίνεται από τον τύπο

$$\frac{2}{k}\binom{2(k-1)}{k-1}$$

Παρατηρούμε ότι ισχύει:

$$\binom{2k}{k} = (2k-1)\frac{2}{k}\binom{2(k-1)}{k-1}$$

με $(k, 2k-1) = 1$ συνεπώς οι συντελεστές του x^k στο δυωνυμικό ανάπτυγμα είναι ακέραιοι, δηλαδή η σειρά συγλίνει p-αδικά και αποτελεί την τετραγωνική ρίζα του $1 + 4x$.

Πόρισμα 4.7 *Η Hasse αναλλοίωτος της ελλειπτικής καμπύλης $K^*/q^{\mathbb{Z}}$ με $|q| < 1$ είναι τετράγωνο.*

Απόδειξη: Πράγματι $\gamma = 216/24(1 + 240 s_3)(1 - 504 s_5)^{-1} = 9y^2$, αφού $|s_3|, |s_5| < 1$.

Θεώρημα 4.8 *Εστω* $\mathrm{E}/\mathbb{Q}$ *ελλειπτική καμπύλη με αναγωγή πολλαπλασιαστικού τύπου modl. Εστω* $\mathrm{E}[p]$ *η ομάδα των σημείων τάξης* p *της* $\mathrm{E}(\bar{K})$*, και έστω* K_p *το σώμα που προκύπτει από το* $\mathbb{Q}$ *με επισύναψη των συντεταγμένων των σημείων* $E[p]$ *στο* $\mathbb{Q}$*. Εστω* $\mathcal{L}$ *διαιρέτης του* l *στο* K_p *και* $\mathrm{K}_{p,\mathcal{L}}$ *η πλήρωση του* K_p *ως προς την θέση* $\mathcal{L}$*. Τότε* $\mathrm{K}_{p,\mathcal{L}} = \mathbb{Q}_p(\zeta_p, \sqrt[p]{j_E})$*.*

Απόδειξη:

Απο το θεώρημα καμπύλων του Tate έχουμε ότι $\exists\ q \in \mathbb{Q}_l$ τέτοιο ώστε $\mathrm{E}(\mathrm{K}_{p,\mathcal{L}}) \cong (\mathrm{K}_{p,\mathcal{L}})^*/q^{\mathbb{Z}}$ και προφανώς η ομάδα $E_p(\mathrm{K}_{p,\mathcal{L}}) \cong \frac{\mathbb{Z}}{p\mathbb{Z}} \times \frac{\mathbb{Z}}{p\mathbb{Z}}$. Εσω στοιχείο τάξης p στην $E(\mathrm{K}_{p,\mathcal{L}})$ τότε αν y η εικόνα του στην $(\mathrm{K}_{p,\mathcal{L}})^*/q^{\mathbb{Z}}$ έχουμε ότι $y^p \in q^{\mathbb{Z}}$ άρα $y = \zeta_p$ ή $y = \sqrt[p]{q}$ από όπου προκύπτει ότι $\mathbb{Q}_p(\zeta_p, \sqrt[p]{q}) \subseteq \mathrm{K}_{p,\mathcal{L}}$. Το q όμως ανήκει στο $\mathrm{K}_{p,\mathcal{L}}$ ανν j_E ανήκει σ'αυτό, συνεπώς $\mathbb{Q}_p(\zeta_p, \sqrt[p]{j_E}) \subseteq \mathrm{K}_{p,\mathcal{L}}$. Για τον αντίστροφο εγκλεισμό παρατηρούμε ότι κάθε πλήρες σώμα, επέκταση του $\mathbb{Q}$ που περιέχει τα σημεία ταξης p περιέχει το $\mathbb{Q}_p(\zeta_p, \sqrt[p]{j_E})$ Το $\mathrm{K}_{p,\mathcal{L}}$ είναι, εξ ορισμού, το ελάχιστο πλήρες σώμα με αύτη την ιδιότητα άρα

$$\mathbb{Q}_p(\zeta_p, \sqrt[p]{j_E}) = \mathrm{K}_{p,\mathcal{L}}.$$

Ορισμός 4.9 *Μιά ελλειπτική καμπύλη* $E/\mathbb{Q}$ *λέγεται ευσταθής αν έχει σταθερή αναγωγή ως προς όλους τους πρώτους.*

Πρόταση 4.10 *Εστω* E *ευσταθής ελλειπτική καμπύλη ορισμένη πάνω από το* $\mathbb{Q}$*,* K_p *η επέκταση του* $\mathbb{Q}$ *που προκύπτει επισυνάπτοντας τις συντεταγμένες των σημείων της* E *τάξης* p*. Το* K_p *είναι μη διακλαδιζόμενο υπέρ το* $\mathbb{Q}$ *στούς πρώτους* l *γιά τους οποίους ισχύει:*

$$l \neq p \text{ με } v_l(j_E) \geq 0$$

είτε

$$v_l(j_E) \equiv 0 mod p$$

Απόδειξη:

- Πρώτη περίπτωση: $l \neq p$ με $v_l(j_E) \geq 0$. Εχουμε δεί (2.14) ότι αν ο p δεν διαιρεί την τάξη του σώματος $k = \mathcal{R}/\pi\mathcal{R}$ και η αναγωγή είναι καλή, τότε έχουμε την εμφύτευση της ομάδας των στοιχείων τάξης p, $E(K_p)[p]$ στο $\tilde{E}(k)$.Ομως $|E(K_p)[p]| = p^2$ άρα έχουμε p^2 διαφορετικά σημεία τάξης p στο $\tilde{E}(k)$. Δηλαδή έχουμε ότι $|E(k)[p]| = p^2$ άρα δεν έχουμε διακλάδωση.
- Δευτερή περίπτωση: $v_l(j_E) \equiv 0 mod p$. Εχουμε $v(j_E) < 0$ συνεπώς, λόγω σταθερής αναγωγής καταναγκην, η αναγωγή θα είναι πολλαπλασιαστική. Εσω $l \in \mathbb{P}$. Κριτήριο γιά το αν ο l διακλαδίζεται είναι το κατά πόσο η νόρμα $|.|_l = c^{v_l}$ του $\mathbb{Q}$ και η επέκταση

της $|.|_l^* = c^{v_l^*}$ στο $\mathbb{Q}_l(\zeta_p, \sqrt[p]{j_E})$ έχουν το ίδιο σύνολο τιμών ή όχι. Αρκεί λοιπόν να ελέγξουμε τι γίνεται στα στοιχεία που επισυνάψαμε, ζ_p και $\sqrt[p]{j_E}$. Ισχύει:

$$v_l^*(\zeta_p) = v_l(N(\zeta_p))^{1/p} = v_l(1)^{1/p} = 0$$

και

$$v_l^*(\sqrt[p]{j_E}) = v_l(N(\sqrt[p]{j_E}))^{1/p} = v_l(j_E)^{1/p}.$$

Επειδή $j_E \in \mathbb{Q}_l$ συνεπάγεται ικανή και αναγκαία συνθήκη γιά να μην παίρνουμε επιπλέον τιμές είναι το $1/p$ να εξαφανίζεται και αυτό το πετυχαίνουμε μόνο στην περίπτωση που $p|v_l(j_E)$.

4.3 Ελλειπτικές καμπύλες σταθερής αναγωγής

Θέλουμε να κατασκευάσουμε ελλειπτικές καμπύλες E με σταθερή αναγωγή mod$p$ γιά όλους τους πρώτους p έτσι ώστε το σώμα K_p, όπως αυτό ορίστηκε στα προηγούμενα, να έχει "μικρή" διακλάδωση, υπέρ το $\mathbb{Q}(\zeta_p)$. Εστω λοιπόν δυό σχετικά πρώτοι ακέραιοι αριθμοί A και B τέτοιοι ώστε $B \equiv 0 mod 2^5$ και $A \equiv -1 mod 4$, θέτουμε $C := -A - B$. Θεωρούμε την ελλειπτική καμπύλη με εξίσωση:

$$E : y^2 = x(x - A)(x + B)$$

Κάνουμε τον μετασχηματισμό:

$$x = 4X$$
$$y = 8Y + 4X$$

και η δοθείσα εξίσωση της E γίνεται:

$$Y^2 + XY = X^3 + \frac{B - 1 - A}{4}X^2 - \frac{AB}{16}X$$

που λόγω των υποθέσεων γιά τα A, B είναι και αυτή ορισμένη υπέρ το $\mathbb{Z}$. Από τους τύπους της παραγράφου 2.1 υπολογίζουμε το $c_4 = B^2 + A^2 + AB$ και την διακρίνουσα $\Delta = 2^{-8}A^2B^2C^2$.

Απο τα παραπάνω έχουμε τα ακόλουθα συμπεράσματα γιά την E:

- Τα σημεία τάξης 2 της E είναι $\mathbb{Q}$-ρητά και είναι ίσα με $P_0 = (0, 0), P_1 = (A, 0), P_2 = (-B, 0)$.
- Μελετούμε τώρα την αναγωγή της E ως προς όλους τους πρώτους αριθμούς p:
  (a) $\underline{p = 2}$
  Εχουμε $v_2(\Delta) = v_2(2^{-8}A^2B^2C^2) > 0$ και $v_2(c_4) = v_2(A^2 + B^2 + AB) = 0$ αφού A περιττός. Αρα η E έχει αναγωγή πολλαπλασιαστικού τύπου mod2.
  (b) $\underline{p \neq 2}$
  Υποθέτουμε αρχικά ότι $p \not| ABC$, άρα $p \not| \Delta$, συνεπώς η E έχει καλή αναγωγή modp. Στην περίπτωση που $p|ABC$ έχουμε:

$$v_p(\Delta) = v_p(2^{-8}A^2B^2C^2) > 0 \text{ και}$$
$$v_p(c_4) = v_p(A^2 + B^2 + AB) = v_p((A+B)^2 - AB) = v_p(C^2 - AB) = 0.$$

Πράγματι αν $p \mid C^2 - AB$ τότε αν $p \mid A$ οπότε $p \mid C$ συνεπώς και $p \mid B$ άτοπο. Αν από την άλλη $p \mid C$ οπότε $p \mid A$ συνεπώς και $p \mid B$ πάλι άτοπο, επομένως έχουμε πολλαπλασιαστική αναγωγή.

Συνοψίζοντας η E έχει ευσταθή αναγωγή ως προς όλους τους πρώτους του $\mathbb{Q}$ και ο οδηγός της είναι ίσος ,εξ ορισμού, με

$$N := \prod_{l \mid ABC} l$$

- Παρατήρουμε ότι η παραπάνω εξίσωση αποτελεί ένα καθολικά ελάχιστο μοντέλο του Weierstrass, αφού γιά κάθε πρώτο p η εκτίμηση v_p της διακρίνουσας και του c_4 είναι μικρότερες του 12 και 4 αντίστοιχα.

Εστω τώρα η εξίσωση

$$C_p : a^p + b^p + c^p = 0$$

Θα αποδείξουμε ότι δεν έχει ακεραία λύση $a, b, c \in \mathbb{Z}$ με $abc \neq 0$. Χωρίς περιορισμό της γενικότητας (στην ανάγκη μεταθέτουμε κυκλικά τα a, b, c) μπορούμε να υποθέσουμε ότι $b \equiv 0 mod\, 2$, $a \equiv -1 mod\, 4$. Θέτουμε $A = a^p$, $B = b^p$, $C = c^p$ και έχουμε:

Πρόταση 4.11 *Εστω (a, b, c) μιά λύση της $a^p + b^p + c^p$ με $abc \neq 0$. Τότε η ελλειπτική καμπύλη $E_{A,B,C}$ που δίνεται από την καθολικά ελάχιστη εξίσωση:*

$$Y^2 = X^3 + \frac{(b^p - a^p - 1)}{4}X^2 - \frac{a^p b^p}{16}X$$

έχει σταθερή αναγωγή υπέρ το $\mathbb{Q}$. Τα σημεία της τάξεως 2 είναι $\mathbb{Q}$-ρητά. Ο οδηγός και η διακρίνουσα της είναι:

$$\mathrm{N} = \prod_{l \mid abc} l$$

$$\Delta_E = (2^{-4}abc)^{2p}.$$

Το σώμα K_p που προκύπτει από την επισύναψη των συντεταγμένων των σημείων τάξης p της E στο $\mathbb{Q}$ είναι μη-διακλαδιζόμενο, υπέρ το $\mathbb{Q}$ εκτός από τους διαιρέτες του $2p$.

<u>Απόδειξη:</u> Αν $v_l(j(E)) \geq 0$ τότε έχουμε καλή αναγωγή και σύμφωνα με προηγούμενη παρατήρηση διακλάδωση υπάρχει μόνο στους διαιρέτες του p. Αν έχουμε $v_l(j(E)) < 0$ δηλαδή $l \mid \Delta$, τότε έχουμε:

$$j_E = \frac{2^8(a^{2p}+b^{2p}+a^pb^p)^3}{(a^pb^pc^p)^2}$$

$$v_l(j_E) = v_l(2^8) + 3v_l(a^{2p}+b^{2p}+a^pb^p) - 2v_l(a^pb^pc^p) =$$

$$= v_l(2^8) + 3v_l((a^p+b^p)^2 - a^pb^p) - 2v_l(a^pb^pc^p) =$$

$$= v_l(2^8) + 3v_l(c^{2p} - a^pb^p) - 2v_l(a^pb^pc^p)$$

Στην περίπτωση μας, αφού $l \mid \Delta$, πρέπει το l να διαιρεί ακριβώς ένα άπο τα a, b, c το οποίο σημαίνει ότι το l δεν διαιρεί το $c^{2p} - a^pb^p$ από όπου έχουμε:

$$v_l(j_E) = v_l(2^8) - 2v_l(a^pb^pc^p)$$

Αν $l = 2$ τότε ισχύει ότι

$$v_2(j_E) = 8 - 2p \cdot max\{v_l(a), v_l(b), v_l(c)\}$$

και προφανώς έχουμε ότι:

$$v_2(j_E) \not\equiv 0 mod p$$

δηλαδή το 2 διακλαδίζεται.
Αν $l \neq 2$ τότε ισχύει :

$$v_l(j_E) = -2pv_l(a) - 2pv_l(b) - 2pv_l(c) \equiv 0 mod p$$

Αρα στους πρώτους αυτούς δεν έχω διακλάδωση.

Από την παραπάνω πρόταση βλέπουμε ότι η ύπαρξη μιας λύσης στην εξίσωση Fermat μας επιτρέπει να κατασκευάσουμε ελλειπτική καμπύλη ύπερ το $\mathbb{Q}$ με αξιοπερίεργες ιδιότητες. Η ιδέα του Frey ήταν να δείξει ότι μιά τέτοια ελλειπτική καμπύλη δεν είναι δυνατόν να υπάρχει. Πριν φτάσουμε όμως έκει ας δούμε και το αντίστροφο της προηγούμενης πρότασης:

Υποθέτουμε ότι $E/\mathbb{Q}$ ευσταθής ελλειπτική καμπύλη της οποίας όλα τα σημεία της τάξης 2 είναι $\mathbb{Q}$-ρητά. Επιπλέον υποθέτουμε ότι στην επέκταση $K_p/\mathbb{Q}$ διακλαδίζονται μόνο οι διαιρέτες του $2p$, και ότι $v_2(j_E) < 0$ καθώς και ότι

$$min(v_p(j_E), 0) \equiv 0 \equiv v_2(j_E) - 8 mod p.$$

Χωρίς περιορισμό της γενικότητας, ένα από τα ρητά σημεία είναι το $(0, 0)$, οπότε η καμπύλη γράφεται στην μορφή:

$$N_E : Y^2 = X^3 + AX^2 + BX$$

όπου $A, B \in \mathbb{Z}$ με (A,B) = 1. Πράγματι θεωρώ ένα καθολικά ελάχιστο μοντέλο του Weierstass, τέτοιο υπάρχει αφού $h_{\mathbb{Q}} = 1$ λόγω της πρότασης 2.2.0. Θα ήταν αδύνατο γιά τα A, B να μην ήταν πρώτα μεταξύ τους αφού τότε η αναγωγή modulo κοινό πρώτο διαιρέτη θα ήταν κακή.

Η διακρίνουσα και η απόλυτη αναλλοίωτος υπολογίζονται σε:

$$\Delta_{\mathrm{E}} = 16B^2(A^2 - 4B)$$

$$j_E = \frac{2^8(A^2 - 3B)}{B^2(A^2 - 4B)}$$

Το $B^2(A^2 - 4B)$ είναι μιά $2p$ δύναμη κάποιου ακεραίου αριθμού. Πράγματι αν $l \mid \Delta$ τότε $v_l(j_E) < 0$ οπότε αν $l \neq p$ επειδή το l δεν διακλαδίζεται στην επέκταση $K_p/\mathbb{Q}$ ισχύει $v_l(j_E) \equiv 0 mod\ p$. Αν $l = p$ τότε η παραπάνω ισοδυναμία ισχύει εξ υποθέσεως: $v_l(j_E) = 8v_l(2) - v_l(B^2(A^2 - 4B)) \equiv 0 modp$. Επομένως γιά $l|\Delta$και αν $l \neq 2$ τότε $v_l(j_E) = v_l(A^2 - 3B) - v_l(B^2(A^2 - 4B)) = -v_l(B^2(A^2 - 4B)) \equiv 0 modp$. Συνεπώς το l βρίσκεται σαν p δύναμη στο $B^2(A^2 - 4B)$. Αν τώρα $l|\Delta$, $l = 2$ τότε $v_2(j_E) = 8 - v_2(B^2(A^2 - 4B)) \equiv 0 modp$. Λόγω της υποθέσης έχουμε ότι και'ανάγκη $v_2(B^2(A^2 - 4B)) \equiv 0 modp$. Συνεπώς και το 2 εμφανίζεται σαν p δύναμη στον $B^2(A^2 - 4B)$. Απο την άλλη το $\mathrm{B}^2(\mathrm{A}^2 - 4B)$ είναι και αυτό τέλειο τετράγωνο, αφού το $\mathrm{A}^2 - 4B$ είναι διακρίνουσα του $\mathrm{X}^2 + \mathrm{AX} + \mathrm{B}$ το όποιο έχει δυό ρητές ρίζες.

Εστω λοιπόν $\mathrm{B}^2(\mathrm{A}^2 - 4B) = u^{2p}$ με $u \in \mathbb{Z}$. Επίσης έχουμε $(B, \mathrm{A}^2 - 4B) = 1$ άρα υπάρχουν $v, w \in \mathbb{Z}$ τέτοια ώστε $\mathrm{A}^2 - 4B = v^{2p}$ και $\mathrm{B} = w^p$. Συνεπώς :

$$(A - v^p)(A + v^p) = 4B = 4w^p.$$

Υπάρχουν τελικά στοιχεια $a, b \in \mathbb{Z}$ με $a^p b^p = B$ και

$$2A = 2^\lambda a^p + 2^\mu b^p \text{ με } 0 \leq \lambda, \mu \leq 2 \text{ και } \lambda + \mu = 2$$

και

$$2v^p = 2^\lambda a^p - 2^\mu b^p.$$

Αν υποθέσουμε ότι $\lambda = 0$, τότε $2 \mid a$ και τότε θα έπρεπε $2 \mid B$ και $2 \mid A$, άτοπο, άρα $\lambda \neq 0$. Ομοίως $\mu \neq 0$, άρα $\lambda = \mu = 1$ και $(a, -b, -v)$ είναι μιά λύση του προβλήματος Fermat. Συνοψίζοντας έχουμε το παρακάτω

Θεώρημα 4.12 *Γιά πρώτο $p \geq 5$ τα παρακάτω είναι ισοδύναμα:*

(a) *Υπάρχει λύση της εξίσωσης Fermat*

(b) *Υπάρχει ευσταθής ελλειπτική καμπύλη $E/\mathbb{Q}$ τέτοια ώστε:*

- *Τα σημεία τάξης 2 είναι $\mathbb{Q}$ ρητά,*
- *Το σώμα K_p που προκύπτει με επισύναψη των συντεταγμένων των σημείων τάξης p στο $\mathbb{Q}$ είναι μη διακλαδιζόμενο έκτος από τους διαιρέτες του $2p$,*
- $min(0, v_p(j_E)) \equiv 0 \equiv (v_2(j_E) - 8) mod p$.

(c) *Υπάρχει ευσταθής ελλειπτική καμπύλη $E/\mathbb{Q}$ με ελάχιστη εξίσωση της μορφής:*

$$Y^2 + XY = X^3 + aX^2 + bX \text{ με } a, b \in \mathbb{Z}$$

και $2^8 \Delta_E \in \mathbb{Z}^{2p}$.

Παρατήρηση: Η ονομαζόμενη 'πρώτη περίπτωση' της εικασίας Fermat είναι όταν p δεν διαιρεί το a, b, c. Αυτό αντιστοιχεί στην περίπτωση που p δεν διαιρεί την Δ_E της ελλειπτικής καμπύλης.

4.4 Εικασία Taniyama-Schimura και το θεώρημα του Fermat

Θεωρούμε μία ελλειπτική καμπύλη $E/\mathbb{Q}$, $E(\mathbb{C}) \simeq \mathbb{C}/\Lambda$, $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ με $Im(\omega_1/\omega_2) > 0$. Γιά κάθε $n \in \mathbb{N}$, $n \geq 1$, θεωρούμε την ομάδα των σημείων τάξης n,

$$E[n] := \{P \in E(\mathbb{C}) / n \cdot P = 0\}$$

Είναι προφανές ότι:

$$E[n] = \frac{\mathbb{Z}}{n\mathbb{Z}} \times \frac{\mathbb{Z}}{n\mathbb{Z}}$$

δηλαδή $E[n]$ ελεύθερο $\mathbb{Z}/n\mathbb{Z}$-module με τάξη 2. Τα σημεία $P \in E[n]$ είναι σημεία της E των οποίων οι συντεταγμένες οι οποίες επαληθεύουν συγκεκριμένες αλγεβρικές εξισώσεις με ρητούς συντελεστές (εξαρτώνται φυσικά από την εξίσωση ορισμού της E). Επομένως η πεπερασμένη ομάδα $E[n]$ αποτελείται απο σημεία της $E(\bar{\mathbb{Q}})$ και ισχύει: $\sigma(E[n]) = E[n], \ \forall \ \sigma \in Gal(\bar{\mathbb{Q}}/\mathbb{Q})$. Δηλαδή η ομάδα $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ δρά στήν $E[n]$ και μάλιστα διατηρεί την πράξη της ομάδος δηλαδή ισχύει $\sigma(P_1 + P_2) = \sigma(P_1) + \sigma(P_2)$ γιά κάθε $P_1, P_2 \in E[n]$ αφού πάλι ο νόμος πρόσθεσης δίνεται μέσω τύπων με συντελεστές ρητούς.

Επομένως, γιά κάθε $n \in \mathbb{N}, n \geq 1$,η δράση της $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ στην ομάδα των σημείων τάξης n επάγει μία παράσταση:

$$\rho_n : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow Aut(E[n]) \simeq GL_2\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)$$

η οποία είναι συνεχής, όπου η $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ είναι εφοδιασμένη με την τοπολογία του Krull (παράρτημα), ενώ η $GL_2(\mathbb{Z}/n\mathbb{Z})$ με την διακριτή τοπολογία. Η συνέχεια της ρ_n είναι ισοδύναμη με το ότι η υποομάδα $\mathrm{H}_n := Ker(\rho_n)$ είναι ανοιχτή. Σύμφωνα με την θεωρία Galois λοιπόν στην ομάδα H_n αντιστοιχεί το σώμα $\mathrm{K}_{\rho_n} := \bar{\mathbb{Q}}^H$, το οποίο είναι το σώμα που προκύπτει απο το $\mathbb{Q}$ με επισύναψη των συντεταγμένων των σημείων της ομάδος $E[n]$.

Ορισμός 4.13 *Θα λέμε ότι μία (συνεχής) παράσταση ρ της $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ είναι μη διακλαδιζομένη στον πρώτο p όταvν $\rho(I_l) = \{1\}$, όπου I_l είναι η ομάδα αδρανείας του l στην επέκαταση $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ (βλέπε παράρτημα).*

Παρατήρηση: $\rho(I_p) = \{1\}$ σημαίνει ότι $I_l \subseteq Ker\rho$ δηλαδή

$$K_p := \bar{\mathbb{Q}}^{I_p} \supseteq \bar{\mathbb{Q}}^{H} = K_\rho$$

δηλαδή ο p δεν διακλαδίζεται στην επέκταση $K_{\rho_n}/\mathbb{Q}$.

Ορισμός 4.14 *Μία παράσταση $\rho : G := Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(\mathbb{F}_l)$ θα λέγεται modular βάρους 2 και επιπέδου N, όταν*

(a) Η ρ είναι ανάγωγη παράσταση και

(b) Υπάρχει μία κανονικοποιημένη ιδιομορφή του Hecke $f \in S_2(\Gamma_0(N))$ τέτοια ώστε αν $f(z) = \sum_{n=1}^{\infty} a_n q^n$ με $a_n \in \mathbb{Z}$, είναι το ανάπτυγμα Fourier της f στο ∞ να ισχύει: $\forall\ p \in \mathbb{P}(\mathbb{Z})$, τέτοιο ώστε $p \not| lN$ έχουμε $tr(\rho(Frob_p)) \equiv a_p mod\ l$

Θεώρημα 4.15 *Η εικασία του Fermat είναι αληθής*

Γιά την απόδειξη θα χρειαστούμε:

Θεώρημα 4.16 *(Wiles 1994)[Wi] Κάθε ημιευσταθής ελλειπτική καμπύλη $E/\mathbb{Q}$ είναι modular.*

Θεώρημα 4.17 *(Ribet 1990)[Ri] Αν η παράσταση*

$$\rho : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(\mathbb{F}_l)$$

είναι modular επιπέδου N και επιπλέον

(a) Η ρ είναι απόλυτα ανάγωγη

(b) Η ρ είναι πεπερασμένη, δηλαδή εξ ορισμού $v_p(\Delta) \equiv 0 mod\ l$, γιά κάθε $p \in \mathbb{P}(\mathbb{Z})$, $p|N$

(c) $p \not\equiv 1 mod\ l$ είτε $l \not| N$

τότε η ρ είναι modular, επιπέδου N/p.

Θα δεχθούμε τα παραπάνω θεωρήματα χωρίς αποδείξεις και θα δούμε πως συνεπάγονται την αλήθεια της εικασίας του Fermat.

Είδαμε ότι μιά λύση του προβλήματος $X^l + Y^l = Z^l$ (a, b, c) με $abc \neq 0$ και, χωρίς περιορισμό της γενικότητας, b άρτιος, $a \equiv 1 mod\ 4$,$(a, b, c) = 1$ επάγει το ότι η ελλειπτική καμπύλη $E/\mathbb{Q}$ με εξίσωση Weierstrass:

$$E_F : y^2 = x(x - a^l)(x - b^l)$$

είναι ημιευσταθής. Στην συνέχεια θα θεωρούμε την $E[l]$ γιά τον πρώτο αυτό $l \geq 5$ και την παράσταση :

$$\rho_l^{E_F} : G = Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow GL_2(\mathbb{F}_l) \simeq Aut(E_F[l])$$

Ισχύουν:

Πρόταση 4.18 *$det(\rho_l) = \chi_l$,όπου χ_l ο modl κυκλοτομικός χαρακτήρας της $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$.*

[Se] Ο κυκλοτομικός χαρακτήρας δίνει την δράση της $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ στην ομάδα των l-ριζών της μονάδας στο $\bar{\mathbb{Q}}$, δηλαδή

$$\chi_l : Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathbb{F}_l^*$$

$Frob_p(\zeta_l) = \zeta_l^{\chi_l(p)}$.

Πρόταση 4.19 *(Mazur) Η παράσταση ρ_l είναι ανάγωγη.*

Απόδειξη: Υποθέτουμε ότι η ρ_l δεν είναι ανάγωγη, δηλαδή υπάρχουν δύο χαρακτήρες

$$\chi_1, \chi_2 : G = Gal(\bar{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathbb{F}_l^*$$

τέτοιοι ώστε η παράσταση να γράφεται στην μορφή:

$$\rho_l^{E_F} \simeq \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}.$$

Εστω $X \subseteq E[l]$ ο $\mathbb{F}_l$-διανυσματικός υπόχωρος του $E[l]$ διάστασης 1, $dim_{\mathbb{F}_l} X = 1$ ο οποίος παραμένει σταθερός ως προς την δράση της ομάδας G και αντιστοιχεί στον χαρακτήρα χ_1. Ο διανυσματικός υπόχωρος που αντιστοιχει στον χ_2 είναι $Y = E[l]/X$.

Λήμμα 4.20 *οι χαρακτήρες χ_1 και χ_2 δεν διακλαδίζονται σε κανένα πρώτο p, $p \neq l$.*

Απόδειξη: ξεχωρίζουμε περιπτώσεις:

- $p \not| N$ άρα η E_F έχει καλή αναγωγή $mod\ p$. Συνεπώς η p δεν διακλαδίζεται στο σώμα $K_l := \bar{\mathbb{Q}}^{Ker \rho_l^{E_F}}$, άρα και οι χαρακτήρες χ_1, χ_2 δεν διακλαδίζονται στο p.
- $p|N$ δηλαδή η ελλειπτική καμπύλη έχει πολλαπλασιαστική αναγωγή $mod\ p$. Οπως αποδείξαμε στο θεώρημα 4.4, υπάρχει $q \in \mathbb{Q}_p$ τέτοιο ώστε $|q|_p < 1$ και γιά το σώμα K_l ισχύει ότι $E_q(K_l) \simeq K^*/q^{\mathbb{Z}}$. Επιπλέον δείξαμε ότι $E_q(K_l)[l] \simeq \mu_l \times q^{\frac{1}{l}\mathbb{Z}}/q^{\mathbb{Z}}$, όπου με μ_l συμβολίζουμε την ομάδα των l-ριζών της μονάδας. Το παραπάνω είναι ισοδύναμο με το ότι η ακολουθία:

  $$0 \longrightarrow \mu_l \longrightarrow E_q[l] \longrightarrow \mathbb{Z}/l\mathbb{Z} \longrightarrow 0$$

  είναι ακριβής. Συνεπώς ο ένας χαρακτήρας είναι ο κυκλοτομικός και ο άλλος ο τετριμμένος. Επομένως και πάλι δεν έχουμε διακλάδωση γιά $p \neq l$.

Πρόταση 4.21 *Γιά την τιμή $p = l$ διακλαδίζεται το πολύ ένας χαρακτήρας.*

Απόδειξη: [Se]

Γιά την τιμή $p = l$, έχουμε ότι ο ένας χαρακτήρας διακλαδίζεται και ότι ο άλλος όχι. Αυτός που δεν διακλαδίζεται θα είναι ο τετριμμένος σύμφωνα με το θεώρημα του Minkowski [Av1]. Ο άλλος θα είναι ο κυκλοτομικός χ_l. Χωρίς περιορισμό της γενικότητας $\chi_1 = 1,\ \chi_2 = X_l$. Δηλαδή έχουμε ότι:

$$E_F(\mathbb{Q})_{torsion} \supseteq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z}$$

Αρα $|E_F(\mathbb{Q})_{torsion}| \geq 20$ αφού $l \geq 5$ το οποίο είναι άτοπο λόγω του θεωρήματος του Mazur (2.22).

Εχουμε δεί ότι ισχύουν:

Γιά κάθε πρώτο $p \not| N$,όπου N είναι ο οδηγός της E_F, η παράσταση ρ_l είναι μη διακλαδιζομένη στο p.

Μάλιστα, ισχύει:

$$tr(\rho_l^{E_F}(Frob_p)) \equiv a_p mod\ l$$

Πρόταση 4.22 *Υποθέτουμε ότι $p \neq l$ και ότι $p|N$. Τότε η $\rho_l^{E_F}$ είναι μη διακλαδιζομένη στο p, τότε και μόνο τότε όταν*

$$v_p(\Delta) \equiv 0 mod\ l$$

Παρατήρηση: Από την παραπάνω πρόταση μπορούμε να απαλείψουμε την υπόθεση $p|N$. Αυτό διότι αν $p \not| N$ τότε $v_p(\Delta) = 0$, οπότε κατά μείζονα λόγω ισχύει $v_p(\Delta) \equiv 0 mod\ l$

Είμαστε σε θέση να αποδείξουμε το θεώρημα του Fermat. Λόγω του Θεωρήματος του Wiles η παράσταση $\rho_l^{E_F}$ είναι modular, βάρους 2 και επιπέδου $N = N_{E_F}$. Το N είναι ελεύθερο τετραγώνου και φυσικά $2|N$. Αν $l|N$ τότε εφαρμόζουμε το θεώρημα του Ribet γιά $p = l$ (αφού $l \not\equiv 1 mod\ l$) από όπου έχουμε ότι $\rho_l^{E_F}$ modular επιπέδου $N_0 = N/l$.

Ξαναγράφουμε αντί γιά N_0 το N, και έχουμε ότι η $\rho_l^{E_F}$ είναι modular επιπέδου N με $l \not| N$. Ξαναεφαρμόζουμε Ribet, όπου μπορούμε να πάρουμε $p|N,\ p \in \mathbb{P},\ p \neq 2$ και αποδεικνύουμε τελικά ότι η $\rho_l^{E_F}$ είναι modular επιπέδου N/p. Συνεχίζουμε με αυτόν τον τρόπο, με όλους τους περιττούς πρώτους η $\rho_l^{E_F}$ είναι modular επιπέδου 2. Αυτό όμως είναι άτοπο αφού $dim S_2(\Gamma_0(2)) = 0$, δηλαδή η εικασία του Fermat είναι αληθής.

5 Παράρτημα

5.0.1 Θεωρία Galois

Σκοπός αυτής της παραγράφου είναι να επεκτείνουμε την θεωρία Galois των πεπερασμένων αλγεβρικών επεκτάσεων σε επεκτάσεις άπειρης διάστασης. Εδώ το θεμελιώδες θεώρημα της συνήθους θεωρίας, της ένα προς ένα αντιστοιχίας μεταξύ ενδιάμεσων σωμάτων και υποομάδων δεν ισχύει, υπάρχουν ποιό πολλές υποομάδες από ενδιάμεσα σώματα. Υπάρχει όμως η γενίκευση της θεωρίας, που οφείλεται στον Krull.

Ορισμός 5.1 *(Τοπολογία του Krull) Εστω N/K επέκταση του Galois με ομάδα Galois (πεπερασμένη ή άπειρη) $G := Gal(N/K)$. Ορίζουμε σαν βάση ανοιχτών περιοχών του $\sigma \in G$ το*

$$\mathcal{B}_\sigma := \{\sigma Gal(N/L)/N \subset L \subset K, \text{με } L/K \text{ πεπερασμένη και } Galois\}$$

και διαπιστώνουμε ότι έχουμε καλά ορισμένη βάση ανοιχτών περιοχών.

Επιπλέον η G είναι τοπολογική ομάδα δηλαδή οι συναρτήσεις:

$$\begin{array}{rcl} G \times G & \longrightarrow & G \\ (\sigma, \tau) & \longmapsto & \sigma\tau \\ G & \longrightarrow & G \\ \sigma & \longmapsto & \sigma^{-1} \end{array}$$

είναι συνεχείς. Πράγματι η αντίστροφη εικόνα της $\sigma\tau Gal(N/L)$ περιέχει την ανοιχτή περιοχή $(\sigma Gal(N/L), \tau Gal(N/L))$ της (σ, τ), αφού $Gal(N/L) \lhd Gal(N/K)$.

Διαπιστώνουμε ότι αν N/K είναι πεπερασμένη τότε η τοπολογία του Krull είναι διακριτή. Αν $\tau, \sigma \in Gal(N/K), \tau \in \sigma Gal(N/L) \Leftrightarrow \sigma^{-1}\tau \in Gal(N/L) \Leftrightarrow \sigma^{-1}\tau(x) = x \;\forall\; x \in L$. Δηλαδή $\sigma|_L = \tau|_L$. Με άλλα λόγια δύο στοιχεία $\sigma, \tau \in G$ είναι "κοντά" ως προς την τοπολογία του Krull όταν συμπίπτουν γιά επέκταση του K μεγάλου βαθμού.

Θεώρημα 5.2 *Η ομάδα Galois $Gal(N/K)$ με την τοπολογία του Krull είναι Hausdorff και συμπαγής.*

Απόδειξη: Εσιω $\sigma, \tau \in G$ με $\sigma \neq \tau$ συνεπώς υπάρχει πεπερασμένη επέκταση του K η L τέτοια ώστε $\sigma|_L \neq \tau|_L$ συνεπώς $\sigma Gal(N/L) \neq \tau Gal(N/L)$ και συνεπώς $\sigma Gal(N/L) \cap \tau Gal(N/L) = \emptyset$ δηλαδή η G είναι Hausdorff.

Γιά την απόδειξη της συμπάγειας θεωρούμε την απεικόνιση

$$\begin{array}{c} h : G \longrightarrow \prod_L Gal(L/K) \\ \sigma \longmapsto \prod_L \sigma|_L \end{array}$$

όπου τα L διατρέχουν τις πεπερασμένες επεκτάσεις Galois του σώματος K. Βλέπουμε τις πεπερασμένες ομάδες $Gal(L/K)$ ώς διακριτές, συμπαγείς τοπολογικές ομάδες και συνεπώς το γινόμενο τους σύμφωνα με το θεώρημα του Tychonoff είναι συμπαγής τοπολογικός χώρος. Ο ομομορφισμός h είναι ένα προς ένα, αφού $\sigma|_L = 1$ γιά όλες τις L είναι ισοδύναμο με $\sigma = 1$. Οταν το L_0/K διατρέχει τις πεπερασμένες επεκτάσεις του K και $\sigma' \in Gal(L_0/K)$ τότε τα σύνολα $U = \prod_{L \neq L_0} G(L/K) \times \{\sigma'\}$ σχηματίζουν μία υποβάση ανοιχτών συνόλων του γινομένου $\prod_L Gal(L/K)$. Αν σ είναι μία αντίστροφη εικόνα του σ' τότε $h^{-1}(U) = \sigma Gal(N/L_0)$ δηλαδή η h είναι συνεχής και επιπλέον $h(\sigma G(N/L_0)) = h(G) \cap U$, οπότε η $h : G \longrightarrow h(G)$ είναι ανοιχτή συνεπώς ένας τοπολογικός ομομορφισμός. Συνεπώς αρκεί να δείξουμε ότι το $h(G)$ είναι κλειστό του συμπαγούς χώρου $\prod_L Gal(L/K)$. Γιά αυτό θεωρούμε γιά κάθε ζευγάρι $L' \supseteq L$ πεπερασμένων επεκτάσεων Galois το σύνολο:

$$M_{L'/L} = \{\prod_{\tilde{L}} \sigma_{\tilde{L}} \in \prod_{\tilde{L}} Gal(\tilde{L}/K) / \sigma_{L'/L} = \sigma_{\bar{L}}\}$$

Είναι προφανές ότι $h(G) = \cap_{L' \supset L} M_{L'/L}$ οπότε αρκεί να δείξουμε την κλειστότητα του $M_{L'/L}$. Ομως αν $G(L/K) = \{\sigma_1, ..., \sigma_n\}$ και είναι $S_i \subset Gal(L'/K)$ το σύνολο των επεκτάσεων των σ_i στο L' τότε έχουμε

$$M_{L'/L} = \bigcup_{i=1}^{n} (\prod_{\tilde{L} \neq L, L'} Gal(\tilde{L}/K) \times S_i \times \sigma_i),$$

οπότε $M_{L'/L}$ είναι πράγμαιι κλειστό.

Το θεμελιώδες θεώρημα της θεωρίας Galois παίρνει στην περίπτωση των απείρων επεκτάσεων την παρακάτω μορφή:

Θεώρημα 5.3 *Εστω N/K μιά πεπερασμένη η άπειρη επέκταση του Galois. Τότε η αντιστοιχία*

$$L \longmapsto Gal(N/L)$$

είναι ένα προς ένα μεταξύ των υποεπεκτάσεων L/K του N/K και των κλειστών υποομάδων του $Gal(N/K)$. Οι ανοιχτές υποομάδες αντιστοιχούν στις πεπερασμένες υποεπεκτάσεις του N/K.

Απόδειξη: Κάθε ανοιχτή υποομάδα της $Gal(N/K)$ είναι επίσης κλειστή, αφού είναι το συμπλήρωμα των ανοιχτών πλευρικών υποομάδων της. Αν L/K είναι μιά πεπερασμένη υποεπέκταση, τότε η $Gal(N/L)$ είναι ανοιχτή, αφού κάθε $\sigma \in Gal(N/K)$ έχει την ανοιχτή περιοχή $\sigma Gal(N/\bar{L}) \subset Gal(N/L)$ όπου $\bar{L}/K$ είναι η κλειστή θήκη της L/K.

Αν L/K μία υποεπέκταση τότε $Gal(N/L) = \bigcup_i Gal(N/L_i)$ όπου L_i/K διατρέχει τις πεπερασμένες υποεπεκτάσεις του L/K συνεπώς η $Gal(N/L)$ είναι κλειστή.

Η αντιστοιχία $L \longrightarrow Gal(N/L)$ είναι ένα προς ένα αφού L είναι το σταθερό σώμα της $Gal(N/L)$. Γιά το επί έχουμε να δείξουμε ότι γιά τυχαία κλειστή υποομάδα H του $Gal(N/K)$ τότε $H = G(N/L)$ όπου L είναι το σταθερό σώμα του H.

Η κατεύθυνση $H \subseteq Gal(N/L)$ είναι τετριμμένη. Εστω αντιστρόφως $\sigma \in Gal(N/L)$. Αν L'/L είναι πεπερασμένη υποεπέκταση του N/L τότε είναι $\sigma Gal(N/L'$ θεμελιώδης ανοιχτή περιοχή του σ στο $Gal(N/L)$. Η απεικόνιση $H \longrightarrow Gal(L'/L)$ είναι επι αφού η εικόνα $\bar{H}$ έχει σταθερό σώμα το L και ισούται με την $Gal(L'/L)$ από την θεωρία Galois πεπερασμένων επεκτάσεων. Μπορούμε να διαλέξουμε $\tau \in H$ με $\tau|_L = \sigma|_L$, και $\tau \in H \cap \sigma Gal(N/L')$ αυτό δείχνει ότι το σ ανήκει στην κλειστότητα της H στην $Gal(N/L)$ δηλαδή στην ίδια την H, οπότε H $= Gal(N/L)$.

Αν η H είναι ανοιχτή υποομάδα της $Gal(N/K)$ τότε είναι και κλειστή και συνεπώς της μορφής $H = Gal(N/L)$. Η $Gal(N/K)$ γράφεται ως ξένη ένωση των ανοιχτών πλευρικών υποομάδων του H. Αφού $Gal(N/K)$ είναι συμπαγής καλύπτεται από πεπερασμένες τέτοιες πλευρικές υποομάδες ,συνεπώς η $H = Gal(N/L)$ έχει πεπερασμένο δείκτη στην $Gal(N/K)$ δηλαδή L/K είναι πεπερασμένου βαθμού.

Θα προσπαθήσουμε στα επόμενα,να ορίσουμε υποομάδες αδρανείας,διακλάδωσης και ανάλυσης της ομάδας Galois σε άπειρες επεκτάσεις του Galois.

Εστω L/K τυχαία επέκταση Galois ,με ομάδα Galois $G = Gal(L/K)$. Αν v είναι μια (αρχιμηδεια ή όχι) εκτίμηση του K και w είναι μια επέκταση της εκτίμησης στο σώμα L, τότε η $w \circ \sigma$ είναι επίσης μία εκτίμηση της v, δηλαδή η ομάδα G δρα πάνω στο σύνολο $w|v$ των επεκτάσεων της εκτίμησης v. Ισχύει η παρακάτω:

Πρόταση 5.4 *Η ομάδα G δρα μεταβατικά στο σύνολο των επεκτάσεων $w|v$.*

Απόδειξη: Εστω w, w' δυό επεκτάσεις της v στο L. Αν η επέκταση είναι πεπερασμένη τότε από την θεωρία πεπερασμένων επεκτάσεων αυτό που θέλουμε ισχύει [Av1]. Στην περίπτωση που η επέκταση είναι άπειρη θεώρουμε όλες τις πεπερασμένες Galois υποεπεκτάσεις M/K και ορίζουμε τα σύνολα:

$$X_M := \{\sigma \in G : w \circ \sigma|_M = w'|_M\}.$$

Τα X_M είναι μη κενά και κλειστά, αφού γιά $\sigma \in G \backslash X_M$ ολόκληρη η ανοιχτή περιοχή $\sigma Gal(L/M)$ βρίσκεται στο συμπλήρωμα του X_M. Εχουμε ότι $\bigcup X_M \neq \emptyset$ γιατί αλλιώς λόγω συμπάγειας θα είχα κενή τομή σε πεπερασμένο σύνολο πεπερασμένων επεκτάσεων, άτοπο.

Ορισμός 5.5 *Ορίζουμε σαν ομάδα αναλύσεως της επέκτασης w της εκτίμησης v στο L ως*

$$G_w = G_w(L/K) = \{\sigma \in Gal(L/K) : w \circ \sigma = w\}.$$

Αν v είναι μία μη αρχιμήδεια εκτίμηση τότε η ομάδα αναλύσεως έχει την κανονική υποομάδα

$$G_w \supseteq I_w,$$

η οποία ορίζεται ως ακολούθως:

Ορισμός 5.6 *Ορίζουμε σαν ομάδα αδρανείας της $w|v$, την υποομάδα της G_w:*

$$I_w = I_w(L/K) := \{\sigma \in G_w : \sigma x \equiv x mod B \forall \ x \in \mathcal{O}\}.$$

όπου με $\mathcal{O}$ συμβολίζουμε τον δακτύλιο εκτίμησης της w και με B το μέγιστο ιδεώδες του.

Οι υποομάδες G_w, I_w, R_w της G είναι κανονικές κλειστές υποομάδες ως προς την τοπολογία του Krull. Ας δούμε για παράδειγμα γιατί αυτό ισχύει στην περίπτωση της ομάδας αναλύσεως. Εστω $\sigma \in G = Gal(L/K)$ ένα στοιχείο το οποίο να ανήκει στην κλειστότητα της G_w. Αυτό σημαίνει ότι σε κάθε περιοχή $\sigma Gal(L/M)$ υπάρχει στοιχείο σ_M της G_w, όπου M διατρέχει όλες της πεπερασμένες ενδιάμεσες της L/K. Αφού $\sigma_M \in \sigma Gal(L/M)$ έχουμε ότι $\sigma_M|_M = \sigma|_M$ και αφου $w \circ \sigma_M = w$ έχουμε ότι $w \circ \sigma|_M = w \circ \sigma_M|_M = w|M$. Ομως η L είναι η ένωση όλων των M, συνεπώς $w \circ \sigma = w$ οπότε $\sigma \in G_w$ και η υποομάδα G_w είναι κλειστή. Με όμοιο τρόπο μπορούμε ότι η ομάδα αδρανείας είναι κλειστή. Συνεπώς σύμφωνα με το θεώρημα του Krull, μπορούμε να αντιστοιχίσουμε σε αυτές επεκτάσεις του Galois, τα σώματα ανάλυσης και αδρανείας. Σε πρώτα ιδεώδη P του δακτυλίου ακεραίων του K αντιστοιχίζουμε όπως είναι γνωστό μη-αρχιμήδειες εκτιμήσεις.

Βιβλιογραφία

[Ah] Ahlfors L. V., Complex Analysis. Mc Graw-Hill, New York 1979

[Av1] Αντωνιάδη Γιάννη Α., Αλγεβρική Θεωρία των Αριθμών Ι,Σημειώσεις, Ηράκλειο 1988

[Av2] Αντωνιάδη Γιάννη Α., Αλγεβρική Θεωρία των Αριθμών ΙΙ, Σημειώσεις, Ηράκλειο 1992

[Av3] Αντωνιάδη Γιάννη Α., Θεωρία Παραστάσεων Πεπερασμένων Ομάδων, Σημειώσεις, Ηράκλειο 1992

[Av4] Αντωνιάδη Γιάννη Α., Ελλειπτικές Καμπύλες, Σημειώσεις, Ηράκλειο 1985

[Ap] Apostol Tom, Modular Functions and Dirichlet Series in Number Theory. GTM 41 Springer Verlag, New York 1976

[A-M] Atiyah M.F. - Macdonald I.G., Introduction to Commutative Algebra, Addison-Wesley California 1969

[Ca] do Carmo M.P., Riemannian Geometry, Birkhäuser, Boston 1992

[Cas] Cassels J.W.S., Lectures on Elliptic Curves. LMS 24 Cambridge University Press, Cambridge 1991

[Fr] Frey Gerhard, Links between Elliptic Curves and certain Diophantine equations, Annales Universitatis Saraviensis 1 (1986), 1-40

[Fo] Forster O., Riemannshe Flächen, Springer-Verlag (Heidelberger Taschenbücher), Berlin 1977

[Ha] Hartshorne R., Algebraic Geometry, Springer-Verlag, New York 1977.

[Hi] Hirsch Morris W, Differential Topology. GTM 33 Springer Verlag, New York 1976

[Hu] Husemöller Dale, Elliptic Curves. GTM 111 Springer-Verlag, New York 1987

[I-R] Ireland K. - Rosen M., A Classical Introduction to Modern Number Theory. GTM 84 Springer-Verlag, New York 1990

[Kn] Knapp Anthony W, Elliptic Curves. Mathematical Notes Princeton University Press, Princeton 1992

[Ko] Koblitz Neal, Introduction to Elliptic Curves and Modular Forms, GTM 97 Springer-Verlag, New York 1984

[Lg] Langlands R.P., L-functions and Automorphic Representations, Proc. of I.C.M., Helsinki 1978, 165-175

[Ma] Massey William S., A Basic Course in Algebraic Topology.

[Maz1] Mazur B., Modular Curves and the Eisenstein Ideal. IHES publ.math. 47 (1977), 33-186

[Maz2] Mazur B., Rational Isogenies of prime degree. Invent. math. 44 (1978), 129-162

[Ri] Ribet K.A,On modular representations of $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$ arising from modular forms, Invent. math. 100 (1990), 431-476

[Se] Serre, J.-P.,Sur les represéntasions modulaires de degré 2 de $Gal(\bar{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. 54 (1987), 179-230

[Sh] Shimura Goro, Introduction to the Arithmetic Theory of Automorphic functions, Princeton University Press, Princeton 1971

[Si] Silverman J.H., The Arithmetic of Elliptic Curves, GTM 106, Springer-Verlag, New York 1986

[Ta] Tate J., Algorithm for determining the type of a singular fiber in an elliptic pencil. Modular Functions of One Variable IV, Lecture Notes in Math. 476, Springer-Verlag, 1975, 33-52.

[Za] Zagier Don, Modular points, modular curves, modular surfaces and modular forms. LNM 1111 Arbeitstagung Bonn σελ. 225-248