Δημητρης Χατζακος

Modular forms και Ελλειπτικες καμπυλες

Μεταπτυχιακη Εργασια

Πανεπιστήμιο Αθηνών, Τμήμα Μαθηματικών

Αθήνα 3 Σεπτεμβρίου 2012

Εισηγητης: Αριστείδης Κοντογεώργης

Επιτροπη

Αντώνης Μελάς

Γιάννης Εμμανουήλ

Περιεχόμενα

1 Στοιχεία Αλγεβρικής Γεωμετρίας 1

1.1 Varieties 1
1.2 Καμπύλες 5
1.3 Divisors και Διαφορικά 8
1.4 Το Θεώρημα Riemann-Roch και το Θεώρημα του Hurwitz 11

2 Ελλειπτικές Καμπύλες 15

2.1 Μορφές Weierstrass 16
2.2 Η ομάδα $E(K)$ 22
2.3 Singular Κυβικές Καμπύλες 25
2.4 Ύπαρξη μορφής Weierstrass 27
2.5 Ισογενείς Ελλειπτικές Καμπύλες 30
2.6 Σημεία στρέψης: Το πρότυπο του Tate και η αντιστοιχία του Weil 36
2.7 Ο δακτύλιος των ενδομορφισμών και η ομάδα των αυτομορφισμών . 41
2.8 Καλή και κακή αναγωγή ελλειπτικών καμπυλών 42
2.9 Η Ομάδα $E(\mathbb{F}_q)$ 49
2.10 Οι Ομάδες $E(\mathbb{C})$ και $E(\mathbb{R})$ 55
2.11 Μιγαδικός Πολλαπλασιασμός 66
2.12 Οι ομάδες $E(\mathbb{Q})$ και $E(K)$: Το Θεώρημα Mordell-Weil 70
2.13 Περαιτέρω θέματα αριθμητικής των ελλειπτικών καμπυλών 93
2.13α΄ Η δομή της torsion υποομάδας 93
2.13β΄ Η rank μιας ελλειπτικής καμπύλης 95
2.13γ΄ Ακέραια σημεία 95
2.13δ΄ Γενικεύσεις 96

3 Ομάδες Fuchs και Επιφάνειες Riemann 97

3.1 Τοπολογικές ομάδες 97
3.2 Επιφάνειες Riemann 100
3.3 Το άνω μιγαδικό επίπεδο $\mathbb{H}$ 104
3.4 Ομάδες Fuchsian και η δράση τους στο $\mathbb{H}$ 106
3.5 Modular Καμπύλες 110
3.5α΄ Η μιγαδική δομή στον $\Gamma(1)\backslash\mathbb{H}$ 111
3.5β΄ Η μιγαδική δομή στον $\Gamma(1)\backslash\mathbb{H}^*$ 111
3.5γ΄ Η μιγαδική δομή στον $\Gamma\backslash\mathbb{H}^*$ 112

4 Modular Forms 115
4.1 Βασικές έννοιες . . . 115
4.2 Οι χώροι $M_k(\Gamma)$ και $S_k(\Gamma)$ . . . 119
4.3 Παραδείγματα modular μορφών και αναπτύγματα Fourier . . . 122
4.3α′ Σειρες Eisenstein . . . 122
4.3β′ Η συνάρτηση $\Delta(z)$ . . . 126
4.3γ′ Η j-συνάρτηση $j(z)$ . . . 130
4.3δ′ Η συνάρτηση $\eta(z)$ . . . 132
4.4 Σειρές Poincare και το εσωτερικό γινόμενο του Petersson . . . 134
4.5 Τελεστές Hecke . . . 142
4.6 Η θεωρία Atkin-Lehner . . . 155
4.7 Εφαρμογές των modular μορφών . . . 162
4.7α′ Το πρόβλημα των τεσσάρων τετραγώνων . . . 162
4.7β′ Το πρόβλημα των διαμερίσεων . . . 164
4.8 Γενικεύσεις . . . 165
4.8α′ Siegel modular forms . . . 165
4.8β′ Hilbert modular forms . . . 166
4.8γ′ Θήτα συναρτήσεις . . . 166
4.8δ′ Automorphic forms . . . 166
4.9 Η modular καμπύλη $X_0(N)$ . . . 168
4.9α′ Άλλες modular καμπύλες . . . 170
4.10 Moduli interpretation . . . 170
4.10α′ Απόδειξη θεωρήματος 4.9.1 . . . 172
4.11 Modular καμπύλες ως πηλίκα του υπερβολικού χώρου . . . 176
4.12 Hecke Correspondences . . . 177
4.12α′ Οι Hecke correspondence στην $X_0(N)$ . . . 177
4.12β′ Moduli interpretation των Hecke correspondences . . . 178
4.12γ′ Οι Hecke correspondences στο υπερβολικό επίπεδο . . . 181
4.13 Hecke correspondences και ο αυτομορφισμός του Frobenious . . . 181

5 L-συναρτήσεις και modularity 187
5.1 L-συναρτήσεις . . . 187
5.2 L-σειρές ελλειπτικών καμπυλών . . . 192
5.3 L-σειρές modular μορφών . . . 195
5.4 Το Modularity Θεώρημα . . . 206

Βιβλιογραφία 211

Εισαγωγή

"There are five elementary operations
in mathematics: addition, subtraction,
multiplication, division and modular forms."

Martin Eichler

Σκοπός της μεταπτυχιακής αυτής εργασίας είναι η μελέτη των Modular forms και των Ελλειπτικών καμπυλών. Τόσο οι modular forms όσο και οι Ελλειπτικές καμπύλες αποτελούν κεντρικούς τομείς της μοντέρνας θεωρίας αριθμών. Για πολύ καιρό μελετόντουσαν σχετικά ανεξάρτητα, προτού, πριν από 60 περίπου χρόνια, διατυπωθεί η εικασία Taniyama-Shimura-Weil (ή εικασία Taniyama-Shimura). Η ενοποιητική αυτή αρχή αποτέλεσε από τότε κεντρικό πρόβλημα της θεωρίας αριθμών μέχρι την πλήρη απόδειξη της το 2001. Η εργασία αυτή ξεκινάει με την μελετη των modular forms και των Ελλειπτικών καμπυλών ως ξεχωριστά μαθηματικά αντικείμενα, και τελειώνει με την περιγραφή του modularity θεωρήματος (εικασία Taniyama-Shimura-Weil). Η δομή της εργασίας είναι η εξής: στα 4 πρώτα κεφάλαια αναπτύσσεται κάπως ξεχώριστα η θεωρία των επιμέρους θεμάτων, ενώ στο τελευταίο κεφάλαιο μελετάται η συνάφεια των δύο αντικειμένων.

Πιο συγκεκριμμένα, στο πρώτο κεφάλαιο γίνεται μια εισαγωγή στο κομμάτι της αλγεβρικής γεωμετρίας που θα μας χρειαστεί για την μελέτη των ελλειπτικών καμπυλών. Αναλυτικότερα, μελετάμε τα βασικά στοιχεία της θεωρίας των προβολικών και affine varieties, των αλγεβρικών καμπύλων και των μορφισμών. Επίσης, διατυπώνονται το θεώρημα Riemann-Roch και ο τύπος του Hurwitz για καμπύλες.

Στο δεύτερο κεφάλαιο μελετάται η αριθμητική και η γεωμετρία των ελλειπτικών καμπυλών. Κύριος σκοπός μας σε αυτό το κεφάλαιο είναι η μελέτη και περιγραφή της ομάδας $E(K)$, οπου $K = \mathbb{F}_q, \mathbb{C}, \mathbb{R}, \mathbb{Q}$ ή ένα τυχαίο σώμα αριθμών (σε όλη την εργασία, με τον όρο «σώμα αριθμών» θα εννοούμε πάντα μια πεπερασμένη επέκταση του $\mathbb{Q}$, ή αλλιώς, αυτό που συχνά στην βιβλιογραφία καλείται αλγεβρικό σώμα αριθμών). Τα πρώτα σημαντικά αποτελέσματα αφορούν την δομή της $E(\mathbb{F}_q)$, και είναι η Αρχή του Hasse και η γενίκευση της από τον Weil (εικασίες του Weil για ελλειπτικές καμπύλες). Όσον αφορά το $\mathbb{C}$, η μελέτη μας είναι κλασσική, και δόθηκε από τον Weierstrass τον 19ο αιώνα. Στο $\mathbb{R}$, η περιγραφή που δίνουμε είναι σύντομη, γεωμετρική και όχι αυστηρή. Για K ένα σώμα αριθμών, το κύριο αποτέλεσμα είναι το θεώρημα Mordell-Weil. Βέβαια, προτού μπορέσουμε να αποδείξουμε τα αποτελέσματα αυτά, θα χρειαστεί να αναπτύξουμε σε κάποιον βαθμό τα εργαλεία της μελέτης των ελλειπτικών καμπυλών: μορφισμούς και ισογένειες, το πρότυπο

του Tate, την αντιστοιχία του Weil και την αναγωγή των ελλειπτικών καμπυλών. Δίνουμε επίσης μια σύντομη περιγραφή της σύνδεσης της θεωρίας των ελλειπτικών καμπυλών με την θεωρία κλάσεως σωμάτων.

Στο τρίτο κεφάλαιο, εισερχόμαστε στο «αναλυτικό» κομμάτι της θεωρίας. Περιγράφουμε συνοπτικά την θεωρία των τοπολογικών ομάδων, των επιφανειών Riemann (μεταξύ των οποίων το θεώρημα Riemann-Roch και ο τύπος του Hurwitz για επιφάνειες Riemann), των ομάδων Fuchsian και των modular καμπυλών (ελλειπτικοί, παραβολικοί και υπερβολικοί μετασχηματισμοί, ελλειπτικά σημεία και cusps).

Στο τέταρτο κεφάλαιο, μελετάμε τις συναρτήσεις και τα διαφορικά που ορίζονται σε μια modular καμπύλη. Αυτές είναι οι modular συναρτήσεις και οι modular forms (μορφές). Οι modular forms, στων οποίων την μελέτη κατά βάση εμβαθύνουμε, έχουν παίξει ήδη από τον δέκατο ένατο αιώνα σημαντικό ρόλο στην ανάπτυξη της θεωρίας αριθμών. Εισήχθησαν πρώτη φορά από τον Gauss, και μελετήθηκαν εκτενώς από τους Gauss, Abel, Jacobi, Eisenstein, Weierstrass, Kronecker και Poincare.Η θεωρία των modular forms άλλαξε σημαντικά στις αρχές του εικοστού αιώνα, ύστερα από την δουλειά των Ramanujan, Hardy, Mordell, Hecke και Petersson, για να αναφέρουμε μόνο κάποιους από τους σημαντικότερους. Αρχικά, μελετάμε την κλασσική θεωρία των modular συναρτήσεων και των modular μορφών, που σε πρώτο επίπεδο αποτελείται κυρίως από την μελέτη των χώρων $M_k(\Gamma)$ και $S_k(\Gamma)$ και τους τελεστές Hecke, οι οποίοι αποτελούν οικογένεια τελεστών που ορίζονται από έναν χώρο μορφών στον εαυτό του και μας δίνουν πληροφορίες για την μορφή των στοιχείων του χώρου. Δύο βασικά προβλήματα υπάρχουν σε αυτό το σημείο: το πρόβλημα της εύρεσης μιας βάσης για έναν δοσμένο συγκεκριμμένο χώρο μορφών, καθώς και το πρόβλημα της εύρεσης ιδιοτιμών και ιδιοσυναρτήσεων για τους τελεστές Hecke. Οι απαντήσεις σε αυτά τα δύο προβλήματα συνδέονται, και οδηγούν ταυτόχρονα στην απόδειξη κάποιων αριθμοθεωρητικών εικασιών του Ramanujan. Επίσης, περιγράφουμε εν συντομία βασικά στοιχεία της θεωρίας Atkin-Lehner (oldforms, newforms και το Κύριο Λήμμα της θεωρίας Atkin-Lehner). Στην συνέχεια, σκιαγραφούμε σε αδρές γραμμές κάποιες εφαρμογές και κάποιες γενικεύσεις των modular μορφών. Το επόμενο βήμα είναι είναι η μελέτη της moduli interpretation των modular καμπυλών, όπου συμπεραίνουμε πως αυτές αποτελούν με φυσιολογικό τρόπο moduli spaces για κατάλληλες κλάσεις ισοδυναμίας μεταξύ ελλειπτικών καμπυλών. Μελετάμε την moduli interpretation των Hecke correspondences, και την σχέση τους με τον αυτομορφισμό του Frobenius (σχέσεις Eichler-Shimura), καθώς επίσης και το θεώρημα του Igusa.

Τέλος, στο πέμπτο κεφάλαιο γίνεται μια σύντομη επεξήγηση του Modularity Θεωρήματος, μέσω διάφορων μορφών του. Γνωστό ως εικασία Taniyama-Shimura-Weil, αποτέλεσε ανοικτό πρόβλημα κεντρικής σημασίας για την θεωρία αριθμών για πολλά χρόνια. Για να το εξηγήσουμε, εισαγάγουμε αρχικά την έννοια της L-σειράς μιας ελλειπτικής καμπύλης και μιας modular μορφής, αποδεικνύουμε κάποια βασικά αποτελέσματα για αυτές (αναλυτικές επεκτάσεις, γινόμενα Euler, συναρτησιακές εξισώσεις, αντίστροφα θεωρήματα) και στην τελευταία παράγραφο δίνουμε μερικές ισοδύναμες διατυπώσεις του.

Θα ήθελα να ευχαριστήσω βαθύτατα τον καθηγητή μου Αριστείδη Κοντογεώργη για την βοήθεια του στην διεκπόνηση της εργασίας αυτής, για την βοήθεια του κατά τα τελευταία δύο χρόνια καθώς και για τα πολύ όμορφα μαθήματικά που με βοήθησε να γνωρίσω και να μάθω. Θα ήθελα επίσης να ευχαριστήσω τα άλλα δύο

μέλη της επιτροπής, τον κ.Εμμανουήλ και τον κ.Μελά, για την συμμετοχή τους σε αυτήν, όπως επίσης και κάθε άλλον δάσκαλο ή καθηγητή μου που με δίδαξε κάτι χρήσιμο ή, ακόμα σπουδαιότερο, κάτι όμορφο. Ιδιαιτέρως, θα ήθελα να ευχαριστήσω τον καθηγητή μου κ.Γιαννόπουλο, που κατά τα χρόνια των σπουδών μου η βοήθεια που μου προσέφερε ήταν μεγάλη.

Ευχαριστώ τους φίλους και συμφοιτητές μου, που κατά τα τελευταία έξι χρόνια μοιραζόμαστε κάθε μέρα μαζί, τόσο στην σχολή όσο και εκτός αυτής, την τόσο συναρπαστική «μαθηματική εμπειρία».

Τέλος, θα ήθελα να ευχαριστήσω την οικογένεια μου, που τόσα χρόνια στηρίζει το όνειρο μου να ασχολούμαι με κάτι που της είναι ανοίκειο και που πάντα με βοηθά να εκπληρώνω τους στόχους μου. Σε αυτήν, και ιδιαιτέρως στους αγαπημένους μου γονείς, αφιερώνω αυτήν την εργασία.

Κεφάλαιο 1

Στοιχεία Αλγεβρικής Γεωμετρίας

Αρχικά, δίνουμε κάποια εισαγωγικά στοιχεία από την αλγεβρική γεωμετρία που θα χρειαστούν για την μελέτη μας πάνω στις ελλειπτικές καμπύλες. Ακολουθούμε κυρίως την παρουσίαση στον [Silverman, [30], κεφ.1,2]. Η παρουσίαση μας είναι σύντομη, και, με λίγες εξαιρέσεις, χωρίς αποδείξεις. Για τις αποδείξεις που λείπουν παραπέμπουμε στους [Silverman, [30], κεφ.1,2], [Hartshorne, [10], κεφ.1,2] και [Ueno, [34], κεφ.1].

1.1 Varieties

Έστω K ένα τέλειο σώμα, δηλαδή ένα σώμα που κάθε αλγεβρική επέκταση του είναι διαχωρίσιμη. Γενικά, οι περισσότερες από τις έννοιες που θα αναπτύξουμε δουλεύουν ικανοποιητικά μόνο για τέλεια σώματα. Ειδικότερα, τα σώματα χαρακτηριστικής 0 και τα πεπερασμένα σώματα είναι τέλεια, και είναι αυτές οι περιπτώσεις που θα μας απασχολήσουν περισσότερο και στην μελέτη των ελλειπτικών καμπυλών.

Ορισμός 1.1.1. *Ο n-διάστατος αφφινικός χώρος υπεράνω του K είναι ο χώρος*

$$\mathbb{A}^n(\bar{K}) = \{P = (x_1, x_2, ..., x_n), x_i \in \bar{K}\}.$$

Αν όλα τα $x_i \in K$, το P λέγεται K-ρητό σημείο.

Πιο πολύ μας ενδιαφέρουν συγκεκριμμένα υποσύνολα του αφφινικού χώρου:

Ορισμός 1.1.2. *Αν I είναι ένα ιδεώδες του $\bar{K}[x_1, ..., x_n]$, ορίζουμε το $V(I) = \{P : f(P) = 0 \ \forall \ f \in I\}$. Ένα σύνολο της μορφής $V(I)$ λέγεται αλγεβρικό.*

Ορισμός 1.1.3. *Έστω V ένα αλγεβρικό σύνολο. Το ιδεώδες του $\bar{K}[x_1, ..., x_n]$ που αντιστοιχεί στο V είναι το $I(V) = \{f \in \bar{K}[x_1, x_2, ..., x_n] : f(P) = 0 \ \forall \ P \in V\}$.*

Αν το $I(V)$ παράγεται από πολυώνυμα στο $K[x_1, x_2, ..., x_n]$, τότε λέμε ότι το V ορίζεται υπεράνω του (ή πάνω από το) K, και γράφουμε V/K. Σ' αυτήν την περίπτωση, το σύνολο των K-ρητών σημείων του V είναι το:

$$V(K) = V \cap \mathbb{A}^n(K).$$

Το επόμενο θεώρημα, που είναι ένα από τα πιο θεμελιώδη της αλγεβρικής γεωμετρίας, μας εγγυάται πως τα ιδεώδη που μόλις ορίσαμε στα $K[x_1, x_2, ..., x_n]$ και $\bar{K}[x_1, x_2, ..., x_n]$ είναι πεπερασμένα παραγόμενα.

Θεώρημα 1.1.4 (Βάσης του Hilbert)**.** *Έστω K ένα σώμα. Τότε, κάθε ιδεώδες του $K[x_1, x_2, ..., x_n]$ είναι πεπερασμένα παραγόμενο.*

Αν σκεφτούμε ότι πολλές φορές οι συναρτήσεις που μελετάμε ορίζονται με συντελεστές από το αρχικό σώμα K, ο παρακάτω ορισμός θα μας είναι συχνά χρήσιμος:

Ορισμός 1.1.5. *Αν V είναι ένα αλγεβρικό σύνολο, ορίζουμε το*

$$I(V/K) = \{f \in K[x_1, x_2, ..., x_n] : f(P) = 0 \; \forall P \in V\}$$

Παρατηρήσεις:

(i) Αν το V/K, τότε $I(V) = I(V/K)\bar{K}[x_1, x_2, ..., x_n]$

(ii) Έστω V/K, και έστω ότι $I(V/K) = \langle f_1, f_2, ..., f_m\rangle$. Τότε το $V(K)$ αποτελείται ακριβώς από τις κοινές ρίζες των $f_i, i = 1, 2, ..., m$.

Ορισμός 1.1.6. *Αν το $I(V)$ είναι πρώτο ιδεώδες του $\bar{K}[x_1, x_2, ..., x_n]$, το V λέγεται αφφινική variety. Ακόμα, αν η V είναι μια variety που ορίζεται υπεράνω του K, ορίζουμε τον δακτύλιο συντεταγμένων της V/K ως εξής:*

$$K[V] = K[X]/I(V/K)$$

Αφού το $I(V/K)$ είναι πρώτο, ο $K[V]$ είναι ακέραια περιοχή. Το σώμα πηλίκο του $K[V]$ συμβολίζεται με $K(V)$ και καλείται σώμα συναρτήσεων της V/K.

Όμοια ορίζονται τα ανωτέρω και για το σώμα $\bar{K}$.

Το ανάλογο της διαίσθησης που έχουμε για την έννοια της διάστασης σε έναν διανυσματικό χώρο είναι λογικό να υπάρχει και εδώ. Ο επόμενος ορισμός από την θεωρία σωμάτων θα μας βοηθήσει να ορίσουμε ακριβώς μια έννοια διάστασης.

Ορισμός 1.1.7. *Έστω F/K μια επέκταση σωμάτων. Βαθμός υπερβατικότητας της επέκτασης ονομάζεται το μέγιστο πλήθος αλγεβρικά ανεξάρτητων στοιχείων του F πάνω από το K. Ισοδύναμα, μπορεί να δείξει κανείς ότι ο βαθμός της επέκτασης F/K είναι r αν και μόνο αν υπάρχουν $a_1, a_2, ..., a_r$ στοιχεία στο F υπερβατικά υπεράνω του K ώστε η επέκταση $F/K(a_1, a_2, ..., a_r)$ να είναι πεπερασμένη.*

Ορισμός 1.1.8. *Έστω V μια variety. Διάσταση της V ονομάζεται ο βαθμός υπερβατικότητας του $\bar{K}(V)$ υπεράνω του $\bar{K}$. Η διάσταση της V συμβολίζεται με* $\dim V$.

Για παράδειγμα, έχουμε $\dim \mathbb{A}^n = n$. Επίσης, $\dim V = n - 1$ αν και μόνο εάν $V = \langle f\rangle$ με $f(x_1, x_2, ..., x_n)$ μη σταθερό πολυώνυμο.

Θέλουμε τώρα να ορίσουμε μια έννοια «ομαλότητας» της καμπύλης. Η έννοια αυτή παίζει πολύ σημαντικό ρόλο στην μελέτη των ελλειπτικών καμπυλών.

Ορισμός 1.1.9. *Έστω V μια variety. Έστω P ένα σημείο της V και $f_1, f_2, \ldots, f_m \in \bar{K}[x_1, x_2, ..., x_n]$ με $I(V) = \langle f_1, f_2, ..., f_m\rangle$. Η V λέγεται nonsingular στο P αν και μόνο αν ο πίνακας*

$$\left(\frac{\partial f_i}{\partial x_j}(P)\right)_{i=1,...,m, j=1,...,n}$$

έχει τάξη $n - \dim V$. Αν η V είναι nonsingular παντού, τότε λέγεται nonsingular ή λεία.

Εστω $M_P = \{f \in \bar{K}[V] : f(P) = 0\}$. Η απεικόνιση

$$\phi : \bar{K}[V]/M_P \to \bar{K} : f \to f(P)$$

είναι ισομορφισμός. Το πηλίκο M_P/M_P^2 είναι διανυσματικός χώρος υπεράνω του $\bar{K}$ πεπερασμένης διάστασης. Η παρακάτω πρόταση δίνει έναν χρήσιμο γεωμετρικό χαρακτηρισμό των nonsingular σημείων.

Πρόταση 1.1.10. *Ένα σημείο P μιας variety V είναι nonsingular αν και μόνο αν*

$$\dim_{\bar{K}} M_P/M_P^2 = \dim V$$

Ορισμός 1.1.11. *Ο τοπικός δακτύλιος της V στο P είναι ο*

$$\bar{K}[V]_P = \{F \in \bar{K}(V) : F = f/g : f, g \in \bar{K}[V], g(P) \neq 0\}$$

και τα στοιχεία του ονομάζονται regular συναρτήσεις στο P.

Ορίζουμε τώρα αντιστοίχως τις παραπάνω έννοιες και για την προβολική περίπτωση.

Ορισμός 1.1.12. *Ο n-διάστατος προβολικός χώρος υπεράνω του K είναι ο χώρος*

$$\mathbb{P}^n(\bar{K}) = \{(x_0, x_1, ..., x_n),\ x_i \in K\},$$

με τουλάχιστον ένα x_i μη μηδενικό, modulo την ισοδυναμία

$$(x_0, x_1, ..., x_n) \sim (y_0, y_1, ..., y_n) \Longleftrightarrow (x_0, x_1, ..., x_n) = \lambda(y_0, y_1, ..., y_n)$$

για κάποιο $\lambda \in K^*$.

Η κλάση ισοδυναμίας του $(x_0, x_1, ..., x_n)$ είναι το σημείο $P = [x_0, x_1, ..., x_n]$. Αν $x_i \in K$, το P λέγεται K-ρητό σημείο. Το σύνολο των K-ρητών σημείων στον $\mathbb{P}^n(\bar{K})$ συμβολίζεται με $\mathbb{P}^n(K)$.

Παρατηρείστε ότι για $K = \mathbb{Q}$ το $P = (x_0, x_1) = (\sqrt{2}, 2\sqrt{2}) \in \mathbb{P}^1(\mathbb{Q})$ αν και $\sqrt{2} \notin \mathbb{Q}$. Η παρατήρηση αυτή οδηγεί φυσιολογικά στον εξής ορισμό.

Ορισμός 1.1.13. *Το ελάχιστο σώμα ορισμού του σημείου $P \in \mathbb{P}^n(\bar{K})$, όπου $P = [x_0, x_1, ...x_n]$, υπεράνω του K είναι το $K(P) = K(x_0/x_i, x_1/x_i, ..., x_n/x_i)$, για οποιοδήποτε i με $x_i \neq 0, i = 1, ..., n$.*

Για να έχει νόημα να ρωτήσει κανείς για τις ρίζες ενός πολυωνύμου f στον προβολικό n-διάστατο χώρο, θα πρέπει αν το f μηδενίζεται σε ένα σημείο $(x_0, x_1, ..., x_n)$, να μηδενίζεται και σε ολόκληρη την κλάση ισοδυναμίας του. Ο επόμενος ορισμός πρόκυπτει φυσιολογικά:

Ορισμός 1.1.14 (Ορισμός (Προβολικής Variety)**.** (i) *Ένα πολυώνυμο $f \in \bar{K}[x_0, x_2, ..., x_n]$ λέγεται ομογενές βαθμού d αν για κάθε $\lambda \in \bar{K}$ ισχύει $f(\lambda x_0, \lambda x_1, ..., \lambda x_n) = \lambda^d f(x_0, x_2, ..., x_n)$.*

(ii) *Ένα ιδεώδες I του $\bar{K}[x_0, x_2, ..., x_n]$ λέγεται ομογενές αν παράγεται από ομογενή πολυώνυμα.*

(iii) *Αν το I είναι ένα ομογενές ιδεώδες, ορίζουμε το προβολικό αλγεβρικό σύνολο του I να είναι το*

$$V(I) = \{P \in \mathbb{P}^n : f(P) = 0 \ \ \forall f \in I\}.$$

Ένα υποσύνολο του $\mathbb{P}^n(\bar{K})$ ονομάζεται προβολικό αλγεβρικό αν είναι της μορφής $V(I)$ για κάποιο ομογενές ιδεώδες I.

(iv) *Αν το V είναι προβολικό αλγεβρικό, το ομογενές ιδεώδες που αντιιστοιχεί στο V είναι το $I(V)$ που παράγεται από όλα τα ομογενή πολυώνυμα του $\bar{K}[x_0, x_2, ..., x_n]$ που μηδενίζονται σε κάθε σημείο του V.*

(v) *Αν τα ομογενή πολυώνυμα που παράγουν το ιδεώδες του V ανήκουν στο $K[x_0, x_2, ..., x_n]$, τότε, αντιστοίχως με πριν, λέμε ότι το V ορίζεται υπεράνω του K και γράφουμε V/K. Όμοια με προηγουμένως, ορίζουμε τα K-ρητά σημεία της V να είναι τα σημεία που ανήκουν στο $V(K) = V \cap \mathbb{P}^n(K)$*

(vi) *Αν το $I(V)$ είναι πρώτο ιδεώδες του $\bar{K}[x_0, x_1, ..., x_n]$, το V λέγεται προβολική variety.*

Έστω ένα ομογενές πολυώνυμο $f(x_0, x_1, ..., x_n)$. Υπάρχει $x_i \neq 0$. Μπορούμε να υποθέσουμε ότι $x_i = 1$. Η αντικατάσταση του $f(x_0, x_1, ..., 1, ..., x_n)$ με το $f(x_0, x_1, ..., x_{i-1}, x_{i+1}, ..., x_n) = f(y_1, y_2, ..., y_n)$ ονομάζεται απομογενοποίηση ως προς την μεταβλητή x_i. Η αντίθετη διαδικασία ονομάζεται ομογενοποίηση. Θα μελετήσουμε ελλειπτικές καμπύλες τόσο σε ομογενείς συντεταγμένες όσο και σε αφφινικές.

Αν $f \in K[x_1, ..., x_n]$, θεωρούμε τα πολυώνυμα f_i που είναι τα ομογενή πολυώνυμα στον n-διάστατο προβολικό χώρο με ομογενοποιήσεις το f. Τώρα, αν V είναι ένα αφφινικό αλγεβρικό σύνολο, ορίζουμε την προβολική θήκη του $\bar{V}$ του V να είναι το προβολικό αλγεβρικό σύνολο που το ιδεώδες του $I(\bar{V})$ παράγεται από τα $\{f_i : f \in I(V)\}$.

Πρόταση 1.1.15. *Αν η V είναι αφφινική variety, τότε η $\bar{V}$ είναι προβολική variety, και ισχύει $V = \bar{V} \cap \mathbb{A}^n(\bar{K})$. Αν V είναι μια προβολική variety, τότε το αφφινκό της ίχνος $V \cap \mathbb{A}^n(\bar{K})$ είναι αφφινική variety. Επίσης, αν το προβολικό ή το αφφινικό κομμάτι μιας variety ορίζεται πάνω από το K, το ίδιο συμβαίνει και με το άλλο κομμάτι. Τα σημεία της $\bar{V} - V$ ονομάζονται επ΄ άπειρον σημεία της variety.*

Η διάσταση μιας προβολικής variety ορίζεται να είναι η διάσταση ενός αφφινικού κομματιού της.

Ορισμός 1.1.16. *Έστω V μια προβολική variety, και $P \in V$. Διαλέγουμε ένα $\mathbb{A}^n$ με $P \in \mathbb{A}^n$. Η V είναι λεία στο P αν και μόνο αν η $V \cap A^n$ είναι λεία στο P. Ομοίως, ο τοπικός δακτύλιος $\bar{K}[V]_P$ της V στο P ορίζεται να είναι ο τοπικός δακτύλιος $K[V \cap \mathbb{A}^n]_P$ της $V \cap \mathbb{A}^n$ στο P.*

Ιδιαιτέρως χρήσιμες για την μελέτη μας θα αποδειχθούν οι απεικονίσεις από ελλειπτικές καμπύλες σε ελλειπτικές καμπύλες. Για αυτόν τον σκοπό, είναι αρχικά σημαντικό να μελετήσουμε απεικονίσεις από varieties σε varieties.

Ορισμός 1.1.17. *Έστω V_1, V_2 δύο προβολικές varieties του n-διάστατου προβολικού χώρου. Μια απεικόνιση:*

$$\phi : V_1 \to V_2$$

λέγεται ρήτη αν $\phi = [g_0, g_1, ..., g_n]$, *όπου κάθε* $g_i \in \bar{K}(V_1)$ *και για κάθε* P *που ορίζονται τα* g_i *ισχύει ότι* $\phi(P) = [g_0(P), g_1(P), ..., g_n(P)] \in V_2$.

Αν υπάρχει ένα $\lambda \in \bar{K}^*$ τέτοιο ώστε τα λf_i να ανήκουν στο $K(V_1)$, τότε η ϕ λέμε ότι ορίζεται πάνω από το K. Επίσης, γία μια ρητή συνάρτηση ϕ δεν είναι απαραίτητο να ορίζεται το $\phi(P)$ για κάθε σημείο P της V_1. Μπορούμε όμως να απαιτήσουμε κάτι ελαφρώς γενικότερο:

Ορισμός 1.1.18. *Έστω* $\phi = [g_0, g_1, ..., g_n] : V_1 \to V_2$ *μια ρητή συνάρτηση. Η* ϕ *είναι regular στο* $P \in V_1$ *αν υπάρχει συνάρτηση* f *στο* $\bar{K}(V_1)$ *ώστε η* fg_i *να είναι regular στο* P *για κάθε* $i = 0, 1, ..., n$, *και για κάποιο* i *να ισχύει* $fg_i(P) \neq 0$.

Στην περίπτωση που η ϕ είναι regular στο P, ορίζουμε

$$\phi(P) = [fg_0(P), fg_1(P), ..., fg_n(P)]$$

Αν μια ρητή συνάρτηση είναι παντού regular,τότε ονομάζεται μορφισμός. Οι μορφισμοί εδώ ονομάζονται έτσι επειδή είναι μορφισμοί με την έννοια της θεωρίας κατηγοριών:

Ορισμός 1.1.19. *Έστω* V_1, V_2 *δύο προβολικές varieties. Αν υπάρχουν μορφισμοί* $\phi_1 : V_1 \to V_2$, $\phi_2 : V_2 \to V_1$ *τέτοιοι ώστε* $\phi_1 \circ \phi_2 = id_{V_1}$ *και* $\phi_2 \circ \phi_1 = id_{V_2}$ *τότε οι* ϕ_1 *και* ϕ_2 *λέγονται ισομορφισμοί και οι varieties ισόμορφες. Αν οι* ϕ_1, ϕ_2 *ορίζονται υπεράνω του* K, *τότε οι* V_1/K, V_2/K *λέγονται ισόμορφες.*

Το επόμενο παράδειγμα μορφισμού είναι πολύ χρήσιμο για την μελέτη μας, και θα το συναντήσουμε πολλές φορές παρακάτω όταν θα μελετάμε πεπερασμένα σώματα:

Παράδειγμα 1.1.20. Έστω $\mathbb{F}_q$ το πεπερασμένο σώμα με $q = p^n$ στοιξεία, και $V \subseteq \mathbb{P}^n(\bar{\mathbb{F}}_q)$ μια variety που ορίζεται πάνω από το $\mathbb{F}_q$. Ορίζουμε την απεικόνιση

$$\phi([x_0, x_1, ..., x_n] = [x_0^q, x_1^q, ..., x_n^q].$$

Η $\phi : V \to V$ είναι μορφισμός, που είναι $1-1$ και επί, αλλά όχι ισομορφισμός. Τα σταθερά σημεία της ϕ είναι τα στοιχεία της $V(\mathbb{F}_q)$. Η ϕ ονομάζεται μορφισμός του Frobenius.

1.2 Καμπύλες

Ορισμός 1.2.1. *Αν μια προβολική variety έχει διάσταση* 1, *τότε λέγεται καμπύλη. Μια καμπύλη συμβολίζεται συνήθως με* C.

Πρόταση 1.2.2. *Αν* C *είναι μια καμπύλη, και* $P \in C$ *λείο σημείο, ο* $\bar{K}[C]_P$ *είναι δακτύλιος διακριτής εκτίμησης (δηλαδή έχει μόνο ένα μέγιστο ιδεώδες).*

Ορισμός 1.2.3 (τάξη ρίζας και πόλου)**.** *Αν* C *είναι μια καμπύλη, και* $P \in C$ *ένα nonsingular σημείο, η κανονικοποιημένη εκτίμηση στον* $\bar{K}[C]_P$ *είναι η:* $\mathrm{ord}_P : \bar{K}[C]_P \to \mathbb{N} \cup \{\infty\}$ *με* $\mathrm{ord}_P(f) = \sup\{k : f \in M_P^k\}$. *Αν* $f/g \in \bar{K}(C)$ *ορίζουμε* $\mathrm{ord}_P(f/g) = \mathrm{ord}_P(f) - \mathrm{ord}_P(g)$, *επεκτείνοντας έτσι την* ord_P *σε* $\mathrm{ord}_P : \bar{K}(C) \to \mathbb{Z} \cup \{\infty\}$. *Ένας γεννήτορας του* M_P, *(δηλαδή ένα στοιχείο της* $\bar{K}(C)$ *με* ord_P *ίση με* 1*) καλείται uniformizer της* C *στο* P.

Αν $\mathrm{ord}_P(f) > 0$ *η* f *έχει ρίζα στο* P, *ενώ αν* $\mathrm{ord}_P(f) < 0$ *η* f *έχει πόλο στο* P. *Στην δεύτερη περίπτωση γράφουμε* $f(P) = \infty$. *Μπορεί να δείξει κανείς ότι αν η* f *δεν είναι ταυτοτικά η μηδενική, τότε έχει ρίζες και πόλους σε πεπερασμένα σημεία. Αν* $\mathrm{ord}_P(f) \geq 0$, *τότε λέμε ότι η* f *ορίζεται (ή είναι regular) στο* P.

Πρόταση 1.2.4. *Αν η καμπύλη C ορίζεται υπεράνω του K, P ένα nonsingular σημείο της $C(K)$ και t ένας uniformizer της C στο P, τότε η επέκταση σωμάτων $K(C)/K(t)$ είναι πεπερασμένη και διαχωρίσιμη.*

Εξετάζουμε τώρα τις ρητές απεικονίσεις σε σχέση με τις καμπύλες. Οι επόμενες δύο προτάσεις είναι κεντρικής σημασίας για την περαιτέρω μελέτη των καμπυλών.

Πρόταση 1.2.5. *Έστω C καμπύλη, P ένα nonsingular σημείο της, $V \subset \mathbb{P}^n$ μια variety και $\phi : C \to V$ μια ρητή συνάρτηση. Τότε η ϕ είναι regular στο P. Αν η C είναι λεία, η ϕ είναι μορφισμός.*

Απόδειξη. Έστω $\phi = [f_0, f_1, ..., f_n]$ και t ένας uniformizer της C στο P. Τότε βέβαια $f_i, t \in \bar{K}[C]$. Έστω m η ελάχιστη των τάξεων $ord_P(f_i)$ των f_i . Πολλαπλασιάζουμε τα πάντα με t^{-m} και έχουμε $\mathrm{ord}_P(f_i/t^m) \geq 0$ και $\mathrm{ord}_P(f_j/t^m) = 0$ για κάποιο f_j. Δηλαδή οι $t^{-m}f_i$ είναι regular και $t^{-m}f_j(P) \neq 0$. Άρα η ϕ είναι regular. □

Πρόταση 1.2.6. *Έστω $\phi : C_1 \to C_2$ μορφισμός καμπυλών. Τότε η ϕ είναι σταθερός μορφισμός ή είναι επί.*

Τώρα, ας θεωρήσουμε δύο καμπύλες C_1/K και C_2/K και $\phi : C_1/K \to C_2/K$ μια μη σταθερή ρητή απεικόνιση, η οποία ορίζεται υπεράνω του K.

Ορισμός 1.2.7. *Η δυική απεικόνιση της ϕ είναι η:*

$$\phi^* : K(C_2) \to K(C_1)$$

με $\phi^*(f) = f \circ \phi$.

Πρόταση 1.2.8. *Έστω C_1/K, C_2/K όπως πριν. Τότε, αν $\phi : C_1/K \to C_2/K$ μη σταθερή ρητή απεικόνιση υπεράνω του K, η επέκταση*

$$K(C_1)/\phi^*(K(C_2))$$

είναι πεπερασμένη. Επίσης:

(i) *Αν θεωρήσουμε $\iota : K(C_2) \to K(C_1)$ 1-1 που κρατάει σταθερό το K, τότε υπάρχει μοναδική μη σταθερή ρητή απεικόνιση ϕ_1 που ορίζεται υπεράνω του K ώστε η δυική ϕ_1^* της ϕ_1 να είναι η ι.*

(ii) *Αν $K \subseteq \mathbb{K} \subseteq K(C_1)$ με $[K(C_1) : \mathbb{K}] < \infty$, τότε υπάρχει μοναδική nonsingular καμπύλη C/K και μη σταθερή ρητή υπεράνω του K απεικόνιση $\phi_2 : C_1 \to C$ με*

$$\phi_2^*(K(C)) = \mathbb{K}.$$

Ορισμός 1.2.9 (Βαθμός απεικόνισης)**.** *Έστω C_1/K, C_2/K δύο καμπύλες που ορίζονται υπεράνω του σώματος K και $\phi : C_1 \to C_2$ μια απεικόνιση. Ορίζουμε τον βαθμό* deg *της ϕ ως εξής:*

(i) *Αν η ϕ είναι η σταθερή απεικόνιση, τότε* $\deg \phi = 0$

(ii) *Αν η ϕ είναι μη σταθερή απεικόνιση, ορίζουμε* $\deg \phi = [K(C_1) : \phi^*(K(C_2))]$.

Από την προηγούμενη πρόταση, ο βαθμός απεικόνισης που ορίσαμε είναι καλά ορισμένος.

Ορισμός 1.2.10. *Έστω F/K μια αλγεβρική επέκταση σωμάτων. Η επέκταση λέγεται:*

(i) *διαχωρίσιμη αν και μόνο αν για κάθε $a \in F$, το ελάχιστο πολυώνυμο του a πάνω από το K αναλύεται σε γινόμενο πρωτοβάθμιων πολυωνύμων στο F.*

(ii) *μη διαχωρίσιμη, αν δεν είναι διαχωρίσιμη.*

(iii) *πλήρως μη διαχωρίσιμη, αν και μόνο αν για κάθε $a \in F - K$, το ελάχιστο πολυώνυμο του a πάνω από το K δεν αναλύεται σε γινόμενο πρωτοβάθμιων πολυωνύμων στο F.*

Ορισμός 1.2.11. *Έστω μια ϕ όπως στο ορισμό 1.2.9. Τότε, η ϕ λέγεται διαχωρίσιμη, μη διαχωρίσιμη ή πλήρως μη διαχωρίσιμη αν η επέκταση $K(C_1)/\phi^*(K(C_2)$ έχει την αντίστοιχη ιδιότητα.*

Πρόταση 1.2.12. *Έστω C_1/K, C_2/K δύο nonsingular καμπύλες, και $\phi : C_1 \to C_2$ με $deg\phi = 1$. Τότε η ϕ είναι ισομορφισμός.*

Απόδειξη. Αφού $\deg \phi = 1$ έχουμε ότι

$$[K(C_1)/\phi^*(K(C_2))] = 1 \Longleftrightarrow K(C_1) = \phi^*(K(C_2)).$$

Έπεται ότι η ϕ^* είναι ισομορφισμός των $K(C_1)$ και $(K(C_2))$. Απ το (i) της πρότασης 1.2.8, υπάρχει $\psi : C_2 \to C_1$ με $\psi^* = (\phi^*)^{-1}$. Αφού η C_2 είναι nonsingular, η ψ είναι μορφισμός. Η $\psi^* \circ \phi^* = (\phi \circ \psi)^*$ είναι η ταυτοτική στο $\bar{K}(C_2)$ (και η $(\psi \circ \phi)^*$ στο $\bar{K}(C_1)$). Πάλι από την μοναδικότητα του (i) της πρότασης 1.2.8, έπεται ότι οι $\phi \circ \psi$ και $\psi \circ \phi$ είναι οι αντίστοιχες ταυτοτικές απεικονίσεις. □

Ορισμός 1.2.13. *Έστω $\phi : C_1 \to C_2$ μια μη σταθερή απεικόνιση, όπου C_1, C_2 nonsingular. Έστω ακόμα ένα σημείο P της C_1 και $t_{\phi(P)}$ ο uniformizer της C_2 στο σημείο $\phi(P)$. Ο δείκτης διακλάδωσης (ramification index) της ϕ στο P ορίζεται να είναι ο αριθμός $\mathrm{ord}_P(\phi^*(t_{\phi(P)}))$, και συμβολίζεται με $e_\phi(P)$. Αν ο δείκτης διακλάδωσης της ϕ στο P είναι 1, η ϕ λέγεται αδιακλάδιστη στο P. Η ϕ λέγεται αδιακλάδιστη αν είναι αδιακλάδιστη παντού στην C_1.*

Η σημασία της επόμενης πρότασης είναι μεγάλη, καταρχάς επειδή μας δίνει έναν τρόπο να μετρήσουμε το βαθμό μιας απεικόνισης μεταξύ καμπυλών.

Πρόταση 1.2.14. *Έστω $\phi : C_1 \to C_2$ μια μη σταθερή απεικόνιση και C_1, C_2 nonsingular. Τότε:*

(i) *Για κάθε σημείο Q της C_2 έχουμε ότι το άθροισμα των βαθμών διακλάδωσης των σημείων $P \in \phi^{-1}(Q)$ ισούται με τον βαθμό $\deg(\phi)$ της ϕ.*

(ii) *Για σχεδόν όλα τα Q της C_2 (εκτός από πεπερασμένα) ισχύει ότι:*

$$|\phi^{-1}(Q)| = \deg_s(\phi)$$

όπου με $\deg_s(\phi)$ συμβολίζουμε τον βαθμό διαχωρισιμότητας της επέκτασης

$$K(C_1)/\phi^*(K(C_2).$$

(iii) *Έστω $\psi : C_2 \to C_3$ όπως η $\phi : C_1 \to C_2$. Τότε ο δείκτης διακλάδωσης της σύνθεσης αναλύεται στους δείκτες διακλάδωσης των συναρτήσεων, δηλαδή:*

$$e_{\psi\circ\phi}(P) = e_\phi(P)e_\psi(P)$$

για κάθε σημείο P της C_1.

Πόρισμα 1.2.15. *Η $\phi : C_1 \to C_2$ είναι αδιακλάδιστη $\iff$ για κάθε σημείο Q της C_2 έχουμε ισότητα στον πρώτο ισχυρισμό πρότασης 1.2.14, δηλαδή $|\phi^{-1}(Q)| = \deg(\phi)$.*

Απόδειξη. Άμεση από την πρόταση 1.2.14, καθώς και το γεγονός ότι $e_\phi(P) \geq 1$. □

Πριν προχωρήσουμε παρακάτω στην θεωρία, ας επιστρέψουμε λίγο στο βασικό παράδειγμα μορφισμού που έχουμε δώσει, τον μορφισμό του Frobenius. Όπως θα δούμε στο επόμενο κεφάλαιο, ο μορφισμός του Frobenius είναι βασικός για την μελέτη των ελλειπτικών καμπυλών που ορίζονται πάνω από πεπερασμένα σώματα.

Έστω λοιπόν πως δουλεύουμε πάνω από ένα σώμα K χαρακτηριστικής $p > 0$ (όχι απαραίτητα πεπερασμένο προς το παρόν) και θεωρούμε ένα πολυώνυμο $f \in K[x_1, x_2, ..., x_n]$. Θεωρούμε τον μορφισμό του Frobenius να δρα πάνω στο f μέσω των συντελεστών του, υψώνοντας δηλαδή κάθε συντελεστή του πολυωνύμου εις την q, όπου $q = p^r$. Συμβολίζουμε με $f^{(q)}$ την εικόνα του f. Ορίζουμε τώρα το ιδεώδες I που παράγεται από τις εικόνες $f^{(q)}$ για όλα τα $f \in I(C)$ και ορίζουμε την καμπύλη $C^{(q)}/K$ να είναι εκείνη που το ομογενές ιδεώδες της $I(C^{(q)})$ ισούται με το I.

Παρατηρούμε ότι ορίζεται με φυσιολογικό τρόπο ένας μορφισμός του Frobenius, ο «ύψωση εις την q-οστή δύναμη» Frobenius:

$$\phi : C \to C^{(q)} : \phi([x_0, x_1, ...x_n]) = [x_0^q, x_1^q, ..., x_n^q]$$

και είναι απλό να δει κανείς ότι ο μορφισμός αυτός ορίζεται καλά.

Το επόμενο θεώρημα μελετάει κάποιες βασικές ιδιότητες του μορφισμού του Frobenius. Η πιο σημαντική από τις παρακάτω ιδιότητες του είναι η τρίτη, η οποία θα μας χρειαστεί άμεσα παρακάτω στην απόδειξη της αρχής του Hasse.

Θεώρημα 1.2.16. *Έστω σώμα K με χαρ(K)$= p > 0$ και q μια δύναμη του p. Θεωρούμε ακόμη μια καμπύλη C που ορίζεται υπεράνω του K και τον μορφισμό του Frobenius $\phi : C \to C^{(q)}$. Τότε ισχύουν:*

(i) $\phi^*(K(C^{(q)}) = K(C)^q$.

(ii) *ο ϕ είναι πλήρως μη διαχωρίσιμος.*

(iii) $\deg \phi = q$.

1.3 Divisors και Διαφορικά

Ορισμός 1.3.1. *Θεωρούμε την ελεύθερη αβελιανή ομάδα που παράγεται από τα στοιχεία της καμπύλης C, δηλαδή την ομάδα που τα στοιχεία της είναι τυπικά αθροίσματα της μορφής $\sum n_P(P)$, $P \in C$, όπου $n_P \in \mathbb{Z}$ και πεπερασμένοι απ' αυτούς είναι μη μηδενικοί. Τα τυπικά αυτά αθροίσματα ονομάζονται divisors, και συμβολίζονται συνήθως με D, η δε ομάδα τους ονομάζεται ομάδα των divisors, και συμβολίζεται με* $\mathrm{Div}(C)$.

Αν $D = \sum n_P(P)$ είναι ένας divisor, ορίζουμε τον βαθμό του να είναι η ποσότητα

$$\deg D = \sum n_P$$

Παρατηρείστε ότι ο βαθμός ενός divisor ορίζεται καλά, αφού το άθροισμα είναι πεπερασμένο. Ένας divisor λέγεται μηδενικός αν $\deg D = 0$. Το σύνολο των μηδενικών divisors είναι προφανώς υποομάδα της $\mathrm{Div}(C)$ και συμβολίζεται με $\mathrm{Div}^0(C)$. Ορίζουμε επίσης με $\mathrm{Div}_K(C)$ την υποομάδα των divisors που μένουν αναλλοίωτοι υπό την δράση της ομάδας Galois $\mathrm{Gal}(\bar{K}/K)$ της επέκτασης $\bar{K}/K$, και παρόμοια την $\mathrm{Div}^0_K(C)$.

Θεωρούμε τώρα μια συνάρτηση $f \in \bar{K}(C)^*$, όπου η C είναι λεία.

Ορισμός 1.3.2. *Ως divisor της f ορίζεται η ποσότητα:*

$$\mathrm{div}(f) = \sum_{P \in C} \mathrm{ord}_P(f)(P).$$

Αφού η f έχει πεπερασμένες ρίζες και πόλους, το άθροισμα αυτό είναι πεπερασμένο, άρα ο $\mathrm{div}(f)$ ορίζεται καλά.

Παρατηρούμε ότι αν η $f \in K(C)$, τότε $\mathrm{div}(f) \in \mathrm{Div}_K(C)$.

Ορισμός 1.3.3. *Ένας divisor D με $D = \mathrm{div}(f)$ για κάποια $f \in \bar{K}(C)^*$ λέγεται πρωταρχικός. Αν D_1, D_2 είναι δύο divisors, τότε αυτοί λέγονται (γραμμικά) ισοδύναμοι αν και μόνο αν η διαφορά τους είναι πρωταρχικός. Σ' αυτήν την περίπτωση, γράφουμε $D_1 \sim D_2$. Παρατηρούμε ότι η σχέση αυτή είναι όντως ισοδυναμία.*

Ορισμός 1.3.4. *Η ομάδα Picard της C είναι η ομάδα πηλίκο της $\mathrm{Div}(C)$ προς την υποομάδα των πρωταρχικών divisors,και συμβολίζεται με $\mathrm{Pic}(C)$. Όμοια με πριν, ορίζουμε την $\mathrm{Pic}_K(C)$ ως τα σημεία της $\mathrm{Pic}(C)$ που μένουν αναλλοίωτα υπό την δράση της $\mathrm{Gal}(\bar{K}/K)$.*

Η $\mathrm{Pic}_K(C)$ δεν ταυτίζεται με το πηλίκο της $\mathrm{Div}_K(C)$ προς τους πρωταρχικούς divisors.

Πρόταση 1.3.5. *Θεωρούμε μια λεία καμπύλη C και μια $f \in \bar{K}(C)^*$. Τότε έχουμε ότι:*

(i) $\mathrm{div}(f) = 0$ *αν και μόνο αν η f είναι σταθερή*

(ii) $\deg(\mathrm{div}(f)) = 0$.

Ορισμός 1.3.6. *Από την προηγούμενη πρόταση έπεται ότι οι πρωταρχικοί divisors αποτελούν υποομάδα της $\mathrm{Div}^0(C)$. Την ομάδα πηλίκο της $\mathrm{Div}^0(C)$ προς τους πρωταρχικούς divisors την συμβολίζουμε με $\mathrm{Pic}^0(C)$. Όμοια με πριν ορίζεται και η $\mathrm{Pic}^0_K(C)$.*

Πρόταση 1.3.7. *Έστω η μη σταθερή απεικόνιση*

$$\phi : C_1 \to C_2,$$

όπου οι C_1 και C_2 είναι λείες. Τότε, η δυική ϕ^* της ϕ έχει τις παρακάτω ιδιότητες:

(i) $\deg \phi^* D = \deg \phi \deg D$ *για κάθε* $D \in \mathrm{Div}(C_2)$

(ii) $\phi^*(\mathrm{div}(f)) = \mathrm{div}(\phi^* f)$ *για κάθε* $f \in \bar{K}(C_2)^*$

(iii) *Αν* η $\psi : C_2 \to C_3$ *είναι όπως η* ϕ, *τότε* $(\psi \circ \phi)^* = \phi^* \circ \psi^*$

Προχωράμε τώρα στην μελέτη των διαφορικών μορφών που ορίζονται πάνω σε μια καμπύλη.

Ορισμός 1.3.8. *Θεωρούμε μια καμπύλη* C *που ορίζεται από ένα σώμα* K. *Θεωρούμε το σύνολο των τυπικών συμβόλων της μορφής* dx, *όπου* $x \in \bar{K}(C)$, *και που υπακούουν στους συνήθεις κανόνες παραγώγισης:*

(i) $d(x + y) = dx + dy$

(ii) $d(xy) = xdy + ydx$

(iii) *Αν* $x \in \bar{K}$, *τότε* $dx = 0$

Συμβολιζουμε με Ω_C *τον διανυσματικό χώρο που παράγουν αυτά τα τυπικά σύμβολα υπεράνω του σώματος* $\bar{K}$. *Ένα σύμβολο της μορφής* $f(x)dx$ *καλείται διαφορική μορφή (ή διαφορικό), και ο* Ω_C *καλείται συνήθως χώρος των διαφορικων μορφών της* C.

Παρατηρούμε ότι η δυική ϕ^* μιας $\phi : C_1 \to C_2$ επάγει μια απεικόνιση $\phi^* : \Omega_{C_2} \to \Omega_{C_1}$ μέσω του κανόνα:

$$\phi^* \left(\sum f_i dx_i \right) = \sum \phi^*(f_i) d(\phi^*(x_i)).$$

Πρόταση 1.3.9. (i) *Ο* $\bar{K}(C)-$*διανυσματικός χώρος* Ω_C *έχει διάσταση 1.*

(ii) *Το* dx *παράγει τον* Ω_C *αν και μόνο αν η* $\bar{K}(C)/\bar{K}(x)$ *είναι πεπερασμένη και διαχωρίσιμη.*

(iii) *Η* ϕ *είναι διαχωρίσιμη αν και μόνο αν η* $\phi^* : \Omega_{C_2} \to \Omega_{C_1}$ *είναι μη τετριμμένη.*

Πρόταση 1.3.10. *Έστω* C *μια καμπύλη,* $P \in C$ *ένα σημείο της και* t *ένας uniformizer της* C *στο* P. *Τότε:*

(i) *Για κάθε διαφορική μορφή* ω *υπάρχει μοναδική* g *στον* $\bar{K}(C)$, *που εξαρτάται μόνο απ' τα* ω *και* t, *ώστε* $\omega = gdt$. *Συμβολίζουμε* $g = \omega/dt$

(ii) *Έστω μια διαφορική μορφή* ω, *που δεν είναι εκ ταυτότητος η μηδενική. Η τάξη* $\mathrm{ord}_P(\omega/dt)$ *είναι ανεξάρτητη του* t. *Την συμβολίζουμε με* $\mathrm{ord}_P(\omega)$. *Η ποσότητα αυτή είναι διαφορετική του* 0 *για πεπερασμένα το πολύ σημεία* P.

Ορισμός 1.3.11 (Divisor διαφορικού)**.** *Έστω* ω *μια διαφορική μορφή της καμπύλης* C. *Ορίζουμε τον divisor της μορφής* ω *να είναι ο:*

$$\mathrm{div}(\omega) = \sum_{P \in C} \mathrm{ord}_P(\omega)(P).$$

Αν για κάθε σημείο P *της καμπύλης η τάξη* $\mathrm{ord}_P(\omega)$ *είναι* ≥ 0, *τότε λεμε ότι το* ω *είναι ολόμορφο. Αν για κάθε* P *έχουμε* $\mathrm{ord}_P(\omega) \leq 0$, *τότε λέγεται nonvanishing.*

Μπορούμε τώρα να ορίσουμε τους κανονικούς divisor:

Ορισμός 1.3.12 (Κανονικός divisor)**.** *Αφού* $\dim_{\bar{K}(C)} \Omega_C = 1$*, αν μας δοθούν δύο διαφορικά* ω_1, ω_2*, τότε τα συνδέει μια γραμμική σχέση* $\omega_1 = f\omega_2$ *για κάποια* f *στον* $\bar{K}(C)$*. Τότε προφανώς* $\operatorname{div}(\omega_1) = \operatorname{div}(f) + \operatorname{div}(\omega_2)$*. Άρα, μπορούμε να διαλέξουμε μια* f *ώστε να έχουμε* $\operatorname{div}(\omega_1) = 0$*. Κάθε divisor που ανήκει στην εικόνα του* $\operatorname{div}(\omega)$ *του τυχόντος μη μηδενικού διαφορικού* ω *μέσα στην ομάδα Picard της* C *καλείται κανονικός divisor της καμπύλης* C*.*

Οι κανονικοί divisors θα αποκτήσουν εξαιρετικά μεγάλη σημασία στην αμέσως επόμενη παράγραφο.

1.4 Το Θεώρημα Riemann-Roch και το Θεώρημα του Hurwitz

Θεωρούμε τώρα μια καμπύλη C και έστω $\operatorname{Div}(C)$ η ομάδα των divisors πάνω στην C.

Ορισμός 1.4.1. *Θα καλούμε έναν divisor* $D = \sum n_P(P)$ *θετικό αν* $n_P \geq 0$ *για κάθε* P*. Ομοίως, αν* D_1, D_2 *είναι δύο divisors, καλούμε τον* D_1 *μεγαλύτερο από τον* D_2 *αν και μόνο αν η διαφορά τους είναι θετικός divisor. (Γράφουμε* $D \geq 0$ *για να συμβολίσουμε ότι ο* D *είναι θετικός).*

Με βάση τα παραπάνω, παρατηρούμε ότι μια συνάρτηση f είναι παντού regular εκτός από το σημείο P, και έχει πόλο τάξης το πολύ n στο P αν και μόνο αν

$$\operatorname{div}(f) \geq -n(P).$$

Ομοίως, η f έχει ρίζα τάξης τουλάχιστον n σε ένα σημείο P και είναι παντού αλλού regular αν και μόνο αν

$$\operatorname{div}(f) \geq n(P).$$

Με αυτόν τον τρόπο δηλαδή, αναγάγαμε τον τρόπο διατύπωσης της ύπαρξης ριζών ή πόλων σε διατύπωση μέσω ανισοτήτων. Για παράδειγμα, παρατηρείστε ότι με βάση τον παραπάνω ορισμό, ένα διαφορικό ω είναι ολόμορφο αν και μόνο αν το $\operatorname{div}(\omega)$ είναι θετικός divisor, ενώ είναι nonvanishing αν και μόνο αν ο $\operatorname{div}(\omega)$ είναι αρνητικός. Η σημασία της μερικής διάταξης που εισαγάγαμε στην ομάδα των divisors θα φανεί αμέσως από τον ορισμό που ακολουθεί:

Ορισμός 1.4.2. *Έστω* D *ένας divisor της καμπύλης* C*. Ορίζουμε των διανυσματικό χώρο όλων των πρωταρχικών divisors που είναι μεγαλύτεροι, με την παραπάνω έννοια, του* $-D$*:*

$$L(D) = \{f \in \bar{K}(C)^* : \operatorname{div}(f) \geq -D\} \cup \{0\}$$

Είναι προφανές ότι ο χώρος $L(D)$ είναι διανυσματικός χώρος υπεράνω του σώματος $\bar{K}$, και συμβολίζουμε με $\ell(D)$ την διάσταση του υπεράνω του $\bar{K}$. Εκείνο που δεν είναι προφανές είναι πως ο χώρος αυτός έχει πεπερασμένη διάσταση:

Θεώρημα 1.4.3. *Έστω* D *ένας divisor της καμπύλης* C*. Τότε:*

(i) *Ο* $L(D)$ *έχει πεπερασμένη διάσταση.*

(ii) *Αν* $\deg D < 0$ *τότε ο* $L(D)$ *είναι τετριμμένος και άρα* $\ell(D) = 0$*.*

(iii) *Αν D_1 είναι ένας άλλος divisor με $D_1 \sim D$, τότε $L(D) \simeq L(D_1)$.*

Απόδειξη. (i) [Hartshorne, [10], κεφ.2, πρόταση 5.19].

(ii) Έστω ότι ο χώρος είναι μη τετριμμένος, και έστω μια $f \in L(D)$ με f όχι ταυτοτικά μηδενική. Τότε θα έχουμε

$$-\deg D = \deg(-D) \leq \deg(\mathrm{div}(f)) = 0$$

δηλαδή $\deg D \geq 0$.

(iii) Γράφουμε τον D_1 στην μορφή $D = D_1 + \mathrm{div}(g)$. Τότε παίρνουμε έναν ισομορφισμό:

$$F : L(D) \to L(D_1)$$

με $F(f) = fg$.

□

Έστω $K = \mathrm{div}(\omega)$ ένας κανονικός divisor της καμπύλης C, και έστω μια f στον $L(K)$. Τότε $\mathrm{div}(f) + \mathrm{div}(\omega) \geq 0 \iff \mathrm{div}(f\omega) \geq 0$. Άρα το $f\omega$ είναι ολόμορφο $\iff f \in L(K)$. Σαν συμπέρασμα, παίρνουμε ότι ο $\bar{K}$-χώρος $L(K)$ είναι ισόμορφος με τον $\bar{K}$-χώρο των ολόμορφων διαφορικών. Δεν είναι καθόλου προφανές με ποιόν τρόπο εξαρτάται ο $\ell(K)$ από την καμπύλη C.

Θεώρημα 1.4.4 (Riemann-Roch για καμπύλες)**.** *Έστω C μια λεία καμπύλη, και έστω K ένας κανονικός divisor της. Τότε, υπάρχει ένας ακέραιος $g \geq 0$, που εξαρτάται μόνο από την καμπύλη C, τέτοιος ώστε για κάθε divisor D της C να ισχύει:*

$$\ell(D) - \ell(K - D) = \deg D - g + 1$$

Ο φυσικός αριθμός g ονομάζεται γένος της καμπύλης C.

Πόρισμα 1.4.5. (i) $\ell(K) = g$

(ii) $\deg K = 2g - 2$

(iii) *Αν $\deg D > 2g - 2$ τότε $\ell(D) = \deg D - g + 1$.*

Απόδειξη. (i) Θέτουμε $D = 0$ στον τύπο του Riemann-Roch.

(ii) Θέτουμε $D = K$ στον τύπο του Riemann-Roch.

(iii) Έχουμε ότι $\deg(K - D) = \deg(K) - \deg(D) < 0$, άρα, χρησιμοποιώντας το ερώτημα (ii) του προηγούμενου ερωτήματος, παίρνουμε ότι $\ell(K - D) = 0$, και αντικαθιστούμε στον τύπο του Riemann-Roch.

□

Μπορούμε τώρα να δούμε κάποια απλά παραδείγματα:

(i) Το γένος του $\mathbb{P}^1$ είναι 0.

(ii) Έστω $C : y^2 = (x - a_1)(x - a_2)(x - a_3)$, όπου $a_i \in \bar{K}$ διακριτά μεταξύ τους και $\mathrm{χαρ}(K) \neq 2$. Τότε η C έχει γένος 1.

Πρόταση 1.4.6. *Έστω μια λεία καμπύλη C που ορίζεται πάνω από ένα σώμα K. Θεωρούμε και έναν divisor D που ανήκει στην $\mathrm{Div}_K(C)$. Τότε ο $L(D)$ έχει μια βάση από στοιχεία του $K(C)$.*

Ο αριθμός $2-2g$ ονομάζεται χαρακτηριστική Euler-Poincare της καμπύλης C. Κλείνουμε την σύντομη αυτήν εισαγωγή με ένα κλασσικό αποτέλεσμα του Hurwitz:

Θεώρημα 1.4.7 (Hurwitz για καμπύλες)**.** *Έστω C_1 και C_2 δύο nonsingular καμπύλες με γένη g_1 και g_2 αντίστοιχα, και $\phi : C_1 \to C_2$ μια μη τετριμμένη διαχωρίσιμη απεικόνιση. Τότε, ισχύει η ανισότητα:*

$$2g_1 - 2 \geq (2g_2 - 2)\deg\phi + \sum_{P \in C_1} (e_\phi(P) - 1)$$

Ειδικότερα, αν είμαστε πάνω από σώμα K με χαρακτηριστική 0, τότε έχουμε ισότητα στον ανωτέρω τύπο.

Είναι δύσκολο να υποτιμήσουμε την σημασία του θεωρήματος Riemann-Roch. Παρατηρούμε ότι προς το παρόν είναι το βασικό αποτέλεσμα που μετράει κάτι. Η βασική του εφαρμογή έγκειται στο να μετράει την διάσταση χώρων συναρτήσεων που εκ των προτέρων θέλουμε να ικανοποιούν συγκεκριμμένες ιδιότητες. Η σημασία του θα φανεί στα επόμενα κεφάλαια, όπου μεταξύ των άλλων εφαρμογών του θεωρήματος Riemann-Roch συμπεριλαμβάνονται η ύπαρξης κανονικής μορφής Weierstrass για κάθε καμπύλη γένους 1 (δηλαδή κάθε καμπύλη γένους 1 αντιστοιχεί σε μια εξίσωση, κάτι που στα μεγαλύτερα γένη δεν συμβαίνει) καθώς και το πεπερασμένο της διάστασης διανυσματικών χώρων που αποτελούνται από modular forms. Το τελευταίο θα προκύψει απ΄ το Riemann-Roch για επιφάνειες Riemann. Σε αυτό το σημείο, αξίζει να αναφερθεί ότι η πρώτη ιστορικά διατύπωση του Riemann-Roch είναι ειδική περίπτωση του ανωτέρου, και δόθηκε για επιφάνειες Riemann (κεφάλαιο 3). Η γενίκευση που δώσαμε πιο πάνω οφείλεται στον Schmidt (1929).

Κεφάλαιο 2

Ελλειπτικές Καμπύλες

Κύριος στοχος μας σε αυτό το κεφάλαιο είναι να μελετήσουμε εκτενώς τις ελλειπτικές καμπύλες. Πριν προχωρήσουμε όμως στην μελέτη τους, θα περιγράψουμε τον λόγο που μελετάει κανείς ελλειπτικές καμπύλες. Αν μπορεί να πει κανένας ότι ένας από τους βασικούς στόχους της άλγεβρας είναι εν γένει να περιγράψει όσο μπορεί καλύτερα τις λύσεις των πολυωνυμικών εξισώσεων, τότε σίγουρα ένας από τους βασικούς στόχους της θεωρίας αριθμών είναι η λύση των διοφαντικών εξισώσεων, οι οποίες είναι πολυωνυμικές με συντελεστές από το $\mathbb{Z}$ (ή, στην χειρότερη περίπτωση, από το $\mathbb{Q}$), και για τις οποίες ζητάει κανείς να βρει τις ακέραιες (αντίστοιχα τις ρητές) λύσεις τους. Αν θεωρήσουμε ότι η θεωρία Galois δίνει μια ικανοποιητική απάντηση στην περίπτωση της μιας μεταβλητής, καλούμαστε να λύσουμε τα πολυώνυμα σε δύο μεταβλητές x, y.

Θεωρούμε λοιπόν ένα πολυώνυμο $f \in \mathbb{Q}[x, y]$, και αναζητούμε τις ρητές λύσεις της εξίσωσης $f(x, y) = 0$. Αν το πολυώνυμο είναι βαθμού 1, δηλαδή είναι γραμμικό, το φέρνουμε στην μορφή $f(x, y) = ax + by - c$ με $a, b, c \in \mathbb{Z}$, και τότε η απάντηση είναι απλή: υπάρχουν λύσεις αν και μόνο αν $(a, b) | c$, και αν υπάρχουν εύκολα τις βρίσκουμε όλες. Αν είναι βαθμού 2, δηλαδή μία κωνική τομή, τότε υπάρχει ένα θεώρημα, που μας δίνει μια εξίσου ικανοιητική απάντηση:

Θεώρημα 2.0.8 (Αρχή Hasse-Minkowski)**.** *Ένα πολυώνυμο 2ου βαθμού $f(x, y)$ με ρητούς συντελεστές έχει λύσεις στο $\mathbb{Q}$ αν και μόνο αν έχει λύσεις στο $\mathbb{R}$ και στο $\mathbb{Q}_p$, για κάθε πρώτο p, όπου με $\mathbb{Q}_p$ συμβολίζουμε το σώμα των p-αδικών ρητών.*

Ερχόμαστε τώρα λοιπόν φυσιολογικά στην μελέτη των τριτοβάθμιων πολυωνύμων σε δύο μεταβλητές. Μια από τις πιο σημαντικές παρατηρήσεις του Weierstrass ήταν πως, αν διαλέξει κάποιος ένα τριτοβάθμιο πολυώνυμο $f(x, y)$ με ρητούς συντελεστές, μπορεί πάντα να το φέρει σε πιο απλή μορφή (την οποία ονομάζουμε μορφή Weierstrass) και αρκεί να λύσει αυτή (τότε, με ρητές απεικονίσεις και δουλεύοντας προς τα πίσω, ανάγεται σε ρητές λύσεις της αρχικής εξίσωσης). Δεν είναι λοιπόν τυχαίο που ξεκινάμε την μελέτη των ελλειπτικών καμπυλών από τις κανονικές μορφές Weierstrass. Επίσης, αν ζητάμε τις λύσεις ενός πολυωνύμου που ορίζεται πάνω από το K, και ονομάσουμε E την καμπύλη που αντιστοιχεί στο πολυώνυμο, οι λύσεις αυτού του πολυωνύμου αποκτούν με φυσιολογικό τρόπο δομή ομάδας (την οποία θα συμβολίσουμε με $E(K)$). Ένας από τους βασικούς μας σκοπούς στο κεφάλαιο αυτό είναι να μελετήσουμε σε διάφορες περιπτώσεις αυτήν την ομάδα, της οποίας η δομή εξαρτάται από το σώμα πάνω από το οποίο βρίσκεται η καμπύλη που εξετάζουμε.

Πιο συγκεκριμμένα, στόχος μας είναι η μελέτη της $E(K)$ οπου $K = \mathbb{F}_q, \mathbb{C}, \mathbb{R}, \mathbb{Q}$ και τέλος ένα τυχαίο σώμα αριθμών. Όπως είναι βέβαια αναμενόμενο, η μέθοδος της μελέτης και η κατανόηση της $E(K)$ διαφερει αναλόγως το σώμα K πάνω από το οποίο ορίζεται. Στο $\mathbb{C}$ και στο $\mathbb{R}$ η κατανόηση έρχεται μέσα από την γεωμετρική δομή της καμπύλης. Πάνω όμως από ένα πεπερασμένο ή πάνω από ένα global σώμα η κατανόηση είναι πιο δύσκολη. Στα πεπερασμένα σώματα, δύο είναι τα βασικά θεωρήματα που θα αποδείξουμε σχετικά με τις ομάδες αυτές: το Θεώρημα του Hasse και οι εικασίες του Weil για ελλειπτικές καμπύλες. Τέλος, όσον αφορά τα σώματα αριθμών, η περιγραφή της δομής τους δίνεται από το θεώρημα Mordell-Weil.

2.1 Μορφές Weierstrass

Όπως σημειώσαμε και παραπάνω, θα ξεκινήσουμε την μελέτη μας θεωρώντας την εξίσωση (δηλαδή την καμπύλη) γραμμένη στην απλούστερη δυνατή μορφή. Η απόδειξη του γεγονότος πως κάθε nonsingular καμπύλη γένους 1 έχει μια εξίσωση Weierstrass (και άρα δεν χάνουμε ιδιαίτερα σε γενικότητα όσον αφορά την μελέτη μας) θα αποδειχθεί σε επόμενη παράγραφο, με χρήση, όπως τονίσαμε και προηγουμένως, του Riemann-Roch.

Ορισμός 2.1.1. *Έστω K ένα τέλειο σώμα. Στο $\mathbb{P}^2(\bar{K})$ θεωρούμε την εξίσωση:*

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

όπου $a_1, ..., a_6 \in \bar{K}$. Μια κυβική καμπύλη (cubic curve) E είναι το σύνολο των λύσεων μιας τέτοιας εξίσωσης. Το σημείο $O = [0, 1, 0]$ λέγεται base point της καμπύλης. Η εξίσωση αυτή λέγεται (κανονική) εξίσωση ή μορφή Weierstrass της καμπύλης.

Αποομογενοποιώντας, μπορούμε, θέτοντας $x = X/Z$ και $y = Y/Z$, να γραψουμε την παραπάνω εξίσωση στην αφφινική μορφή:

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

μην ξεχνώντας ότι υπάρχει και ένα σημείο $O = [0, 1, 0]$ στο άπειρο. Αν ισχύει ότι $a_1, ..., a_6 \in K$, τότε, ως συνήθως, λέμε ότι η E ορίζεται υπεράνω του K και γράφουμε E/K.

Παρατηρήσεις:

(i) Αν $\text{χαρ}(K) \neq 2$, ο μετασχηματισμός

$$y \longrightarrow \frac{1}{2}(y - a_1x - a_3)$$

φέρνει την E στην μορφή

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

όπου $b_2 = {a_1}^2 + 4a_4$, $b_4 = 2a_4 + a_1a_3$ και $b_6 = a_3^2 + 4a_6$

(ii) Αν επιπλέον ισχύει ότι $\text{χαρ}(K) \neq 2, 3$ τότε οι μετασχηματισμοί

$$x \longrightarrow \frac{x - 3b_2}{36}, y \longrightarrow \frac{y}{108}$$

φέρνουν την E στην μορφή

$$E : y^2 = x^3 - 27c_4x - 54c_6 = x^3 + Ax + B.$$

Ορισμός 2.1.2. *Έστω μια κυβική καμπύλη στην αφφινική της μορφή Weierstrass. Ορίζουμε τις ποσότητες:*

$$\begin{aligned} b_8 &= {a_1}^2 a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 \\ c_4 &= b_2^2 - 24b_4 \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6 \\ \Delta &= b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 \\ j &= c_4^3/\Delta \end{aligned}$$

καθώς και το διαφορικό

$$\omega = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}$$

Η ποσότητα Δ λέγεται διακρίνουσα της εξίσωσης Weierstrass, η j λέγεται j-invariant (j-αναλλοίωτη) της καμπύλης και το ω λέγεται invariant (αναλλοίωτο) διαφορικό της εξίσωσης. Συχνά θα συμβολίζουμε με j_E, Δ_E και ω_E ή $j(E)$, $\Delta(E)$ και $\omega(E)$ τις αντίστοιχες ποσότητες της καμπύλης E. Παρατηρείστε ότι η $j(E)$ της E ορίζεται αν και μόνο αν $\Delta(E) \neq 0$.

Ορισμός 2.1.3. *Έστω P ένα σημείο της καμπύλης E. Αν $f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6$ και το P είναι singular point της E, έπεται ότι:*

$$\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0$$

Τότε, αν $P = (x_0, y_0)$, έπεται ότι υπάρχουν $\alpha, \beta \in \bar{K}$ τέτοια ώστε

$$f(x, y) - f(x_0, y_0) = ((y - y_0) - \alpha(x - x_0))((y - y_0) - \beta(x - x_0)) - (x - x_0)^3$$

Διακρίνουμε δύο περιπτώσεις:

(i) *Αν $\alpha \neq \beta$ το P λέγεται node σημείο της E. Τότε, η καμπύλη E έχει δύο εφαπτόμενες στο σημείο P, τις:*

$$y = \alpha(x - x_0) + y_0$$

και

$$y = \beta(x - x_0) + y_0$$

(ii) *Αν $\alpha = \beta$ το P λέγεται cusp σημείο της E. Τότε η καμπύλη E έχει μία εφαπτόμενη στο σημείο P, την*

$$y = \alpha(x - x_0) + y_0.$$

Ορισμός 2.1.4. *Αν η κυβική καμπύλη E δεν έχει singular point, τότε η E ονομάζεται ελλειπτική καμπύλη (elliptic curve).*

Παρατηρούμε οτι αν χαρ$(K) \neq 2, 3$ τότε, όπως είπαμε και προηγουμένως, η E έχει μια εξίσωση Weierstrass της μορφής

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

που είναι η απλούστερη δυνατή μορφή στην οποία μπορούμε εν γένει να φέρουμε μια κυβική καμπύλη. Σε αυτήν την περίπτωση, είναι απλό να δει κανείς ότι η E είναι ελλειπτική αν και μόνο αν το $g(x)$ δεν έχει διπλή ρίζα σε μία αλγεβρική κλειστότητα του σώματος ορισμού. Πριν προχωρήσουμε παρακάτω, είναι χρήσιμο να αναφέρουμε δύο ειδικές μορφές μιας κυβικής καμπύλης οι οποίες σε ορισμένες περιπτώσεις παρουσιάζουν ξεχωριστό ενδιαφέρον:

Ορισμός 2.1.5. (i) *Μια μορφή Legendre μιας κυβικής καμπύλης είναι μια εξίσωση της μορφής*

$$E_\lambda : y^2 = x(x-1)(x-\lambda)$$

Αν ισχύει ότι χαρ$(K) \neq 2$ τότε κάθε ελλειπτική καμπύλη είναι ισόμορφη υπεράνω του $\bar{K}$ με μια ελλειπτική καμπύλη στην μορφή Legendre για κάποιο $\lambda \in \bar{K}$ με $\lambda \neq 0, 1$.

(ii) *(Κανονική Μορφή Deuring) Αν χαρ$(K) \neq 3$ τότε η E έχει μια εξίσωση Weierstrass υπεράνω του $\bar{K}$ της μορφής*

$$E_a : y^2 + axy + y = x^3$$

όπου $a \in \bar{K}$ και $a^3 \neq 27$.

Κάτω από τους μετασχηματισμούς $x = u^2x' + r$ και $y = u^3y' + u^2sx' + t$, όπου $u, r, s, t \in \bar{K}$ και $u' \neq 0$, παρατηρούμε ότι η ποσότητα j' ισούται με j, δηλαδή η j-invariant μένει αναλλοίωτη από τους ανωτέρω μετασχηματισμούς. Θα δείξουμε πως υπό τον φυσιολογικό περιορισμό η E να τέμνει την επ΄ άπειρον ευθεία μόνο στο $[0, 1, 0]$, αυτοί είναι όλοι οι μετασχηματισμοί της καμπύλης στο $\mathbb{P}^2$ (δηλαδή, μέχρις $\bar{K}$-ισομορφισμού, δύο κανονικές μορφές Weierstrass E, E' αντιπροσωπεύουν την ίδια καμπύλη αν και μόνο αν $j(E) = j(E')$.

Έστω χαρ$(K) \neq 2, 3$. Τότε, θεωρώντας την καμπύλη στην απλοποιημένη κανονική μορφή Weierstrass

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

έχουμε

$$\Delta = -16(4A^3 + 27B^2)$$

και

$$j = -1728\frac{(4A)^3}{\Delta}$$

Σ΄ αυτήν την περίπτωση, θα δείξουμε ότι η μόνη αλλαγή μεταβλητών που διατηρεί την κανονική μορφή Weierstrass είναι η:

$$(x, y) \to (u^2x', u^3y')$$

όπου $u \in \bar{K}^*$. Εχουμε $A = u^4A', B = u^6B', \Delta = u^{12}\Delta'$

Πρόταση 2.1.6. *Έστω μια κυβική καμπύλη E που δίνεται από μια εξίσωση Weierstrass. Τότε:*

(i) *Η E είναι ελλειπτική καμπύλη (δηλαδή nonsingular) αν και μόνο αν $\Delta \neq 0$.*

(ii) *Η καμπύλη έχει node αν και μόνο εαν $\Delta = 0$ και $c_4 \neq 0$.*

(iii) *Η καμπύλη έχει cusp αν και μόνο εάν $\Delta = 0$ και $c_4 = 0$.*

(iv) *Αν η E έχει singular σημείο, αυτό είναι μοναδικό.*

Απόδειξη. (i), (ii), (iii) Θεωρούμε την E δοσμένη σε μια Weierstrass μορφή της

$$E : f(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

και αντίστοιχα στην ομογενή μορφή της

$$E : F(X, Y, Z) = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3 = 0.$$

Αρχικά θα δείξουμε ότι το επ΄ άπειρον σημείο $O = [0, 1, 0]$ είναι nonsingular. Πράγματι:

$$\frac{\partial F}{\partial Z}(O) \neq 0.$$

Έστω τώρα ένα σημείο $P = (x_0, y_0)$ στο αφφινικό κομμάτι της E, στο οποίο η E έχει singularity. Επειδή η μετατόπιση κατά σημείο αφήνει τις ποσότητες Δ και c_4 αναλλοίωτες, μπορούμε χωρίς βλάβη της γενικότητας να υποθέσουμε ότι $P = (0, 0)$. Τότε, παίρνουμε:

$$f(0, 0) = \frac{\partial f}{\partial x}(0, 0) = \frac{\partial f}{\partial y}(0, 0) = 0$$

δηλαδή

$$a_6 = a_4 = a_3 = 0$$

δηλαδή η μορφή Weierstrass της καμπύλης E γίνεται

$$E : f(x, y) = y^2 + a_1xy - x^3 - a_2x^2 = 0$$

με $c_4 = (a_1^2 + 4a_2)^2$ και $\Delta = 0$. Αν $c_4 = 0$ τότε $a_1^2 + 4a_2 = 0$, άρα η μορφή Weierstrass γίνεται:

$$E : f(x, y) = y^2+a_1xy-a_2x^2-x^3 = y^2+a_1xy+\frac{a_1^2}{4}x^2-x^3 = (y+\frac{a_1}{2}x)^2-x^3 = 0$$

δηλαδή

$$E : (y + \frac{a_1}{2}x)^2 = x^3$$

η οποία με μια μετατόπιση γίνεται

$$E : y^2 = x^3$$

για την οποία ειναι απλό να δει κανείς ότι έχει cusp. Ομοίως διαπιστώνει κανείς ότι αν $c_4 \neq 0$, τότε η E έχει node.

Πρέπει να δείξουμε πως αν η καμπύλη E είναι nonsingular (δηλαδή ελλειπτική) θα έχουμε $\Delta \neq 0$. Υποθέτουμε πως χαρ$(K) \neq 2$ (η περίπτωση για χαρ$(K) = 2$ έχει σαφώς περισσότερες πράξεις, αλλα είναι αντίστοιχη). Παίρνουμε μια μορφή Weierstrass της E:

$$E : y^2 - 4x^3 - b_2x^2 - 2b_4x - b_6 = g(x) = 0$$

Τότε η E έχει singularity σε ένα σημείο $P = (x_0, y_0)$ αν και μόνο αν

$$2y_0 = g'(x_0) = 0.$$

Με άλλα λόγια η E έχει singularity ακριβώς στα σημεία $P = (x_0, 0)$, όπου το x_0 είναι διπλή ρίζα του $g(x)$. Άρα, η E είναι singular αν και μόνο αν το $g(x)$ έχει διακρίνουσα ίση με 0. Όμως η διακρίνουσα του $g(x)$ είναι ίση με 16Δ.

(iv) Παρατηρείστε ότι αν το $g(x)$ έχει διπλή ρίζα, τότε αυτή είναι μοναδική. □

Πρόταση 2.1.7. (i) *Δύο ελλειπτικές καμπύλες E_1, E_2 είναι ισόμορφες υπεράνω του $\bar{K}$ αν και μόνο αν $j(E_1) = j(E_2)$.*

(ii) *Αν $j_0 \in \bar{K}$ τότε υπάρχει ελλειπτική καμπύλη E υπεράνω του $K(j_0)$ με $j(E) = j_0$.*

Απόδειξη. (i) Την μια κατεύθυνση την έχουμε ήδη δει. Υποθέτουμε πως χαρ$(K) \neq 2, 3$, και θεωρούμε δύο καμπύλες E_1, E_2 υπεράνω του K, με $j(E_1) = j(E_2)$. Ας υποθέσουμε πως έχουν εξισώσεις Weierstrass τις:

$$E_i : {y_i}^2 = {x_i}^3 + A_i x_i + B_i$$

για $i = 1, 2$. Αφού $j(E_1) = j(E_2)$ παίρνουμε:

$$\frac{(4A_1)^3}{4A_1^3 + 27B_1^2} = \frac{(4A_2)^3}{4A_2^3 + 27B_2^2} \Longrightarrow {A_1}^3 {B_2}^2 = {A_2}^3 {B_1}^2$$

Για να δείξουμε τον ισχυρισμό μας θα πρέπει να βρούμε έναν ισομορφισμό $(x_1, y_1) = (u^2 x_2, u^3 y_2)$.

Αν $A_1 = 0$, τότε $B_1 \neq 0$ (αφού $\Delta \neq 0$) άρα $A_2 = 0$ και μπορούμε να διαλέξουμε $u = B_1/{B_2}^{1/6}$. Σ′ αυτήν την περίπτωση έχουμε $j = 0$.

Αν $B_1 = 0$, τότε $A_1 \neq 0$, άρα $B_2 = 0$ και διαλέγουμε $u = A_1/{A_2}^{1/4}$. Σ′ αυτήν την περίπτωση έχουμε $j = 1728$.

Αν $A_1 B_1 \neq 0$, τότε $A_2 B_2 \neq 0$ και μπορούμε να πάρουμε σαν u την ποσότητα $A_1/{A_2}^{1/4} = B_1/{B_2}^{1/6}$. Σ′ αυτήν την περίπτωση $j \neq 0, 1728$.

(ii) Αν $j_0 \neq 0, 1728$, τότε μπορούμε να διαλέξουμε σαν καμπύλη που να έχει τις ζητούμενες ιδιότητες την καμπύλη:

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

Αν $j_0 = 0$, τότε μπορούμε να διαλέξουμε την καμπύλη

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

και αν $j_0 = 1728$ διαλέγουμε την

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

Παρατηρείστε ότι η επιλογή των καμπυλών είναι καλή, ανεξαρτήτως την χαρακτηριστικής του σώματος. Αν είμαστε σε σώμα χαρακτηριστικής 2 ή 3 τότε προφανώς οι τελευταίες δύο καμπύλες ταυτίζονται.

□

Πρόταση 2.1.8. *Έστω E μια ελλειπτική καμπύλη, και ω το invariant διαφορικό μιας εξίσωσης της E. Τότε* $\mathrm{div}(\omega) = 0$.

Απόδειξη. Υιοθετούμε τον συμβολισμό $\frac{\partial f}{\partial x} = f_x$, και θεωρούμε μια εξίσωση Weierstrass της E:

$$E : f(x,y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$$

και $P = (x_0, y_0)$ ένα σημείο της E. Τότε το διαφορικό της E ισούται με:

$$\omega = \frac{d(x-x_0)}{f_y(x,y)} = -\frac{d(y-y_0)}{f_x(x,y)}.$$

Αν το P ήταν πόλος του ω θα είχαμε $f_y(x_0,y_0) = 0 = f_x(x_0,y_0)$, δηλαδή το P θα ήταν singular σημείο, το οποίο είναι άτοπο. Αν τώρα θεωρήσουμε την απεικόνιση ϕ:

$$\phi : E \to \mathbb{P}^1 : \phi([x,y,1]) = [x,1]$$

αυτή είναι βαθμού 2, άρα $\mathrm{ord}_P(x-x_0) \leq 2$. Ισότητα έχουμε μόνο στην περίπτωση που το $F(x_0,y)$ έχει διπλή ρίζα. Άρα, παίρνουμε πως είτε $\mathrm{ord}(x-x_0) = 1$, είτε $\mathrm{ord}(x-x_0) = 2$ και $F(x_0,y_0) = 0$. Σε κάθε περίπτωση θα έχουμε πως $\mathrm{ord}_P(\omega) = 0$, δηλαδή το διαφορικό ω δεν έχει ούτε ρίζα στο P.

Για το επ΄ άπερον σημείο O, θεωρούμε έναν uniformizer t στο O, και επειδή $\mathrm{ord}_O(x) = -2$ και $\mathrm{ord}_O(y) = -3$, θα έχουμε $x = t^{-2}f$, $y = t^{-3}g$ για κάποιες f,g: $f(O) \neq 0, \infty \neq g(O)$. Γράφουμε $f' = df/dt$ και υπολογίζουμε ότι

$$\omega = \frac{-2f + tf'}{2g + a_1tf + a_3t^3}dt.$$

Η f' είναι regular στο O. Αν υποθέσουμε, για λόγους απλότητας, πως $\mathrm{χαρ}(K) \neq 2$, τότε η

$$\frac{-2f + tf'}{2g + a_1tf + a_3t^3}dt$$

είναι regular και nonvanishing το O, άρα $\mathrm{ord}_O(\omega) = 0$. Αν $\mathrm{χαρ}(K) = 2$, το αποτέλεσμα έπεται χρησιμοποιώντας τον τύπο $\omega = dy/f_x(x,y)$. □

Πρόταση 2.1.9. *Αν η E που δίνεται από μια εξίσωση Weierstrass είναι singular, τότε υπάρχει ρητή συνάρτηση $\phi : E \to \mathbb{P}^1$ βαθμού 1.*

Απόδειξη. Χωρίς βλάβη της γενικότητας, μπορούμε (κάνοντας αλλαγή μεταβλητών) να υποθέσουμε ότι η E έχει singular σημείο στο $(0,0)$. Παραγωγίζοντας, βλέπουμε ότι η E έχει εξίσωση:

$$E : y^2 + a_1xy = x^3 + a_2x^2.$$

Η ρητή συνάρτηση $\phi : E \to \mathbb{P}^1$ με

$$\phi(x,y) = [x,y]$$

είναι βαθμού 1, αφού έχει αντίστροφη την $f : \mathbb{P}^1 \to E$ με

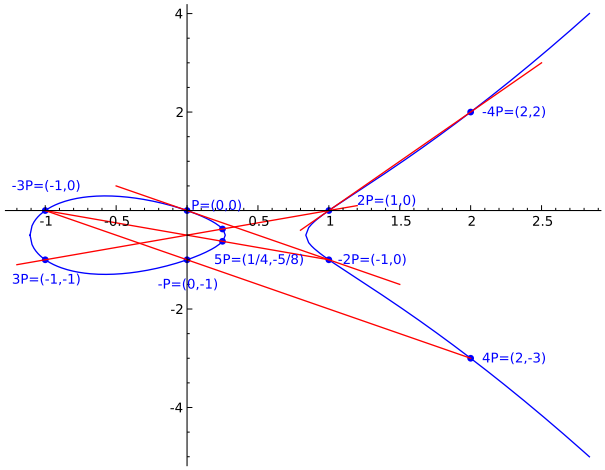
$$f([1,t]) = (t^2 + a_1t - a_2, t^3 + a_1t^2 - a_2t)$$

και η απόδειξη είναι πλήρης. □

2.2 Η ομάδα $E(K)$

Ας υποθέσουμε για λίγο ότι η καμπύλη μας ορίζεται πάνω από το $\mathbb{R}$, δηλαδή έχει μια εξίσωση Weierstrass με συντελεστές από το $\mathbb{R}$. Τότε, η E ως υποσύνολο του $\mathbb{P}^2$ μοιάζει με μια καμπύλη όπως στο σχήμα 2.1, μαζί με ένα επ' άπειρον σημείο $O = [0, 1, 0]$.

Σχήμα 2.1: Ελλειπτική καμπύλη και δυνάμεις σημείου



Προσπαθώντας να εξηγήσουμε την ιδέα που κρύβεται πίσω απ' την θεωρία της αριθμητικής στις ελλειπτικές καμπύλες που σκοπεύουμε να περιγράψουμε, ας θεωρήσουμε για αρχή πως η E έχει ρητούς συντελεστές (ορίζεται δηλαδή πάνω απ' το $\mathbb{Q}$) και πως έχει δύο ρητά σημεια $P, Q \in E$. Τότε, είναι άμεση παρατήρηση πως η ευθεία ℓ που τα ενώνει είναι ρητή (έχει δηλαδή ρητούς συντελεστές). Επίσης, από το Θεώρημα του Bezout ([Silverman-Tate, [32], appendix A]) έχουμε ότι η ℓ τέμνει την E σε ακριβώς 3 σημεία μέσα στο $\mathbb{P}^2$, έστω $S = (x_0, y_0)$ το τρίτο σημείο τομής, και είναι απλό να δει κανείς πως $x_0, y_0 \in \mathbb{Q}$, δηλαδή το S είναι και αυτό ρητό σημείο (αν $P = Q$ τότε προφανώς η αντίστοιχη διαδικασία είναι να θεωρησούμε την εφαπτόμενη ευθεία στο P). Θεωρούμε το συμμετρικό του S ως προς τον άξονα του x, έστω $T = (x_0, -y_0)$. Το σημαντικό γεγονός δίνεται από την επόμενη πρόταση.

Πρόταση 2.2.1. *Η διαδικασία (πράξη) που ορίσαμε παραπάνω $(P, Q) \to T$ δίνει στα ρητά σημεία της E δομή αβελιανής ομάδας.*

Η ιδέα των παραπάνω ορισμών και της διαδικασίας που ακολουθήσαμε μοιάζει κατά κάποιον τρόπο με τις ιδέες της Θεωρίας Galois. Προσπαθούμε να δώσουμε αλγεβρική δομή στο σύνολο των λύσεων μιας εξίσωσης, που είναι γεωμετρικό αντικείμενο, και να εξάγουμε πληροφορίες για την αλγεβρική δομή. Θέλουμε να γενικεύσουμε την παραπάνω διαδικασία στην γενική περίπτωση για τυχόν τέλειο σώμα K. Η διαδικασία που περιγράψαμε, όπως φαίνεται και στο σχήμα, και η παραπάνω «πρόταση» οδηγούν άμεσα στην γενικότερη θεώρηση:

Ορισμός 2.2.2 (της πράξης στην E)**.** *Αν $E \subseteq \mathbb{P}^2(\bar{K})$, η E ορίζεται πάνω από το $\bar{K}$, $O = [0, 1, 0]$ και $P, Q \in E$, ορίζουμε S και T ως εξής: το S να είναι το τρίτο*

σημείο της ευθείας που ενώνει τα P και Q και ανήκει την E, και T να είναι το τρίτο σημείο της ευθείας που ενώνει τα O και S και ανήκει την E. Ορίζουμε την πράξη $P + Q = T$.

Σημείωση: Απαιτείται μια προσοχή στον χειρισμό της πράξης, καθώς εννοείται πως μετράμε και πολλαπλόττητες τομής δύο καμπυλών, άρα μπορεί κάποια από τα παραπάνω σημεία μερικές φορές να ταυτίζονται.

Πρόταση 2.2.3. *Η πράξη $+$ που περιγράψαμε δίνει στα σημεία της καμπύλης δομή αβελιανής ομάδας με ουδέτερο στοιχείο το O. Πιο συγκεκριμμένα:*

(i) *Αν $P, Q, S \in E$ όπως πρίν, τότε $(P + Q) + S = O$*

(ii) *$P + O = P$ για κάθε $P \in E$.*

(iii) *$P + Q = Q + P$*

(iv) *Αν $P \in E$, τότε υπάρχει ένα σημείο της E, που συμβολίζεται με $-P$, τέτοιο ώστε $P + (-P) = O$*

(v) *Αν $P, Q, R \in E$ τρία τυχόντα σημεία της E, τότε $(P+Q)+R = P+(Q+R)$*

(vi) *Αν η E ορίζεται υπεράνω του K, τότε η*

$$E(K) = \{(x, y) \in K^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}$$

είναι υποομάδα της E.

Απόδειξη. (i) Άμεσο, από τον ορισμό της πράξης στην E, και το γεγονός ότι η εφαπτόμενη της E στο O τέμνει την E με πολλαπλότητα 3.

(ii) Παίρνουμε $Q = O$. Τότε, για τις δύο ευθείες που ορίσαμε παραπάνω, βλέπουμε ότι η μία διέρχεται από τα σημεία P, O, S και η άλλη από τα $O, S, P+O$. Αφού έχουν δύο κοινά σημεία ταυτίζονται, άρα ταυτίζονται και τα τρίτα σημεία τους P, $P + O$.

(iii) Άμεσο, επειδή ο τρόπος που ορίστηκε η πράξη είναι ο ίδιος είτε συμμετρικός ως προς την σειρά επιλογής των P και Q.

(iv) Το S του ερωτήματος (ii) έχει την ιδιότητα που επιθυμούμε.

(v) Μπορεί κανείς να το αποδείξει χρησιμοποιώντας τους αναλυτικούς τύπους της πράξης που θα δώσουμε αμέσως μετά. Μια γεωμετρική απόδειξη υπάρχει στο [Silverman-Tate, [32], κεφ.1].

(vi) Αν τα P και Q είναι K-ρητά, τότε και η ευθεία που τα ενώνει είναι K-ρητή (δηλαδή έχει συντελεστές στο K). Αφού η E έχει συντελεστές στο K, και τα δύο από τα τρία σημεία τομής της E με την ευθεία είναι K-ρητά, έπεται ότι και το τρίτο σημείο πρέπει να είναι K-ρητό.

□

Συμβολισμός: Από δω και πέρα, θα καλούμε την πράξη που ορίσαμε πρόσθεση. Γράφουμε $[m]P$ για το $P+P+...+P$ m-φορές, $[m]P$ για το $-P-P-...-P$ αν $m < 0$ και $[0]P = O$. Επίσης, θα γράφουμε $x(P)$ και $y(P)$ για τις x και y συντεταγμένες του σημείου P αντίστοιχα (δηλαδή $P = (x(P), y(P))$.

Μπορεί κανείς να δώσει αναλυτικούς τύπους για την πράξη της ομάδας, χρησιμοποιώντας μόνο τον γεωμετρικό ορισμό της πρόσθεσης στην E. Η απόδειξη των παρακάτω δεν είναι δύσκολη. Για μια απόδειξη τους παραπέμπουμε στο [Silverman, [30], κεφ.3] ή στο [Silverman-Tate, [32], κεφ.1].

Πρόταση 2.2.4 (Τύποι για την πράξη στην $E(K)$)**.** *Έστω μια ελλειπτική καμπύλη E που δίνεται από την εξίσωση Weierstrass:*

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

(i) *Έστω $P = (x_0, y_0)$. Τότε:*

$$-P = (x_0, -y_0 - a_1x_0 - a_3)$$

(ii) *Έστω $P = (x_1, y_1)$, $Q = (x_2, y_2)$, $R = (x_3, y_3)$ και $P+Q = R$. Αν $x_1 = x_2$ και $y_1 + y_2 + a_1x_2 + a_3 = 0$ τότε $P + Q = O$. Αλλιώς, όρισε λ και ν ως ακολούθως:*

(α′) Αν $x_1 \neq x_2$:

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

και

$$\nu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1}$$

(β′) Αν $x_1 = x_2$:

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}$$

και

$$\nu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}$$

(iii) *Με τον συμβολισμό όπως πριν, το $R = P + Q$ έχει συντεταγμένες*

$$(x_3, y_3) = (\lambda^2 + a_1\lambda - a_2 - x_1 - x_2, -(\lambda + a_1)x_3 - \nu - a_3)$$

(iv) *Ειδικότερα, αν $P = Q$ έχουμε ότι ότι το σημείο $[2]P$ έχει συντεταγμένες:*

$$[2]P = (x([2]P), y([2]P))$$

$$= \left(\frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6}, \frac{Y([2]P) - a_1x(2[P]) - a_3}{2}\right)$$

όπου

$$Y(2[P]) = \frac{2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + (b_4b_8 - b_6^2)}{(2y + a_1x + a_3)^3}.$$

Πόρισμα 2.2.5. *Έστω E μια ελλειπτική καμπύλη και έστω μια $f \in \bar{K}(E) = \bar{K}(x, y)$. Η f είναι άρτια ($f(P) = f(-P)$ για κάθε $P \in E$) αν και μόνο αν $f \in \bar{K}(x)$.*

Απόδειξη. Κάθε $f \in \bar{K}(x)$ είναι άρτια, αφού

$$P = (x_0, y_0) \Longrightarrow -P = (x_0, -y_0 - a_1 x_0 - a_3)$$

Αν τώρα μια άρτια $f \in \bar{K}(E)$, τότε, παίρνοντας υπ' όψην μας ότι η εξίσωση Weierstrass της E εκφράζει τις δυνάμεις $y^2, y^3, ...$ συναρτήσει των $y, x, x^2, ...$ γράφουμε την f ως $f(x, y) = g(x) + yh(x)$. Παίρνουμε:

$$f(x, y) = f(x, -y - a_1 x - a_3) \Longrightarrow g(x) + yh(x) = g(x) + (-y - a_1 x - a_3)h(x)$$

$$\Longrightarrow (2y + a_1 x + a_3)h(x) = 0$$

για κάθε $x, y \in E$. Άρα είτε $h(x) \equiv 0$, οπότε και έχουμε το ζητούμενο, είτε $2y + a_1 x + a_3 \equiv 0$ που δίνει $2 = a_1 = a_3 = 0$ που είναι άτοπο, γιατί δίνει singularity στην καμπύλη E. Η απόδειξη είναι πλήρης. □

2.3 Singular Κυβικές Καμπύλες

Θα μελετήσουμε την συμπεριφορά των σημείων μιας singular κυβικής καμπύλης. Θα δούμε ότι η κατανόηση των singular καμπυλών είναι σχετικά απλή, εξίσου απλή με των κωνικών τομών. Θα δούμε επίσης παρακάτω ότι η απλή αυτή περιγραφή θα χαθεί όταν θα περάσουμε στην μελέτη των ελλειπτικών καμπυλών.

Ορισμός 2.3.1. *Αν η E είναι μια singular κυβική καμπύλη με singular σημείο το S, τότε ορίζουμε το nonsingular μέρος της να είναι το $E - S$, και το συμβολίζουμε με E_{ns}. Ομοίως ορίζεται το $E_{\text{ns}}(K)$ στην περίπτωση που E/K.*

Το παρακάτω Θεώρημα μας δίνει την δομή της ομάδας E_{ns}:

Θεώρημα 2.3.2. *Έστω E μια singular κυβική καμπύλη στο $\mathbb{P}^2(\bar{K})$ με singular σημείο S. Τότε, η πράξη που ορίσαμε στην E κάνει την $E_{\text{ns}}(\bar{K})$ αβελιανή ομάδα ως εξής:*

(i) *Έστω ότι η E έχει node. Τότε $c_4 \neq 0$. Έστω:*

$$y = a_1 x + b_1$$

$$y = a_2 x + b_2$$

οι εφαπτόμενες ευθείες της E στο S. Τότε η απεικόνιση:

$$E_{\text{ns}} \to \bar{K}^* : (x, y) \to \frac{y - a_1 x - b_1}{y - a_2 x - b_2}$$

είναι ισομορφισμός αβελιανών ομάδων.

(ii) *Έστω ότι η E έχει cusp. Τότε $c_4 = 0$. Έστω:*

$$y = ax + b$$

η εφαπτόμενη της της E στο S. Τότε η απεικόνιση:

$$E_{\text{ns}} \to \bar{K}^+ : (x, y) \to \frac{x - x(S)}{y - ax - b}$$

είναι ισομορφισμός αβελιανών ομάδων.

Σημείωση: Αντίστοιχη απλή συμπεριφορά υπάρχει και όταν η καμπύλη μας ορίζεται πάνω από ένα αλγεβρικά μη κλειστό σώμα K.

Απόδειξη. Το σύνολο $E_{\rm ns}(\bar{K})$ είναι κλειστό ως προς την πράξη που έχουμε ορίσει. Αυτό μπορεί να το δει κανείς ως εξής: αν πάρουμε μια ευθεία ℓ που τέμνει το $E_{\rm ns}(\bar{K})$ σε δύο σημεία ή σε ένα σημείο με πολλαπλότητα 2, αν διερχόταν και από το S θα το έτεμνε με τάξη τουλάχιστον 2. Τότε η ℓ θα είχε πολλαπλότητα τομής με την E τουλάχιστον 4, κάτι που αντιφάσκει στο Bezout.

Για να δείξουμε τον ισομορφισμό, θα δείξουμε ότι αν τρία σημεία στην $E_{\rm ns}(\bar{K})$ ικανοποιούν την ιδιότητα (i) της πρότασης 2.2.3, τότε και οι εικόνες τους στις $\bar{K}^*$, $\bar{K}^+$ την ικανοποιούν. Τότε, παρατηρώντας ότι οι ιδιότητες (ii)- (v) της ομάδας έπονται ουσιαστικά από την ιδιότητα (i) , παίρνουμε ότι η απεικόνιση είναι ισομορφισμός.

Αφού οι ισομορφισμοί ορίζονται μέσω ευθειών, μπορούμε, όπως και προηγουμένως, να υποθέσουμε πως η E έχει singularity στο $(0,0)$, και εξίσωση

$$E : y^2 + a_1xy = x^3 + a_2x^2.$$

Θεωρούμε μια ρίζα s στο $\bar{K}$ του πολυωνύμου $s^2 + a_1s - a_2 = 0$. Η αντικατάσταση με $y + sx$ του x απλοποιεί την εξίσωση της E

$$E : y^2 + axy - x^3 = 0$$

ή αλλιώς σε ομογενείς συντεταγμένες

$$E : Y^2Z + AXYZ - X^3.$$

Σε αυτήν την μορφή, η E έχει cusp αν και μόνο αν $A = 0$.

(i) $(A \neq 0)$ Οι εφαπτόμενες της E στο $S = [0,0,1]$ είναι οι $Y = 0$, $Y = -AX$, άρα η απεικόνιση της εκφώνησης παίρνει την μορφή:

$$[X, Y, Z] \longrightarrow 1 + \frac{AX}{Y}.$$

Ξαναεφαρμόζουμε αλλαγή μεταβλητών $X = A^2(X' - Y')$, $Y = A^3Y'$, $Z = Z'$, διαιρούμε με A^6 και αποομογενοποιούμε θέτοντας $Y = 1$, καταλήγοντας στην εξίσωση

$$E : xz - (x-1)^3 = 0$$

και την απεικόνιση

$$E_{ns} \to \bar{K}^* : (x, z) \to x.$$

Η απεικόνιση αυτή έχει αντίστροφη, την

$$\bar{K}^* \to E_{ns} : t \to \left(t, \frac{(t-1)^3}{t}\right)$$

έχοντας έτσι κατασκευάσει μια 1-1 και επί απεικόνιση συνόλων.

Έστω τώρα τρία σημεία της E συνευθειακά τέτοια ώστε η ευθεία ℓ που τα ενώνει να μην διέρχεται του $[0,0,1]$. Ας τα ονομάσουμε (x_i, z_i) για $i = 1,2,3$. Η ℓ έχει τύπο $z = ax + b$, άρα τα x_i είναι ρίζες του πολυωνύμου

$$x(ax + b) - (x-1)^3$$

και από τους τύπους του Vieta έπεται ότι $x_1x_2x_3 = 1$, δηλαδή οι εικόνες των σημείων ικανοποιούν την ιδιότητα (i) της πρότασης 2.2.3.

(ii) $(A = 0)$ Θα εφαρμόσουμε την ίδια μέθοδο με το προηγούμενο ερώτημα. Η εφαπτόμενη της E στο $S = [0, 0, 1]$ είναι η $Y = 0$, και η απεικόνιση της εκφώνησης είναι η

$$E_{\text{ns}} \longrightarrow \bar{K}^+$$

με

$$[X, Y, Z] \longrightarrow X/Y.$$

Αποομογενοποιούμε ξανά, και παίρνουμε

$$E : Z - X^3 = 0$$

και η απεικόνιση γίνεται

$$E_{\text{ns}} \to \bar{K}^+ : (x, z) \to x$$

η οποία έχει αντίστροφη

$$\bar{K}^* \to E_{\text{ns}} : t \to (t, t^3).$$

Αν η ευθεία ℓ με εξίσωση $z = ax+b$ τέμνει την E στα (x_i, z_i) για $i = 1, 2, 3$, τότε τα x_i είναι ρίζες του πολυωνύμου

$$ax + b - x^3$$

το οποίο έχει μηδενικό συντελεστή στο x^2, άρα $x_1+x_2+x_3 = 0$. Η απόδειξη είναι πλήρης.

□

2.4 Ύπαρξη μορφής Weierstrass

Μέχρι στιγμής έχουμε μελετήσει κυβικές καμπύλες του $\mathbb{P}^2(\bar{K})$ που υποθέτουμε από πριν πως έχουν μια μορφή Weierstrass. Σκοπός μας λοιπόν σε αυτήν την παράγραφο είναι να δείξουμε πως αυτή η υπόθεση δεν είναι ιδιαιτέρως περιοριστική, μιας και στην πραγματικότητα όλες οι καμπύλες γένους 1 στο $\mathbb{P}^2(\bar{K})$ έχουν μια nonsingular μορφή Weierstrass , κι άρα το να μελετάμε τις τριτοβάθμιες εξισώσεις που έχουν μια τέτοια μορφή είναι ουσιαστικά ισοδύναμο με το να μελετάμε τις τριτοβάθμιες εξισώσεις δύο μεταβλητών. Όπως έχουμε ήδη αναφέρει, στην απόδειξη του επόμενου θεωρήματος κεντρικό ρόλο παίζει το Θεώρημα Riemann-Roch.

Θεώρημα 2.4.1. *Έστω E μια nonsingular καμπύλη γένους 1 στο $\mathbb{P}^2$ που ορίζεται πάνω από το K και υποθέτουμε ότι έχουμε διαλέξει ένα σταθερό σημείο O στην E τέτοιο ώστε $O \in E(K)$. Τότε:*

(i) *Υπάρχουν συναρτήσεις $x, y \in K(E)$ ώστε η*

$$\phi : E \to \mathbb{P}^2 : \phi = [x, y, 1]$$

να δίνει έναν ισομορφισμό της E/K με μια καμπύλη

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

με $a_i \in K$ και η εικόνα του O να είναι το επ΄ άπειρον σημείο $[0, 1, 0]$ του $\mathbb{P}^2$. Οι x και y λέγονται τότε συντεταγμένες Weierstrass για την E.

(ii) *Για κάθε δύο εξισώσεις Weierstrass της E υπάρχει μετασχηματισμός*

$$(X, Y) \to (u^2X' + r, u^3Y' + su^2X' + t)$$

από την μία μορφή στην άλλη, με r, s, t στο K και u στο K^*

(iii) *Κάθε λεία κυβική καμπύλη C με εξίσωση Weierstrass που έχει συντελεστές στο K είναι nonsingular κυβική καμπύλη γένους* 1.

Απόδειξη. (i) Θεωρούμε τους divisors $n(O)$ και τους χώρους $L(n(O))$. Το θεώρημα Riemann-Roch δίνει, για $g = 1$

$$\ell(n(O) = dimL(n(O)) = n$$

για κάθε $n \geq 1$. Από την πρόταση 1.4.6, μπορούμε να διαλέξουμε x, y συναρτήσεις στο $K(E)$ ώστε η $\{1, x\}$ να είναι βάση του $L(2(O))$ και η $\{1, x, y\}$ να είναι βάση του $L(3(O))$. Αυτό σημαίνει πως η x έχει πόλο τάξης 2 στο O και η y έχει πόλο τάξης 3 στο O. Τότε, ο $L(6(O))$ περιέχει τα εφτά στοιχεία $1, x, y, x^2, xy, y^2, x^3$ και έχει διάσταση 6. Αυτό σημαίνει πως υπάρχει μια γραμμική εξάρτηση των στοιχείων του

$$\lambda_1 + \lambda_2 x + \lambda_3 y + \lambda_4 x^2 + \lambda_5 xy + \lambda_6 y^2 + \lambda_7 x^3 = 0$$

όπου λ_i ανήκουν στο K. Επειδή η x έχει πόλο στο O ακριβώς 2 και η y ακριβώς 3. έπεται ότι $\lambda_6\lambda_7 \neq 0$, άρα, αντικαθιστώντας το x με $-\lambda_6\lambda_7 x$, το y με $\lambda_6\lambda_7^2 y$ και διαιρώντας με $\lambda_6^3\lambda_7^4$ παίρνουμε μια μορφή Weierstrass της καμπύλης.

Η διαδικασία αυτή μας επιτρέπει να ορίσουμε μια απεικόνιση

$$\phi : E \longrightarrow \mathbb{P}^2 : \phi(x, y) = [x, y, 1]$$

με εικόνα την C. Η ϕ είναι μορφισμός (πρόταση 1.2.5) που είναι επί (πρόταση 1.2.6), και ικανοποιεί $\phi(O) = [0, 1, 0]$, επειδή η y έχει ανώτερης τάξης πόλο στο O.

Από την πρόταση 1.2.14, η απεικόνιση $[x, 1] : E \to \mathbb{P}^1$ έχει βαθμό 2, άρα $[K(E) : K(x)] = 2$, και όμοια η $[y, 1] : E \to \mathbb{P}^1$ έχει βαθμό 3, άρα $[K(E) : K(y)] = 3$. Έπεται ότι $[K(E) : K(x, y)] = 1$, άρα $K(E) = K(x, y)$, το οποίο μας δίνει ότι η απεικόνιση $\phi : E \to C$ που ορίσαμε είναι βαθμού 1.

Έστω ότι η C δεν είναι λεία. Τότε είναι singular , και από την πρόταση 2.1.9, υπάρχει απεικόνιση $\psi : C \to \mathbb{P}^1$ βαθμού 1. Τότε η σύνθεση $\psi \circ \phi : E \to \mathbb{P}^1$ είναι βαθμού 1, το οποίο είναι άτοπο, αφού το $\mathbb{P}^1$ είναι γένους 0 και η E γένους 1. Άρα η C είναι λεία, και από την πρόταση 1.2.12 οι E, C είναι ισόμορφες.

(ii) Έστω $\{x, y\}$, $\{x', y'\}$ δύο διαφορετικά ζεύγη συναρτήσεων όπως στο (i) για την E. Τότε τα σύνολα $\{1, x\}$, $\{1, x'\}$ είναι και τα δύο βάσεις του $L(2(O))$, όπως και τα $\{1, x, y\}$,$\{1, x', y'\}$ του $L(3(O))$. Άρα υπάρχουν u_1, u_2 μονάδες του K και r, s_2, t στο K τέτοια ώστε

$$x = u_1x' + r$$

$$y = u_2 y' + s_2 x' + t$$

Αφού οι $\{x, y\}$, $\{x', y'\}$ ικανοποιούν εξισώσεις Weierstrass που έχουν μεγιστοβάθμιους συντελεστές 1, παίρνουμε $u_1^3 = u_2^2$. Θέτουμε $u = u_2/u_1$ και $s = s_2/u^2$, και έχουμε το ζητούμενο.

(iii) Έστω λοιπόν πως η E δίνεται από μια εξίσωση Weierstrass. Είδαμε (πρόταση 2.1.8) πως για το ολόμορφο διαφορικό ω_E της E ισχύει $\mathrm{div}(\omega) = 0$, και το Riemann-Roch μας δίνει ότι

$$2g - 2 = \deg(\mathrm{div}(\omega)) = 0$$

άρα $g = 1$. Παίρνουμε σαν O το $[0, 1, 0]$ και έχουμε το ζητούμενο.

□

Χρησιμοποιώντας τώρα το Riemann-Roch, μπορεί κανείς να ορίσει μια δομή ομάδας στην γένους 1 καμπύλη E και να δείξει ότι η ομάδα αυτή ταυτίζεται με την ομάδα $E(K)$ που έχουμε ήδη κατασκευάσει. Η κατασκευή αυτή είναι πολύ χρήσιμη, όμως δεν θα την κάνουμε. Παραπέμπουμε στο [Silverman, [30], κεφ.3] για την κατασκευή αυτήν. Μεταξύ άλλων, η κατασκευή αυτή δίνει μια συντομη απόδειξη του επόμενου λήμματος, το οποίο θα μας χρειαστεί για να ορίσουμε την αντιστοιχεία του Weil. Για μια απόδειξη του βασισμένη στην παραπάνω κατασκευή παραπέμπουμε επίσης στον [Moreno, [25], κεφ. 5].

Λήμμα 2.4.2. *Έστω E μια ελλειπτική καμπύλη και $D = \sum n_P(P) \in \mathrm{Div}(E)$. Τότε ο D είναι πρωταρχικός αν και μόνο αν*

$$\sum_{P \in E} n_P = 0$$

και

$$\sum_{P \in E} [n_P]P = O$$

Το επόμενο αποτέλεσμα είναι θεμελιώδες όσων αφορά την μελέτη των μορφισμών μεταξύ ελλειπτικών καμπυλών

Πρόταση 2.4.3. *Έστω E/K μια ελλειπτική καμπύλη. Τότε οι απεικονίσεις*

$$+ : E \times E \longrightarrow E : (P, Q) \longrightarrow P + Q$$

και

$$- : E \longrightarrow E : P \longrightarrow -P$$

που ορίζονται από τις πράξεις της ομάδας $E(K)$ είναι μορφισμοί.

Απόδειξη. (Σκιαγράφηση) Η απεικόνιση

$$- : E \longrightarrow E : P \longrightarrow -P$$

δίνεται κατά συντεταγμένες ως

$$(x, y) \longrightarrow (x, -y - a_1 - a_3)$$

άρα είναι προφανώς ρητή, και χρησιμοποιώντας την πρόταση 1.2.5 παίρνουμε το ζητούμενο.

Σταθεροποιούμε ένα σημείο Q και δείχνουμε ότι η μεταφορά κατά Q είναι μορφισμός : $E \longrightarrow E$. Από τους τύπους που δίνουν την πράξη στην $E(K)$ βλέπει κανείς ότι είναι κι αυτή ρητή, και είναι μορφισμός με αντίστροφη απεικόνιση την μεταφορά κατά $-Q$.

Τέλος, χρησιμοποιώντας πάλι του τύπους της πρόσθεσης και κάνοντας πράξεις, δείχνει κανείς ότι η πρόσθεση είναι μορφισμός (Μια περισσότερη δουλειά με τους τύπους χρειάζεται όταν έχουμε σημεία της μορφής $(P, P), (P, -P), (O, P), (P, O)$). □

Η σημασία της παραπάνω πρότασης έγκειται στο ότι θα μας επιτρέψει να ορίσουμε αλγεβρική δομη στο σύνολο των μορφισμών από μια καμπύλη E_1 σε μια καμπύλη E_2.

2.5 Ισογενείς Ελλειπτικές Καμπύλες

Ορισμός 2.5.1. *Έστω E_1, E_2 δύο ελλειπτικές καμπύλες. Μια ισογένεια είναι ένας μορφισμός $\phi : E_1 \to E_2$ με $\phi(O) = O$. Δύο καμπύλες λέγονται ισογενείς αν υπάρχει μη τετριμμένη ισογένεια $\phi : E_1 \to E_2$ (δηλαδή αν ισχύει $\phi(E_1) \neq \{O\}$).*

Ξέχουμε, από το πρώτο κεφάλαιο, ότι μία μη τετριμμένη ισογένεια είναι επί.

Παρατήρηση. Έστω E μία ελλειπτική καμπύλη και m ένας ακέραιος αριθμός. Τότε, ο πολλαπλασιασμός με m :

$$[m] : E \to E, P \to [m]P$$

είναι ισογένεια. Αυτό έπεται από την πρόταση 2.4.3 εφαρμόζωντας την διαδοχικά m φορές. Αν $m = 0$ τότε προφανώς η ισογένεια $[0]$ είναι τετριμμένη. Το αντίστροφο, δηλαδή ότι αν ο πολλαπλασιασμός με $[m]$ είναι τετριμμένος τότε $m = 0$, δεν είναι προφανές, είναι όμως σωστό.

Έστω $\phi : E_1 \to E_2$ μια μη τετριμμένη ισογένεια. Από το γεγονός ότι κάθε μη τετριμμένη ισογένεια είναι επί, έπεται ότι έχει πεπερασμένο βαθμό και έχουμε την συνηθισμένη απεικόνιση που ορίσαμε στο πρώτο κεφάλαιο:

$$\phi^* : \bar{K}(E_2) \longrightarrow \bar{K}(E_1)$$

όπου έχουμε ορίσει

$$\deg \phi = \bar{K}(E_1)/\phi^*(\bar{K}(E_2))$$

και, εξ΄ ορισμού, θέτουμε

$$\deg[0] = 0.$$

Παρατηρούμε ότι από τα παραπάνω παίρνουμε την πολλαπλασιαστικότητα της σύνθεσης. Δηλαδή, αν έχουμε μορφισμούς

$$\phi : E_1 \to E_2, \psi : E_2 \to E_3$$

τότε ισχύει

$$\deg(\psi \circ \phi) = (\deg \psi)(\deg \phi)$$

Αν τώρα έχουμε $\phi : E_1 \to E_2$ και $\psi : E_1 \to E_2$ δύο ισογένειες μεταξύ δύο καμπυλών, το κατά σημείο άθροισμα τους $\phi + \psi$ είναι επίσης ισογένεια. Έχουμε έτσι δείξει την εξής πρόταση:

Πρόταση 2.5.2. *Έστω E_1, E_2 δύο ελλειπτικές καμπύλες. Το σύνολο των ισογενειών*

$$\mathrm{Hom}(E_1, E_2) = \{\phi : E_1 \to E_2\}$$

είναι αβελιανή ομάδα.

Ορισμός 2.5.3. *Ορίζουμε τον δακτύλιο* $\mathrm{End}(E) = \mathrm{Hom}(E, E)$*, με πρόσθεση αυτήν που ορίσαμε παραπάνω και πολλαπλασιασμό την σύνθεση των μορφισμών $E \to E$, και τον ονομάζουμε δακτύλιο ενδομορφισμών της E. Η ομάδα αυτομορφισμών* $\mathrm{Aut}(E)$ *της E ορίζεται να είναι τα αντιστρέψιμα στοιχεία του:*

$$\mathrm{Aut}(E) = (\mathrm{End}(E))^*$$

Αν οι καμπύλες μας ορίζονται υπεράνω του K, μπορουμε βέβαια να μελετάμε τα στοιχεία των παραπάνω δομών που ορίζονται υπεράνω του K. Παρατηρούμε, παραδείγματος χάριν, πως όταν E/K, τότε ο μορφισμός $[m]$ οριζεται υπεράνω του K (η ομάδα $E(K)$ είναι κλειστή ως προς την πράξη της).

Θεώρημα 2.5.4. (i) *Έστω E/K μια ελλειπτική καμπύλη και $m \in \mathbb{Z}$ με $m \neq 0$. Τότε ο πολλαπλασιασμός με m είναι μη σταθερή ισογένεια.*

(ii) *Έστω E_1, E_2 δύο ελλειπτικές καμπύλες. Τότε η ομάδα των ισογενειών*

$$\mathrm{Hom}(E_1, E_2)$$

είναι ελεύθερο $\mathbb{Z}$-πρότυπο.

(iii) *Έστω E/K μια ελλειπτική καμπύλη. Τότε ο* $\mathrm{End}(E)$ *είναι ακέραια περιοχή χαρακτηριστικής* 0.

Απόδειξη. (i) Για λόγους απλότητας υποθέτουμε πως $\mathrm{χαρ}(K) \neq 2$. Θα δείξουμε ότι υπάρχουν πεπερασμένα σημεία στον $\ker[m]$.

Έστω P ένα σημείο τάξης 2. Χρησιμοποιώντας τον τύπο για τις συντεταγμένες του $[2]P$, βλέπουμε ότι αν το P έχει τάξη 2 τότε η $x([P])$ είναι ρίζα του τριτοβάθμιου πολυωνύμου $4x^3 + b_2x^2 + 2b_4x + b_6$, το οποίο έχει πεπερασμένες ρίζες. Άρα ο $\ker[2]$ είναι πεπερασμένος.

Έστω τώρα ένας περιττός m. Το πολυώνυμο $f(x) = 4x^3 + b_2x^2 + 2b_4x + b_6$ δεν διαιρεί το $g(x) = x^4 - b_4x^2 - 2b_6x - b_8$, γιατί αν το διαιρούσε θα παίρναμε $\Delta = 0$. Άρα, υπάρχει x_0 στο $\bar{K}$ ώστε το f να έχει ρίζα μεγαλύτερης τάξης στο x_0 από το g. Διαλέγουμε ένα y_0 στο $\bar{K}$ ώστε το $P_0 = (x_0, y_0)$. Απ' τον τρόπο που επιλέξαμε το x_0 και τον τύπο για το $x([2]P)$ παίρνουμε ότι $x([2]P_0) = \infty$, άρα $[2]P_0 = O$. Κατασκευάσαμε έτσι ένα σημείο τάξης 2, άρα το P_0 δεν ανήκει στον $\ker[m]$ για κανένα περιττό m. Έπεται ότι η ισογένεια δεν είναι τετριμμένη, άρα είναι πεπερασμένη. Για την γενική περίπτωση, χρησιμοποίουμε την σχέση $[mn] = [m] \circ [n]$.

Αν $\mathrm{χαρ}(K) = 2$, δείχνουμε ότι το να είναι ο $[2]$ τετριμμένη ισογένεια συνεπάγεται $\Delta = 0$, το οποίο είναι άτοπο. Για τους περιττούς m, μπορεί να αποδειχθεί με χρήση του τύπου για τα $x([3]P)$, $y([3]P)$.

(ii) Έστω $\phi \in \mathrm{Hom}(E_1, E_2)$ και ένας ακέραιος m με $[m] \circ \phi = [0]$. Αφού

$$(\deg[m])(\deg \phi) = 0$$

συμπεραίνουμε πως είτε $m = 0$ είτε $\deg[m] \geq 1$, οπότε και θα έχουμε $\phi \equiv [0]$.

(iii) Από το προηγούμενο ερώτημα παίρνουμ ότι ο $\mathrm{End}(E)$ είναι χαρακτηριστικής 0. Έστω δύο μηδενοδιαιρέτες του ϕ, ψ. Τότε

$$\phi \circ \psi = [0] \Longrightarrow (\deg \phi)(\deg \psi) = \deg(\phi \circ \psi) = 0$$

άρα ένας εκ των μορφισμών ϕ, ψ είναι τετριμμένος.

□

Ορισμός 2.5.5. *Έστω E μια ελλειπτική καμπύλη και m ένας φυσικός αριθμός. Η m-υποομάδα στρέψης της E αποτελείται από τα σημεία της E τάξης m (δηλαδή είναι ο $\ker[m]$), και συμβολίζεται με $E[m]$. Η ένωση τους*

$$E_{\mathrm{tors}} = \bigcup_{m \in \mathbb{N}} E[m]$$

είναι η υποομάδα στρέψης της E (torsion subgroup). Τα στοιχεία της E_{tors}, δηλαδή τα σημεία πεπερασμένης τάξης, λέγονται και torsion σημεία της E. Αν E/K, τότε τα torsion σημεία της $E(K)$ θα συμβολίζονται με $E_{\mathrm{tors}}(K)$.

Την επόμενη πρόταση μπορεί κανείς να την αποδείξει κάνοντας αρκετές πράξεις. Μια απόδειξη θα δοθεί παρακάτω.

Πρόταση 2.5.6. *Ο μορφισμός $[m]$ έχει βαθμό $\deg[m] = m^2$.*

Έστω E μια ελλειπτική καμπύλη που ορίζεται πάνω από ένα σώμα K με $\mathrm{χαρ}(K) = 0$. Τότε βέβαια, παίρνουμε έναν μονομομορφισμό δακτυλίων:

$$\phi : \mathbb{Z} \to \mathrm{End}(E), \phi(m) = [m]$$

Είναι ένα φυσιολογικό ερώτημα να ρωτήσουμε ποιός μπορεί να είναι ο $\mathrm{End}(E)$. Η απάντηση είναι πως τις περισσότερες φορές ο $\mathrm{End}(E)$ είναι ακριβώς ο $\mathbb{Z}$, δηλαδή οι πολλαπλασιασμοί επί m που μας δίνει η πράξη της ομάδας εξαντλούν τις ισογένιες της καμπύλης στον εαυτό της. Υπάρχουν και εξαιρέσεις:

Ορισμός 2.5.7. *Έστω E μια ελλειπτική καμπύλη που ορίζεται πάνω από ένα σώμα K με $\mathrm{χαρ}(K) = 0$. Αν ο $\mathrm{End}(E)$ περιέχει ισογένεια που δεν είναι της μορφής $[m]$ για κάποιον ακέραιο m, τότε λέμε ότι η E έχει την ιδιότητα του μιγαδικού πολλαπλασιασμού (complex multiplication ή εν συντομία CM).*

Οι ελλειπτικές καμπύλες με μιγαδικό πολλαπλασιασμό έχουν πολλές ιδιότητες. Θα ασχοληθούμε περισσότερο ενδελεχώς με αυτές σε επόμενη παράγραφο, αφότου δούμε την δομή της $E(\mathbb{C})$.

Έστω $K = \mathbb{F}_q$ ένα πεπερασμένο σώμα με $\mathrm{χαρ}(K) = p$ και $q = p^n$ στοιχεία. Θεωρούμε μια ελλειπτική καμπύλη $E/\mathbb{F}_q$ με δοσμένη μορφή Weierstrass, και την απεικόνιση του Frobenius:

$$\phi_q : E \to E^{(q)}, \phi_q(x, y) = (x^q, y^q)$$

όπου η $E^{(q)}/\mathbb{F}_q$ έχει μορφή Weierstrass την μορφή της E με τους συντελεστές όλους υψωμένους εις την q. Αυτό το παράδειγμα, όπως έχουμε ξαναναφέρει, θα αποδειχτεί εξαιρετικά σημαντικό στην μελέτη της της $E/\mathbb{F}_q$.

Παρατηρούμε ότι η ϕ_q είναι η ταυτοτική απεικόνιση, δηλαδή $E = E^{(q)}$. Ο ενδομορφισμός ϕ_q λέγεται ενδομορφισμός του Frobenius, και τα σταθερά του σημεία είναι ακριβώς η $E/\mathbb{F}_q$.

Το επόμενο αποτέλεσμα μας λέει ότι οι ισογένιες είναι καλές, από αλγεβρικής σκοπιάς, απεικονίσεις.

Πρόταση 2.5.8. *Έστω $\phi : E_1 \to E_2$ μια ισογένεια. Τότε η ϕ είναι ομομορφισμός ομάδων.*

Πόρισμα 2.5.9. *Ο πυρήνας μιας μη τετριμμένης ισογένειας είναι πεπερασμένη ομάδα.*

Απόδειξη. Από την προηγούμενη πρόταση, είναι ομάδα. Το ότι είναι πεπερασμένη, έπεται από την πρόταση 1.2.14, αφού η ταξη της ομάδας ειναι το μικρότερη ή ίση από τον βαθμό της ισογένειας. □

Πρόταση 2.5.10. *Έστω $\phi : E_1 \to E_2$ μια μη τετριμμένη διαχωρίσιμη ισογένεια. Τότε η ϕ είναι αδιακλάδιστη, $|\ker\phi| = \deg\phi$ και η επέκταση*

$$\bar{K}(E_1)/\phi^*(\bar{K}(E_2))$$

είναι Galois.

Απόδειξη. (Σκιαγράφηση) Αφού η ϕ είναι διαχωρίσιμη, έχουμε

$$|\phi^{-1}(Q)| = \deg\phi$$

για κάθε σημείο Q της E, και για $Q = O$ έχουμε το ζητούμενο. Επίσης, ισχύει ότι αν συμβολίσουμε με τ_Q την απεικόνιση της μεταφοράς κατά Q στην E (δηλαδή $\tau_Q(P) = P + Q$), τότε η απεικόνιση:

$$\psi : \ker\phi \to Aut(\bar{K}(E_1)/\phi^*(\bar{K}(E_2))) : Q \to \tau_Q^*$$

είναι ισομορφισμός, άρα

$$|\mathrm{Aut}(\bar{K}(E_1)/\phi^*(\bar{K}(E_2)))| = |\ker\phi| = |\deg\phi| = [\bar{K}(E_1) : \phi^*(\bar{K}(E_2))]$$

δηλαδή η επέκταση είναι Galois. □

Έχουμε ορίσει το διαφορικό

$$\omega_E = \omega = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y} \in \Omega_E$$

το οποίο είπαμε πως ονομάζουμε invariant διαφορικό της καμπύλης E. Μέχρι στιγμής δεν έχει γίνει σαφές γιατί να το ονομάσουμε invariant , και οι ακόλουθες δύο προτάσεις, τις οποίες απλά επικαλούμαστε χωρίς αποδείξεις, δικαιολογούν την ονομασία αυτήν, δείχνοντας ότι το ω_E συμπεριφέρεται με καλό τρόπο ως προς την δομή της E.

Πρόταση 2.5.11. *Έστω E/K μια ελλειπτική καμπύλη, ω το ολόμορφο διαφορικό της (για κάποια εξίσωση Weierstrass της καμπύλης) και P ένα σημείο της E. Τότε*

$$\tau_P^*(\omega) = \omega$$

όπου τ_P η συνάρτηση μεταφοράς που ορίσαμε πιο πάνω

$$\tau_P(Q) = Q + P$$

Πρόταση 2.5.12. *Έστω E_1 και E_2 δύο ελλειπτικές καμπύλες και ϕ, ψ δύο ισογένειες από την E_1 στην E_2. Τότε:*

$$(\phi + \psi)^*(\omega_{E_2}) = \phi^*(\omega_{E_2}) + \psi^*(\omega_{E_2})$$

όπου η πρώτη πράξη είναι πρόσθεση στον δακτύλιο $\mathrm{Hom}(E_1, E_2)$ *και η δεύτερη είναι η πρόσθεση στον χώρο των διαφορικών Ω_{E_2}.*

Πόρισμα 2.5.13. *Έστω $E/\mathbb{F}_q$ μια ελλειπτική καμπύλη που ορίζεται πάνω από ένα πεπερασμένο σώμα με q στοιχεία, $q = p^n$, $\phi_q = \phi$ η απεικόνιση του Frobenius από την καμπύλη στον εαυτό της και m,n δύο ακέραιοι. Τότε η απεικόνιση $m + n\phi$ είναι διαχωρίσιμη αν και μόνο αν ο p δεν διαιρεί τον m.*

Απόδειξη. Έστω ω_E το αναλλοίωτο διαφορικό της E. Ξέρουμε ότι μια απεικόνιση ψ από την καμπύλη E στον εαυτό της είναι διαχωρίσιμη αν και μόνο αν η δυική της

$$\psi^* : \Omega_E \to \Omega_E$$

δεν είναι εκ ταυτότητος μηδεν. Τώρα, χρησιμοποιώντας την προηγούμενη πρόταση και το γεγονός ότι $[m]^*(\omega) = m\omega$ έχουμε:

$$[m + n\phi]^*(\omega) = [m]^*(\omega) + [n]^* \circ \phi^*(\omega) = m\omega + n\phi^*(\omega)$$

και αφού η ϕ δεν είναι διαχωρίσιμη θα έχουμε $\phi^*(\omega) = 0$, καταλήγουμε στην σχέση

$$[m + n\phi]^*(\omega) = m\omega$$

το οποίο δεν είναι ταυτοτικά μηδεν αν και μόνο αν ο p δεν διαιρεί τον m. □

Ειδικότερα παρατηρούμε πως ο $1 - \phi$ είναι διαχωρίσιμος, άρα, από την πρόταση 2.5.10, παίρνουμε την σχέση:

$$|\ker(1 - \phi)| = \deg(1 - \phi)$$

Πόρισμα 2.5.14. *Αν E/K και $\chi\alpha\rho(K) = 0$, τότε ο* $\mathrm{End}(E)$ *είναι μεταθετικός δακτύλιος.*

Απόδειξη. Ορίζουμε απεικόνιση

$$\mathrm{End}(E) \to \bar{K}, \phi \to a_\phi$$

όπου $\phi^*(\omega) = a_\phi \omega$. Η απεικόνιση αυτή είναι ομομορφισμός δακτυλίων, και ο πυρήνας της αποτελείται από όλους τους μη διαχωρίσιμους ενδομορφισμούς της E. Όμως, όταν $\chi\alpha\rho(K) = 0$ τότε κάθε ενδομορφισμός είναι διαχωρίσιμος. Άρα η απεικόνιση που ορίσαμε έχει τετριμμένο πυρήνα και μας δίνει μια εμφύτευση του $\mathrm{End}(E)$ στο $\bar{K}$. □

Οι ισογένειες είναι οι πιο σημαντικές απεικονίσεις μεταξύ ελλειπτικών καμπυλών. Η δυική μιας ισογένειας είναι συχνά εξίσου σημαντική απεικόνιση.

Πρόταση 2.5.15. *Έστω $\phi : E_1 \to E_2$ μια μη τετριμμένη ισογένεια βαθμού m. Τότε υπάρχει μοναδική ισογένεια*

$$\hat{\phi} : E_2 \longrightarrow E_1$$

τέτοια ώστε $\hat{\phi} \circ \phi = [m]$. Η $\hat{\phi}$ ονομάζεται δυική ισογένεια της ϕ.

Απόδειξη. (Σκιαγράφηση) Η μοναδικότητα έπεται απλά καθώς $(\hat{\phi} - \hat{\phi}') \circ \phi = [0]$, και αφού η ϕ δεν είναι σταθερή, τότε η $\hat{\phi} - \hat{\phi}'$ θα πρέπει να είναι σταθερή. Αφού η διαφορά τους μηδενίζεται σε ένα σημείο, μηδενίζεται παντού, δηλαδή οι $\hat{\phi}$ και $\hat{\phi}'$ ταυτίζονται παντού.

Για την ύπαρξη η απόδειξη είναι πιο περίπλοκη, και μπορεί να δείξει κανείς ότι απόδειξη σπάει ουσιαστικά σε δύο περιπτώσεις: για ϕ να είναι διαχωρίσιμη και για ϕ να είναι ο μορφισμός του Frobenius. Για τις λεπτομέρειες της απόδειξης παραέμπουμε στο [Silverman, [30], κεφ.3]. □

Παρατηρήστε ότι έχουμε ορίσει την $\hat{\phi}$ για μη τετριμμένες ισογένειες. Ορίζουμε την δυική ισογένεια της $[0]$ να είναι η $[0]$. Οι πολλές και χρήσιμες ιδιότητες της δυικής ισογένειας συνοψίζονται ουσιαστικά στην ακόλουθη πρόταση:

Πρόταση 2.5.16. *Έστω $\phi : E_1 \to E_2$ μια ισογένεια. Τότε ισχύουν:*

(i) *Αν $m = \deg \phi$ τότε*

$$\phi \circ \hat{\phi} = [m]$$

στην E_2.

(ii) *Αν $\psi_1 : E_2 \to E_3$ και $\psi_2 : E_1 \to E_2$ είναι ισογένειες, τότε*

$$\widehat{\psi_1 \circ \phi} = \hat{\phi} \circ \hat{\psi_1}$$

και

$$\widehat{\phi + \psi_2} = \hat{\phi} + \hat{\psi_2}$$

(iii) $\hat{[m]} = [m]$ *και* $\deg[m] = m^2$

(iv) $\deg \phi = \deg \hat{\phi}$ *και* $\hat{\hat{\phi}} = \phi$

Απόδειξη. Αν η ϕ είναι η μηδενική ισογένεια, τότε είναι όλα προφανή. Υποθέτουμε πως η ϕ είναι μη μηδενική.

(i)

$$(\phi \circ \hat{\phi}) \circ \phi = \phi \circ (\hat{\phi} \circ \phi) = \phi \circ [m] = [m] \circ \phi$$

και αφού η ϕ δεν είναι η τετριμμένη ισογένεια, έπεται το ζητούμενο.

(ii) Θέτουμε $n = \deg \psi_1$ και έχουμε

$$(\hat{\phi} \circ \hat{\psi_1}) \circ (\psi_1 \circ \phi) = \hat{\phi} \circ [n] \circ \phi = [n] \circ \hat{\phi} \circ \phi = [nm]$$

και

$$(\widehat{\psi_1 \circ \phi}) \circ (\psi_1 \circ \phi) = \deg[\psi_1 \circ \phi] = [nm]$$

και το συμπέρασμα έπεται από την μοναδικότητα της δυικής. Για το δεύτερο σκέλος, δες [Silverman, [30], κεφ.3].

(iii) Για $m = 1$ αληθεύει. Προχωράμε με επαγωγή. Έστω ότι ισχύει για ένα m σταθερό. Από το ερώτημα β) έχουμε

$$\widehat{[m+1]} = \hat{[m]} + \hat{[1]} = [m] + [1] = [m+1]$$

και ο πρώτος ισχυρισμός έπεται. Επίσης:

$$[\deg[m]] = [\hat{m}] \circ [m] = [m] \circ [m] = [m^2]$$

και αφού ο $\mathrm{End}(E)$ είναι ελεύθερο στρέψης $\mathbb{Z}$-πρότυπο, έχουμε ότι $\deg[m] = m^2$.

(iv) Αν $m = \deg \phi$, τότε

$$m^2 = \deg[m] = \deg(\phi \circ \hat{\phi}) = (\deg \phi)(\deg \hat{\phi}) = m(\deg \hat{\phi})$$

άρα $(\deg \hat{\phi}) = m = \deg \phi$. Για τον άλλον ισχυρισμό:

$$\hat{\phi} \circ \phi = [m] = [\hat{m}] = \widehat{\hat{\phi} \circ \phi} = \hat{\phi} \circ \hat{\hat{\phi}}$$

που δίνει $\phi = \hat{\hat{\phi}}$. □

□

Ορισμός 2.5.17. *Μια απεικόνιση $d : A \to \mathbb{R}$ από μια αβελιανή ομάδα A στους πραγματικούς αριθμούς που για κάθε a στοιχείο της A ικανοποιεί $d(a) = d(-a)$ και η αντιστοιχία $A \times A \to \mathbb{R}$ με*

$$(a, b) \longrightarrow d(a + b) - d(a) - d(b)$$

είναι διγραμμική λέγεται τετραγωνική μορφή πάνω στην ομάδα A. Αν η d παίρνει τιμές στο $\mathbb{R}_+$ και παίρνει την τιμή 0 μόνο στο $0 \in A$, τότε λέγεται θετικά ορισμένη.

Πόρισμα 2.5.18. *Η $\deg \phi : \mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$ είναι θετικά ορισμένη τετραγωνική μορφή.*

Απόδειξη. Θα δείξουμε την διγραμμικότητα της παράστασης $\deg(\phi+\psi)-\deg(\phi)-\deg(\psi)$. Συμβολίζουμε την ποσότητα αυτήν με $\langle \phi, \psi \rangle$ και έχουμε

$$[\langle \phi, \psi \rangle] = [\deg(\phi + \psi)] - [\deg(\phi)] - [\deg(\psi)]$$

το οποίο με χρήση της πρότασης 2.5.16 αποδεικνύεται πως ισούται με $\hat{\phi} \circ \psi + \hat{\psi} \circ \phi$. Η έκφραση αυτή είναι διγραμμική, άρα και η $\langle \phi, \psi \rangle$. Οι υπόλοιπες ιδιότητες είναι άμεσες. □

Μέχρι στιγμής έχουμε μελετήσει την ομάδα $E(K)$, καθώς και γεωμετρικές ιδιότητες της καμπύλης. Μια ιδέα για την περαιτέρω μελέτη είναι να μελετήσουμε σε περισσότερο βάθος αυτήν καθ' εαυτήν την δομή της ομάδας.

2.6 Σημεία στρέψης: Το πρότυπο του Tate και η αντιστοιχία του Weil

Μπορούμε τώρα να βρούμε την δομή της $E[m]$ για μια E που ορίζεται πάνω από ένα αλγεβρικά κλειστό σώμα K:

Θεώρημα 2.6.1. *Έστω E μια ελλειπτική καμπύλη, και m ένας μη μηδενικός ακέραιος αριθμός. Τότε:*

(i) *Αν* $\chi\alpha\rho(K) = 0$ *ή αν* $\chi\alpha\rho(K) = p$ *και* $(\chi\alpha\rho(K), m) = 1$, *τότε*

$$E[m] \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}$$

(ii) *Αν* $\chi\alpha\rho(K) = p$, *τότε η υποομάδα* $E[p^n]$ *είναι είτε τετριμμένη για κάθε* $n \geq 1$, *είτε για κάθε* $n \geq 1$ *ισχύει:*

$$E[p^n] \cong \frac{\mathbb{Z}}{p^n\mathbb{Z}}$$

Απόδειξη. (i) Απ΄ την υπόθεση, και αφού $\deg[m] = m^2$, έπεται ότι ο $[m]$ είναι πεπερασμένη διαχωρίσιμη απεικόνιση. Άρα, από την πρόταση 2.4.10, έπεται ότι

$$|E[m]| = m^2$$

και προφανώς, για τον ίδιο λόγο, για κάθε διαιρέτη d του m έχουμε

$$|E[d]| = d^2.$$

Άρα η $E[m]$ είναι αβελιανή ομάδα τάξης m^2 και για κάθε διαιρέτη d του m η υποομάδα $E[d]$ της $E[m]$ έχει τάξη d^2. Άρα

$$E[m] \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}$$

(ii) Θεωρούμε τον Frobenius ϕ_p. Τότε:

Περίπτωση 1: Ο $\hat{\phi_p}$ είναι μη διαχωρίσιμος. Σ΄ αυτήν την περίπτωση έχουμε:

$$|E[p^n]| = 1$$

για κάθε $n \in \mathbb{N}$.

Περίπτωση 2: Ο $\hat{\phi_p}$ είναι διαχωρίσιμος. Σ΄ αυτήν την περίπτωση έχουμε:

$$|E[p^n]| = p^n$$

για κάθε $n \in \mathbb{N}$. Όπως και πιο πάνω, συμπεραίνουμε πως:

$$E[p^n] \cong \frac{\mathbb{Z}}{p^n\mathbb{Z}}$$

Η απόδειξη είναι πλήρης.

□

Ορίζουμε τώρα το πρότυπο του Tate , το οποίο θα αποδειχτεί εξαιρετικά χρήσιμο στην μελέτη των ελλειπτικών καμπυλών που ορίζονται πάνω από πεπερασμένα σώματα.

Ορισμός 2.6.2. *Έστω* E/K *μια ελλειπτική καμπύλη, και* ℓ *ένας πρώτος αριθμός. Θεωρούμε το αντίστροφο όριο των* ℓ^n-*torsion ομάδων:*

$$T_\ell(E) = \varprojlim E[\ell^n]$$

όπου το αντίστροφο όριο είναι ως προς τους εγκλεισμούς της $E[\ell^{n+1}] \longrightarrow E[\ell^n]$. *Το* $T_\ell(E)$ *ονομάζεται το* ℓ*-αδικό πρότυπο του Tate.*

Το $E[\ell^n]$ είναι $\mathbb{Z}/\ell^n\mathbb{Z}-$πρότυπο, άρα το πρότυπο του Tate γίνεται φυσιολογικά $\mathbb{Z}_\ell-$πρότυπο. Το παρακάτω πόρισμα είναι άμεσο χρησιμοποιώντας το θεώρημα 2.6.1.

Πρόταση 2.6.3. (i) *Έστω $\ell \neq$ χαρ$(K)= p$. Τότε το $\mathbb{Z}_\ell-$πρότυπο του Tate είναι ισόμορφο με $\mathbb{Z}_\ell \times \mathbb{Z}_\ell$*

(ii) *Αν $\ell = p$ τότε $T_\ell(E) \cong 0$ ή $T_\ell(E) \cong \mathbb{Z}_\ell$*

Απόδειξη. Είναι και τα δύο άμεσα, γιατί στην πρώτη περίπτωση παίρνουμε το αντίστροφο όριο της

$$E[\ell^n] \cong \frac{\mathbb{Z}}{\ell^n\mathbb{Z}} \times \frac{\mathbb{Z}}{\ell^n\mathbb{Z}}$$

και στην δέυτερη περίπτωση παίρνουμε το αντίστροφο όριο ή της τετριμμένης ή της

$$E[p^n] \cong \frac{\mathbb{Z}}{p^n\mathbb{Z}},$$

όπου έχουμε χρησιμοποιήσει βέβαια το γεγονός ότι το αντίστροφο όριο των κυκλικών ομάδων τάξης p^n μας δίνει του p-αδικούς ακέραιους $\mathbb{Z}_p$. □

Δεν είναι στην πρόθεση μας να ασχοληθούμε σε αυτό το σημείο εκτενέστερα με το ℓ-αδικό πρότυπο του Tate. Για λόγους πληρότητας, αναφέρουμε πως μπορεί κανείς να μελετήσει την ℓ-αδική αναπαράσταση

$$\rho_\ell : Gal(\bar{K}/k) \longrightarrow Aut(T_\ell(E)$$

και να χρησιμοποιήσει συνομολογιακά εργαλεία για να αναπτύξει περισσότερο την θεωρία. Με αυτά τα εργαλεία δείχνει λόγου χάρη κανείς πως η τάξη του $Hom(E_1, E_2)$ ως $\mathbb{Z}$-πρότυπο είναι το πολύ 4. Θα επανέλθουμε στο πρότυπο του Tate αμέσως μετά την μελέτη της αντιστοιχίας Weil.

Θεωρούμε λοιπόν μια ελλειπτική καμπύλη E ορισμένη πάνω από ένα σώμα K και έναν ακέραιο $m > 1$ τον οποίον εν προκειμένω τον επιλέγουμε να είναι σχετικά πρώτος προς την χαρακτηριστική p του σώματος για να μην έχουμε πρόβλημα με την δομή της $E[m]$, επειδή ξέρουμε ότι σ΄ αυτήν την περίπτωση έχουμε ισομορφισμό ομάδων

$$E[m] \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}},$$

και θεωρούμε ένα στοιχείο Q της $E[m]$. Τώρα, ο divisor

$$D = m(Q) - m(O)$$

είναι πρωταρχικός, γιατί το Q έχει τάξη m, οπότε μπορούμε να εφαρμόσουμε το λήμμα 2.4.2. Διαλέγουμε μια f τέτοια ώστε $\mathrm{div}(f) = D$, και μια m-οστή ρίζα T του Q. Τώρα ο divisor

$$D' = \sum_{R \in E[m]} (T + R) - (R)$$

είναι κι αυτός πρωταρχικός, οποότε μπορούμε να διαλέξουμε μια συνάρτηση g ώστε $\mathrm{div}(g) = D'$. Τώρα, πολλαπλασιάζοντας ίσως με μια σταθερά αν χρειαστεί, παίρνουμε την ισότητα

$$g^m = f \circ [m]$$

Αν P είναι τώρα ένα στοιχείο της $E[m]$, όπου μπορεί να έχουμε $P = Q$, για κάθε X στην E έχουμε

$$g(X+P)^m = f([m]X + [m]P) = f([m]X) = g(X)^m$$

άρα

$$\left(\frac{g(X+P)}{g(X)}\right)^m = 1$$

κι άρα, επειδή η συνεχής συνάρτηση

$$h(X) = \frac{g(X+P)}{g(X)}$$

παίρνει πεπερασμένες τιμές, θα πρέπει να είναι αναγκαστικά σταθερή στο $E[m]$. Αυτή η παρατήρηση μας δίνει τώρα την δυνατότητα να ορίσουμε την αντιστοιχία του Weil:

Ορισμός 2.6.4. *Η m-αντιστοιχία (ή e_m-αντιστοιχία) του Weil είναι η απεικόνιση*

$$e_m : E[m] \times E[m] \longrightarrow \mu_m : e_m(P,Q) = \frac{g(X+P)}{g(X)}$$

όπου Q, P όπως ορίστηκαν παραπάνω και μ_m είναι οι m-οστές ρίζες της μονάδας.

Οι πιο χρήσιμες ιδιότητες της m-αντιστοιχίας του Weil συνοψίζονται στην ακόλουθη πρόταση:

Πρόταση 2.6.5. *Η αντιστοιχία Weil έχει τις ιδιότητες:*

(i)
$$e_m(P+P',Q) = e_m(P,Q)e_m(P',Q)$$
και
$$e_m(P,Q+Q') = e_m(P,Q)e_m(P,Q')$$

(ii)
$$e_m(P,P) = 1$$

(iii) *Αν*
$$e_m(P,Q) = 1$$
για κάθε $P \in E[m]$ τότε $Q = O$.

(iv)
$$e_m(P,Q) = e_m(P^\sigma, Q^\sigma)$$
για κάθε $\sigma \in \mathrm{Gal}(\bar{K}, K)$.

(v)
$$e_{mn}(P,Q) = e_m([n]P, Q)$$
για κάθε $P \in E[mn]$, για κάθε $Q \in E[m]$.

Πρόταση 2.6.6. *Έστω $\phi : E_1 \to E_2$ μια ισογένεια ελλειπτικών καμπυλών. Τότε, για κάθε $P \in E_1[m]$, για κάθε $Q \in E_2[m]$*

$$e_m(P, \hat{\phi}(Q)) = e_m(\phi(P), Q).$$

Δηλαδή οι $\phi, \hat{\phi}$ συμπεριφέρονται σαν συζυγείς απεικονίσεις ως προς τα e_m.

Αφού η αντιστοιχία Weil ορίστηκε στο $E[m] \times E[m]$, μπορούμε, για $m = \ell^n$, περνώντας στο όριο, να ορίσουμε μια ℓ-αδική αντιστοιχία $e : T_\ell(E) \times T_\ell(E) \to T_\ell(\mu)$, όπου στα μ_{ℓ^n} παίρνουμε εγκλεισμούς μέσω της $\zeta \to \zeta^\ell$. Η κατασκευή που περιγράψαμε σέβεται τα αντίστροφα όρια και τις ιδιότητες της πρότασης 2.6.5. Οδηγούμαστε έτσι φυσιολογικά στο θεώρημα:

Θεώρημα 2.6.7. *Υπάρχει μια αντιστοιχία*

$$e : T_\ell(E) \times T_\ell(E) \to T_\ell(\mu)$$

που ικανοποιεί τις ιδιότητες της πρότασης 2.6.5., και για κάθε ισογένεια ελλειπτικών καμπυλών $\phi : E_1 \to E_2$ ισχύει ότι $e(P, \hat{\phi}(Q)) = e(\phi(P), Q)$

Πρόταση 2.6.8. *Αν ϕ ένας ενδομορφισμός της E και*

$$\phi_\ell : T_\ell(E) \longrightarrow T_\ell(E)$$

η απεικόνιση που επάγει ο ϕ στο ℓ-αδικό πρότυπο του Tate, τότε

$$\det(\phi_\ell) = \deg(\phi)$$

και

$$\mathrm{tr}(\phi_\ell) = 1 + \deg(\phi) - \deg(1 - \phi)$$

Απόδειξη. Διαλέγουμε μια βάση u, v για το $T_\ell(E)$ υπεράνω του $\mathbb{Z}$ και γράφουμε $\phi_\ell(u) = au + bv$ και $\phi_\ell(v) = cu + dv$, δηλαδή ο πίνακας

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

αντιστοιχεί στην ϕ_ℓ. Χρησιμοποιώντας τις ιδιότητες της e, παίρνουμε

$$e(u, v)^{\deg \phi} = e([\deg \phi]u, v) = e(\hat{\phi}_\ell \phi_\ell(u), v)$$

και από το γεγονός ότι οι ϕ και $\hat{\phi}$ είναι e-συζυγείς έπεται

$$e(\hat{\phi}_\ell \phi_\ell(u), v) = e(\phi_\ell(u), \phi_\ell(v)) = e(au+bv, cu+dv) = e(u, v)^{ad-bc} = e(u, v)^{\det(\phi_\ell)}$$

οπότε, από την ιδιότητα (iii) της αντιστοιχίας Weil, έπεται το ζητούμενο. Επίσης, για κάθε δισδιάστατο πίνακα ισχύει

$$\mathrm{tr}(A) = 1 + \det(A) - \det(I - A)$$

το οποίο, σε συνδυασμό με το πρώτο σκέλος, μας δίνει ότι

$$\mathrm{tr}(\phi_\ell) = 1 + \det(\phi_\ell) - \det(1 - \phi_\ell) = 1 + \deg(\phi) - \deg(1 - \phi)$$

και η απόδειξη είναι πλήρης. □

2.7 Ο δακτύλιος των ενδομορφισμών και η ομάδα των αυτομορφισμών

Όπως παρατηρήσαμε και προηγουμένως, ο δακτύλιος ενδομορφισμών $\mathrm{End}(E)$ μιας ελλειπτικής καμπύλης E/K συνήθως είναι ισόμορφος με το $\mathbb{Z}$, ενίοτε όμως μπορεί να είναι και γνήσια μεγαλύτερος. Το επόμενο θεώρημα, το οποίο απλά παραθέτουμε χωρίς περισσότερες λεπτομέρειες, περιγράφει αυτές τις δυνατότητες.

Θεώρημα 2.7.1. *Έστω μια ελλειπτική καμπύλη E που ορίζεται πάνω από ένα σώμα K. Τότε ο $\mathrm{End}(E)$ είναι ισόμορφος είτε με το $\mathbb{Z}$, είτε ισόμορφος με έναν $\mathbb{Z}$-πεπερασμένα παραγόμενο υποδακτύλιο ενός μιγαδικού τετραγωνικού σώματος αριθμών K τέτοιου ώστε*

$$\mathrm{End}(E) \otimes \mathbb{Q} = K$$

είτε ισόμορφος με έναν $\mathbb{Z}$-πεπερασμένα παραγόμενο υποδακτύλιο μιας quaternion άλγεβρας L τέτοιας ώστε

$$\mathrm{End}(E) \otimes \mathbb{Q} = L$$

Εάν $\chi\alpha\rho(K) = 0$ τότε η τελευταία περίπτωση είναι αδύνατη (ένας δακτύλιος με αυτήν την ιδιότητα λέγεται order του $\mathbb{K}$ ή της L αντίστοιχα).

Σε αυτό το σημείο το παραπάνω θεώρημα ίσως φαντάζει υπερβολικά γενικό για τα παραδείγματα που μας ενδιαφέρουν να μελετήσουμε. Όπως σημειώσαμε και παραπάνω, θα επανέλθουμε στην μελέτη των ελλειπτικών καμπυλών με μιγαδικό πολλαπλασιασμό μετά την μελέτη των $E/\mathbb{C}$. Γενικά πάντως, το πρόβλημα την εύρεσης του $\mathrm{End}(E)$ δοσμένης καμπύλης E/K είναι δύσκολο. Για την $\mathrm{Aut}(E)$ όμως έχουμε το εξής γενικό θεώρημα:

Θεώρημα 2.7.2 (Χαρακτηρισμός της $\mathrm{Aut}(E)$)**.** *Έστω E/K μια ελλειπτική καμπύλη. Τότε η $\mathrm{Aut}(E)$ είναι πεπερασμένη ομάδα, και $|\mathrm{Aut}(E)| \mid 24$. Πιο συγκεκριμμένα, έχουμε τις εξής περιπτώσεις:*

(i) *Αν $j(E) \neq 0, 1728$, τότε $|\mathrm{Aut}(E)| = 2$*

(ii) *Αν $j(E) = 1728$, και $\chi\alpha\rho(K) \neq 2, 3$ τότε $|\mathrm{Aut}(E)| = 4$*

(iii) *Αν $j(E) = 0$, και $\chi\alpha\rho(K) \neq 2, 3$ τότε $|\mathrm{Aut}(E)| = 6$*

(iv) *Αν $j(E) = 0 = 1728$ με $\chi\alpha\rho(K) = 3$ τότε $|\mathrm{Aut}(E)| = 12$*

(v) *Αν $j(E) = 0 = 1728$ με $\chi\alpha\rho(K) = 2$ τότε $|\mathrm{Aut}(E)| = 24$*

Απόδειξη. Έστω $\mathrm{χαρ}(K) \neq 2, 3$. Τότε, η E έχει μια μορφή Weierstrass

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

και κάθε αυτομορφισμός της δίνεται από μια αλλαγή μεταβλητών $x = u^2x'$, $y = u^3y'$, όπου το u είναι μια μονάδα του $\bar{K}$. Μια τέτοια αλλαγή μεταβλητών επάγει έναν αυτομορφισμό αν και μόνο αν $u^4A = A$ και $u^6B = B$.

Αν $j(E) \neq 0, 1728$, θα έχουμε $AB \neq 0$ και καταλήγουμε ότι $u = 1$ ή -1.

(ii) Αν $B = 0$ τότε $j(E) = 1728$ και για να έχουμε αυτομορφισμό πρέπει να ισχύει $u^4 = 1$.

(iii) Αν $A = 0$ τότε $j(E) = 0$ και έχουμε αυτομορφισμό αν και μόνο $u^6 = 1$. Σε κάθε περίπτωση η $\mathrm{Aut}(E)$ προκύπτει μια κυκλική ομάδα τάξης που διαιρεί το 12.

Η απόδειξη για χαρακτηριστική 2 ή 3 παραλείπεται.

□

2.8 Καλή και κακή αναγωγή ελλειπτικών καμπυλών

Η ιδέα της αναγωγής ελλειπτικών καμπυλών είναι θεμελιώδης, και θα προσπαθήσουμε αρχικά να την περιγράψουμε με ένα παράδειγμα:

Παράδειγμα 2.8.1. Θεωρούμε την ελλειπτική καμπύλη E με εξίσωση Weierstrass

$$E : y^2 = x^3 - 4x$$

η οποία ορίζεται υπεράνω του $\mathbb{Q}$. Είναι άμεσο να δει κανείς ότι η E είναι ελλειπτική, δηλαδή $\Delta \neq 0$. Όμως, μπορούμε να «αναγάγουμε» την E modulo έναν πρώτο p και να πάρουμε την

$$E_p : y^2 = x^3 - [4]_p x$$

όπου με $[4]_p$ συμβολίζουμε την κλάση του 4 στο $\mathbb{Z}/p\mathbb{Z}$. Αν $p \neq 2$, τότε η E_p είναι ελλειπτική. Όμως για $p = 2$, παίρνουμε την

$$E_2 : y^2 = x^3$$

η οποία είναι singular! Καταμία έννοια, η E έχει «καλή» αναγωγή modulo όλους τους πρώτους εκτός από το 2, και έχει «κακή» αναγωγή στο 2.

Ορισμός 2.8.2. *Μια απόλυτη τιμή σε μια ακέραια περιοχή D είναι μια συνάρτηση $|\cdot| : D \to \mathbb{R}$ τέτοια ώστε:*

(i) $|x| \geq 0$.

(ii) $|x| = 0 \Leftrightarrow x = 0$.

(iii) $|xy| = |x||y|$ *για κάθε x και y στην D.*

(iv) $|x + y| \leq |x| + |y|$ *για κάθε x και y στην D.*

Αν επιπλέον ισχύει $|x + y| \leq max(|x|, |y|)$ τότε η απόλυτη τιμή λέγεται μη Αρχιμήδεια. Σε αντίθετη περίπτωση λέγεται Αρχιμήδεια.

Αν $|\cdot|$ είναι μια μη Αρχιμήδεια απόλυτη τιμή και $b > 1$, και ορισουμε $v(x) = -\log_b |x|$ και $v(0) = \infty$, τότε η συνάρτηση v έχει τις εξής ιδιότητες:

(i) $v(x) = \infty \Rightarrow x = 0$,

(ii) $v(xy) = v(x) + v(y)$,

(iii) $v(x + y) \geq \min(v(x)\ v(x))$.

Η v ονομάζεται εκτίμηση (valuation). Συχνά, λέμε ότι η v είναι η εκτίμηση που αντιστοιχεί στην $|\cdot|$. Επίσης, η v καλείται Αρχιμήδεια ή μη Αρχιμήδεια αν και μόνο αν η αντίστοιχη $|\cdot|$ είναι.

Ορισμός 2.8.3. *Ένα τοπικό σώμα K είναι ένα τοπικά συμπαγές τοπολογικό σώμα ως προς μια μη διακριτή τοπολογία.*

Δοθέντος ενός τέτοιου σώματος, μπορούμε να ορίσουμε μια εκτίμηση υ. Αν η εκτίμηση είναι Αρχιμήδεια, το σώμα ονομάζεται Αρχιμήδειο τοπικό σώμα, ενώ σε αντίθετη περίπτωση ονομάζεται μη Αρχιμήδειο.

Η κατάταξη των τοπικών σωμάτων (ως τοπολογικά σώματα) είναι η εξής:

(i) Αρχιμήδεια σώματα: Αν ένα τοπικό σώμα K ειναι Αρχιμήδειο, τότε είναι χαρακτηριστικής 0 και είναι ισόμορφο με το $\mathbb{R}$ ή με το $\mathbb{C}$.

(ii) Μη Αρχιμήδεια σώματα χαρακτηριστικής 0: Τότε το K είναι ισόμορφο με μια πεπερασμένη επέκταση κάποιου $\mathbb{Q}_p$.

(iii) Μη Αρχιμήδεια σώματα χαρακτηριστικής p: Τότε το K είναι ισόμορφο με τις τυπικές σειρές Laurent $\mathbb{F}_q(T)$ κάποιου $\mathbb{F}_q$ (όπου $q = p^n$).

Σε αυτήν την παράγραφο, συμβολίζουμε με K ένα τοπικό σώμα, που είναι πλήρες ως προς μια διακριτή εκτίμηση υ. Επίσης, το σύνολο

$$R = \{x \in K : \upsilon(x) \geq 0\}$$

ονομάζεται δακτύλιος ακεραίων της εκτίμησης υ, και το σύνολο

$$R^* = \{x \in K : \upsilon(x) = 0\}$$

ονομάζεται ομάδα των μονάδων στο R. Ο R είναι τοπικός δακτύλιος, και το μοναδικό μέγιστο ιδεώδες του είναι το

$$M = \{x \in K : \upsilon(x) > 0\}.$$

Θεωρούμε έναν uniformizer π για τον R (δηλαδή $M = \pi R$), και το σώμα $k = R/M$. Θεωρούμε ότι η υ είναι κανονικοποιημένη έτσι ώστε να έχουμε $\upsilon(\pi) = 1$. Εξ' ορισμού $\upsilon(0) = \infty$. Υποθέτουμε τέλος, ως συνήθως, πως τα K και k είναι τέλεια σώματα. Έστω λοιπόν μια ελλειπτική καμπύλη E/K με εξίσωση Weierstrass

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

Η αντικατάσταση

$$(x, y) \to (u^{-2}x, u^{-3}y)$$

οδηγεί σε μια νέα εξίσωση, στην οποία τα a_i έχουν αντικατασταθεί από $u^i a_i$. Αν διαλέξουμε το u να διαιρείται από μια αρκετά μεγάλη δύναμη του π, οδηγούμαστε σε μια εξίσωση Weierstrass όπου όλοι οι συντελεστές της είναι στον R. Σε αυτήν την περίπτωση θα έχουμε $\upsilon(\Delta) \geq 0$, και αφού η εκτίμηση υ είναι διακριτή, μπορούμε, ανάμεσα σε όλες τις εξισώσεις Weierstrass της καμπύλης με συντελεστές στον R, να διαλέξουμε εκείνην που ελαχιστοποιείται η τιμή $\upsilon(\Delta)$.

Ορισμός 2.8.4. *Έστω E/K μια ελλειπτική καμπύλη. Μια ελάχιστη εξίσωση Weierstrass για την E είναι μια εξίσωση Weierstrass τέτοια ώστε οι συντελεστές να ανήκουν στο R και η $\upsilon(\Delta)$ να ελαχιστοποιείται. Η τιμή αυτή $\upsilon(\Delta)$ καλείται εκτίμηση της ελάχιστης διακρίνουσας της E στην υ.*

Πρόταση 2.8.5. (i) *Κάθε καμπύλη E/K έχει μια ελάχιστη εξίσωση Weierstrass.*

(ii) *Μια ελάχιστη εξίσωση Weierstrass είναι μοναδική μέχρις αλλαγής μεταβλητών*

$$x = u^2x' + r, y = u^3y' + u^2sx' + t,$$

όπου $u \in R^*$ *και* $r, s, t \in R$.

(iii) *Το invariant διαφορικό*

$$\omega = \frac{dx}{2y + a_1x + a_3}$$

μιας ελάχιστης εξίσωσης Weierstrass είναι μοναδικό μέχρις πολλαπλασιασμού με ένα στοιχείο του R^*.

(iv) *Αντιστρόφως, αν ξεκινήσουμε με μια εξίσωση Weierstrass της* E/K *η οποία έχει συντελεστές στο* R, *και η αλλαγή μεταβλητών*

$$x = u^2x' + r, y = u^3y' + u^2sx' + t$$

οδηγεί σε μια ελάχιστη εξίσωση Weierstrass, τότε $u, r, s, t \in R$.

Απόδειξη. (i) Άμεσο από την συζήτηση που προηγήθηκε, αφού η εκτίμηση v είναι διακριτή.

(ii) Ξέρουμε ότι κάθε εξίσωση Weierstrass της E/K είναι μοναδική μέχρις αλλαγής μεταβλητών όπως παραπάνω, με $u \in K^*$ και $r, s, t \in K$. Αν και η αρχική εξίσωση και η εξίσωση που προκύπει μετά την αλλαγή μεταβλητών είναι ελάχιστες, τότε εξ΄ ορισμού $v(\Delta) = v(\Delta')$. Όμως $\Delta = u^{12}\Delta'$, άρα $u \in R^*$. Επίσης, με αυτήν την αλλαγή μεταβλητών βλέπουμε ότι τα $4r^3$ και $3r^4$ ανήκουν στον R, άρα το r ανήκει στον R. Ομοίως προκύπτουν ότι $s, t \in R$.

(iii) Άμεσο από το (ii) .

(iv) Αφού η καινούρια εξίσωση θα είναι ελάχιστη, θα έχουμε $v(\Delta') \leq v(\Delta)$. Επίσης, έχουμε $u^{12}\Delta' = \Delta$. Άρα $v(u) \geq 0$, δηλαδή $u \in R$. Επαναλαμβάνουμε την απόδειξη του (ii) και παίρνουμε $r, s, t \in R$.

□

Έστω τώρα η συνάρτηση της συνήθους προβολής modulo π, την οποία καλούμε συνάρτηση αναγωγής:

$$R \to k = R/\pi R : t \to \tilde{t}$$

Αν έχουμε διαλέξει μια ελάχιστη εξίσωση Weierstrass για την καμπύλη E/K, μπορούμε να κάνουμε αναγωγή modulo π στους συντελεστές της εξίσωσης και να πάρουμε την καμπύλη πάνω από το k, την

$$\tilde{E} : y^2 + \tilde{a}_1xy + \tilde{a}_3y = x^3 + \tilde{a}_2x^2 + \tilde{a}_4x + \tilde{a}_6.$$

Ορισμός 2.8.6. *Η καμπύλη* $\tilde{E}/k$ *ονομάζεται αναγωγή της* E *modulo* π.

Αφου ξεκινήσαμε με μια ελάχιστη εξίσωση Weierstrass για την E, η προηγούμενη πρόταση μας λέει ότι η εξίσωση για την $\tilde{E}$ είναι μοναδική υπό τις συνήθεις αλλαγές μεαβλητών

$$x = u^2x' + r, y = u^3y' + u^2sx' + t,$$

όπου $u \in k^*$ και $r, s, t \in k$.

Έστω ένα σημείο P της $E(K)$. Βρίσκουμε ομογενείς συντεταγμένες $R = [x_0, y_0, z_0]$, με $x_0, y_0, z_0 \in R$ και τουλάχιστον μια εξ' αυτών στο R^*. Τότε το σημείο

$$\tilde{P} = [\tilde{x}_0, \tilde{y}_0, \tilde{z}_0]$$

ανήκει στην $\tilde{E}(k)$. Ορίζεται έτσι μια απεικόνιση αναγωγής

$$E(K) \longrightarrow \tilde{E}(k)$$

με

$$P \longrightarrow \tilde{P}.$$

Ομοιως μπορούμε να ορίσουμε απεικόνιση αναγωγής

$$\mathbb{P}^n(K) \longrightarrow \mathbb{P}^n(k),$$

και σε αυτήν την περίπτωση η απεικόνιση αναγωγής $E(K) \to \tilde{E}(k)$ είναι ο περιορισμός της παραπάνω απεικόνισης. Η καμπύλη $\tilde{E}/k$ μπορεί να είναι singular. Ορίζουμε τα εξής σύνολα:

$$E_0(K) = \{P \in E(K) : \tilde{P} \in \tilde{E}_{ns}(k)\}$$

και

$$E_1(K) = \{P \in E(K) : \tilde{P} = \tilde{O}\}.$$

Από την πρόταση 2.8.5, τα $E_0(K)$ και $E_1(K)$ δεν εξαρτώνται από την ελάχιστη εξίσωση Weierstrass που διαλέγουμε.

Πρόταση 2.8.7. *Υπάρχει ακριβής ακολουθία αβελιανών ομάδων*

$$0 \longrightarrow E_1(K) \longrightarrow E_0(K) \longrightarrow \tilde{E}_{ns}(k) \longrightarrow 0,$$

όπου η απεικόνιση $E_0(K) \longrightarrow \tilde{E}_{ns}(k)$ είναι η αναγωγή modulo π.

Η παραπάνω πρόταση θα μας δώσει την ευχέρεια να χειριστούμε την συμπεριφορά των torsion σημείων σε μια αναγωγή.

Πρόταση 2.8.8. *Έστω E/K μια ελλειπτική καμπύλη και $m \geq 1$ ένας ακέραιος σχετικά πρώτος προς την χαρ(k). Τότε:*

(i) *Η $E_1(K)$ δεν περιέχει μη τετριμμένα σημεία τάξης m.*

(ii) *Αν η $\tilde{E}/k$ είναι nonsingular, τότε η απεικόνιση αναγωγής*

$$E(K)[m] \longrightarrow \tilde{E}(k)$$

είναι 1-1.

Απόδειξη. Για την απόδειξη του ερωτήματος (i) απαιτείται η έννοια της formal group μιας ελλειπτικής καμπύλης. Η απόδειξη παραλείπεται. Για το ερώτημα (ii) , αν η $\tilde{E}$ είναι nonsingular τότε $E_0(K) = E(K)$ και $\tilde{E}_{ns}(k) = \tilde{E}(k)$, το οποίο, σε συνδυασμό με την παραπάνω ακριβή ακολουθία, δίνει ότι η m-torsion υποομάδα της $E(K)$ εμφυτεύεται στην $\tilde{E}(k)$. □

Για να εκτιμήσουμε την ισχύ του παραπάνω αποτελέσματος, θα δούμε κάποια παραδείγματα που μας δείχνουν πως μπορούμε να συνάγουμε γρήγορα συμπεράσματα για τις υποομάδες στρέψης ελλειπτικών καμπυλών.

Παράδειγμα 2.8.9. (i) Θεωρούμε την $E/\mathbb{Q}$ με εξίσωση

$$E : y^2 + y = x^3 - x + 1.$$

Η E έχει διακρίνουσα $\Delta = -611$, άρα η $\tilde{E}$ είναι nonsingular modulo 2. Επειδή $\tilde{E}(\mathbb{F}_2) = \{O\}$ και $E(\mathbb{Q})[2] = \{O\}$, η πρόταση 2.8.8 μας δίνει ότι η $E(\mathbb{Q})$ δεν έχει μη τετριμμένα σημεία στρέψης.

(ii) Θεωρούμε την

$$E : y^2 = x^3 + 3.$$

Η E έχει διακρίνουσα $\Delta = -2^4 \cdot 3^5$, άρα η $\tilde{E}$ είναι nonsingular για κάθε πρώτο $p \geq 5$. Επειδή

$$|\tilde{E}(\mathbb{F}_5)| = 6$$

και

$$|\tilde{E}(\mathbb{F}_7)| = 13$$

συμπεραίνουμε πως η $E(\mathbb{Q})$ δεν έχει μη τετριμμένα σημεία στρέψης. Αφού όμως $(1, 2) \in E(\mathbb{Q})$, έπεται πως η $E(\mathbb{Q})$ είναι άπειρη.

Περισσότερη πληροφορία για τα torsion σημεία μιας ελλειπτικής καμπύλης δίνει το παρακάτω αποτέλεσμα, που οφείλεται στον Cassels.

Θεώρημα 2.8.10 (Cassels)**.** *Έστω χαρ(K)= 0 και χαρ(k)= $p > 0$. Έστω επίσης μια ελλειπτική καμπύλη E/K με εξίσωση Weierstrass*

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

με όλα τα $a_i \in R$. Έστω P ένα σημείο της $E(K)$ με τάξη $m \geq 2$. Τότε:

(i) *Αν το m δεν είναι δύναμη του p, τότε $x(P), y(P) \in R$.*

(ii) *Αν $m = p^n$, τότε*

$$\pi^{2r}x(P), \pi^{3r}y(P) \in R,$$

όπου

$$r = \left[\frac{v(p)}{p^n - p^{n-1}}\right],$$

όπου $[x]$ είναι, ως συνήθως, το ακέραιο μέρος του x.

Απόδειξη. Αν $x(P) \in R$, τότε το ζητούμενο ισχύει. Αν όχι, τότε $v(x(P)) < 0$. Αν η εξίσωση Weierstrass που ξεκινήσαμε δεν είναι ελάχιστη και (x', y') είναι οι μεταβλητές μιας ελάχιστης εξίσωσης Weierstrass, τότε

$$v(x(P)) \geq v(x'(P))$$

και

$$v(y(P)) \geq v(y'(P)).$$

Αυτή η παρατήρηση μας δείχνει ότι αρκεί να δείξουμε το ζητούμενο για μια ελάχιστη εξίσωση Weierstrass.

Η απόδειξη της πρότασης για μια ελάχιστη εξίσωση Weierstrass απαιτεί την έννοια της formal group $\hat{E}(M)$ μιας ελλειπτικής καμπύλης, και για αυτό παραλείπεται. □

Μπορούμε τώρα να δώσουμε τον κύριο ορισμό αυτής της παραγράφου:

Ορισμός 2.8.11. *Έστω E/K μια ελλειπτική καμπύλη και $\tilde{E}$ η αναγωγή modulo $M = \pi R$ μιας ελάχιστης Weierstrass εξίσωσης της. Τότε, υπάρχουν τρεις περιπτώσεις για την $\tilde{E}$:*

(i) *Αν η $\tilde{E}$ είναι nonsingular, τότε λέμε ότι η E έχει καλή (ή ευσταθή) αναγωγή στο π (ή στο M).*

(ii) *Αν η $\tilde{E}$ έχει node, τότε λέμε ότι η E έχει πολλαπλασιαστική (ή ημιευσταθή) αναγωγή στο π.*

(iii) *Αν η $\tilde{E}$ έχει cusp, τότε λέμε ότι η E έχει προσθετική (ή ασταθή) αναγωγή στο π.*

Αν η E έχει ημιευσταθή ή ασταθή αναγωγή, τότε λέμε ότι έχει κακή αναγωγή στο π. Αν η E έχει ημιευσταθή αναγωγή, τότε λέμε ότι είναι split αν οι συντελεστές των εφαπτόμενων ευθειών στο node ανήκουν στο k. Αλλιώς, λέμε ότι η E είναι nonsplit.

Μια ελάχιστη εξίσωση Weierstrass της E μας δίνει όλη την πληροφορία για το είδος της αναγωγής της.

Πρόταση 2.8.12. *Έστω E/K μια ελλειτική καμπύλη με ελάχιστη εξίσωση Weierstrass*

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

Έστω επίσης το c_4 όπως στον ορισμό 2.1.2.

(i) *Η E έχει καλή αναγωγή αν και μόνο αν $v(\Delta) = 0$. Τότε προφανώς η $\tilde{E}/k$ είναι ελλειπτική καμπύλη.*

(ii) *Η E έχει ημιευσταθή αναγωγή αν και μόνο αν $v(\Delta) > 0$ και $v(c_4) = 0$. Σε αυτήν την περίπτωση*

$$\tilde{E}_{ns}(\bar{k}) \cong \bar{k}^*.$$

(iii) *Η E έχει ασταθή αναγωγή αν και μόνο αν $v(\Delta) > 0$ και $v(c_4) > 0$. Σε αυτήν την περίπτωση*

$$\tilde{E}_{ns}(\bar{k}) \cong \bar{k}^+.$$

Απόδειξη. Άμεσο πόρισμα της πρότασης 2.1.6 και του θεωρήματος 2.3.2. □

Η επόμενη ιδιότητα είναι συχνά χρήσιμη για την μελέτη του είδους της αναγωγής που έχει μια ελλειπτική καμπύλη.

Ορισμός 2.8.13. *Έστω E/K μια ελλειπτική καμπύλη. Λέμε ότι η E/K έχει potential καλή αναγωγή αν υπάρχει μια πεπερασμένη επέκταση K' του K τέτοια ώστε η E να έχει καλή αναγωγή πάνω από το K'.*

Για παράδειγμα, μπορεί να αποδείξει κανείς ότι αν το K είναι μια πεπερασμένη επέκταση του $\mathbb{Q}_p$ και η E/K έχει μιγαδικό πολλαπλασιασμό, τότε η E έχει potential καλή αναγωγή πάνω από το K.

Η επόμενη πρόταση μελετάει την συμπεριφορά της αναγωγής σε σχέση με τις επεκτάσεις σωμάτων.

Θεώρημα 2.8.14 (Ημιευσταθούς αναγωγής)**.** *Έστω E/K μια ελλειπτική καμπύλη.*

(i) *Αν η επέκταση K'/K είναι αδιακλάδιστη, τότε το είδος της αναγωγής της E πάνω από το K είναι το ίδιο με το είδος της αναγωγής της E πάνω από το K'.*

(ii) *Αν η επέκταση K'/K είναι πεπερασμένη, και η E έχει πάνω από το K καλή ή ημιευσταθή αναγωγή, τότε έχει το ίδιο είδος αναγωγής και πάνω από το K'.*

(iii) *Υπάρχει πεπερασμένη επέκταση K'/K τέτοια ώστε η E να έχει καλή ή (split) ημιευσταθή αναγωγή πάνω από το K'.*

Η επόμενη πρόταση δίνει ένα κριτήριο για potential καλή αναγωγή συναρτήσει της j-invariant της καμπύλης.

Πρόταση 2.8.15. *Έστω E/K μια ελλειπτική καμπύλη. Τότε η E έχει potential καλή αναγωγή αν και μόνο αν $j(E) \in R$.*

Τέλος, αξίζει να αναφερθεί το ακόλουθο γνωστό αποτέλεσμα που αποτελεί χρήσιμο κριτήριο για την εύρεση καμπυλών καλής αναγωγής.

Θεώρημα 2.8.16 (Θεώρημα (Κριτήριο των Neron-Ogg-Shafarevich)**.** *Έστω E/K μια ελλειπτική καμπύλη. Τα ακόλουθα είναι ισοδύναμα:*

(i) *Η E έχει καλή αναγωγή πάνω από το K.*

(ii) *Η $E[m]$ είναι αδιακλάδιστη στην v για κάθε $m \geq 1$ που είναι σχετικά πρώτος προς την χαρακτηριστική του k.*

(iii) *Το πρότυπο του Tate $T_\ell(E)$ είναι αδιακλάδιστο στην v για κάποιους πρώτους ℓ διάφορους από την χαρακτηριστική του k.*

(iv) *Η $E[m]$ είναι αδιακλάδιστη στην v για άπειρους $m \geq 1$ που είναι σχετικά πρώτοι προς την χαρακτηριστική του k.*

2.9 Η Ομάδα $E(\mathbb{F}_q)$

Σε αυτήν την παράγραφο η μελέτη μας εστιάζεται στις καμπύλες που ορίζονται πάνω από πεπερασμένα σώματα. Δίνουμε μια απόδειξη της αρχής του Hasse, καθώς και μια απόδειξη των εικασιών του Weil για ελλειπτικές καμπύλες. Τέλος, εξετάζουμε εν συντομία κάποια αποτελέσματα για τους δακτύλιους ενδομορφισμών $\mathrm{End}(E)$ ελλειπτικών καμπυλών E που ορίζονται πάνω από σώματα πεπερασμένης χαρακτηριστικής. Χρησιμοποιούμε, όπως έχουμε ήδη αναφέρει, τον συμβολισμό $\mathbb{F}_q$ για να δηλώσουμε ένα σώμα χαρακτηριστικής p με q στοιχεία, όπου $q = p^n$. Για αρχή θα χρειαστούμε ένα βασικό λήμμα:

Πρόταση 2.9.1 (Ανισότητα Cauchy-Schwarz για αβελιανές ομάδες)**.** *Αν G είναι μια αβελιανή ομάδα, και $d : G \to \mathbb{Z}$ μια θετικά ορισμένη τετραγωνική μορφή. Τότε:*

$$|d(\psi - \phi) - d(\psi) - d(\phi)| \leq 2\sqrt{d(\psi)d(\phi)}$$

για κάθε ψ, $\phi \in G$.

Απόδειξη. Αν $\psi = 0$ η ανισσότητα είναι τετριμμένη. Έστω $\psi \neq 0$, $\phi \in G$. Ορίζουμε την ποσότητα $L(\psi, \phi) = d(\psi - \phi) - d(\psi) - d(\phi)$. Αφού η d είναι τετραγωνική μορφή, η L είναι διγραμμική μορφή. Επίσης, αφού η d είναι θετικά ορισμένη, ισχύει

$$0 \leq d(m\psi - n\phi) = m^2 d(\psi) + mnL(\psi, \phi) + n^2 d(\phi)$$

για κάθε m,$n \in \mathbb{Z}$.

Επιλέγοντας $m = -L(\psi, \phi)$ και $n = 2d(\psi)$, παίρνουμε ότι

$$0 \leq 4d(\psi)^2 d(\phi) - d(\psi)L(\psi, \phi)^2 = d(\psi)(4d(\psi)d(\phi) - L(\psi, \phi)^2).$$

Αφού $\psi \neq 0$ έπεται ότι $d(\psi) > 0$ και έχουμε τελειώσει. □

Έστω λοιπόν μια ελλειπτική καμπύλη υπεράνω του $\mathbb{F}_q$. Θέλουμε να μετρήσουμε την τάξη της ομάδας $E(\mathbb{F}_q)$ δηλαδή τα $(x, y) \in \mathbb{F}_q^2$ που ικανοποιούν μια εξίσωση Weierstrass της καμπύλης. Αφού κάθε τιμή του x δίνει δύο τιμές για το y, έχουμε τετριμμένα ότι

$$|E(\mathbb{F}_q)| \leq 2q + 1.$$

Μια σκέψη είναι ότι υπάρχει περίπου 50% πιθανότητα μια τυχαία τιμή του x να δίνει μια λύση (x, y), άρα θα πρέπει να περιμενουμε $|E(\mathbb{F}_q)| \simeq q$. Η ακριβής εκτίμηση του παρακάτω θεωρήματος ήταν εικασία του Artin.

Θεώρημα 2.9.2 (Αρχή του Hasse)**.** *Αν μια ελλειπτική καμπύλη E ορίζεται υπεράνω του πεπερασμένου σώματος $\mathbb{F}_q$, τότε*

$$||E(\mathbb{F}_q)| - q - 1| \leq 2\sqrt{q}$$

Απόδειξη. Θεωρούμε μια κανονική μορφή Weierstrass για την E με συντελεστές στο $\mathbb{F}_q$ και τον μορφισμό του Frobenius :

$$\phi : E \to E$$

με

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

Ο μορφισμός του Frobenius παράγει την ομάδα Galois της επέκτασης $\bar{\mathbb{F}}_q/\mathbb{F}_q$, άρα για κάθε σημείο P στην καμπύλη $E(\bar{\mathbb{F}}_q)$ θα έχουμε ότι $P \in E(\mathbb{F}_q) \iff$ το P είναι σταθερό σημείο του μορφισμού του Frobenius, δηλαδή αν και μόνο αν:

$$P \in ker(1-\phi).$$

Εφαρμόζωντας την πρόταση 2.5.10 και το πόρισμα 2.5.13, βλέπουμε ότι

$$|E(\mathbb{F}_q)| = |ker(1-\phi)| = deg(1-\phi).$$

Στο πόρισμα 2.5.18 δείξαμε ότι η deg είναι θετικά ορισμένη τετραγωνική μορφή, άρα, από την Cauchy-Schwarz (πρόταση 2.9.1) και το γεγονός ότι $\deg\phi = q$ έχουμε το ζητούμενο. □

Αν και η αρχή του Hasse βρίσκει φράγματα για το πλήθος των σημείων μιας ελλειπτικής καμπύλης που ορίζεται πάνω από ένα πεπερασμένο σώμα, εντούτοις πρέπει να σημειωθεί ότι δεν υπάρχει αρκετά γρήγορος αλγόριθμος που να μετράει ακριβώς την τάξη της ομάδας αυτής. Μια σύντομη συζήτηση πάνω στους αλγόριθμους αυτούς υπάρχει στο [Silverman, [30], κεφ.11].

Αξίζει επίσης να αναφερθεί η παρακάτω γενίκευση της αρχής του Hasse που αποδείχθηκε από τον Weil το 1948:

Θεώρημα 2.9.3 (Θεώρημα (Αρχή Hasse-Weil))**.** *Αν μια καμπύλη C γένους g ορίζεται υπεράνω ενός πεπερασμένου σώματος $\mathbb{F}_q$, τότε*

$$||C(\mathbb{F}_q)| - q - 1| \leq 2g\sqrt{q}$$

Η γενίκευση αυτή μπορεί να συναχθεί ως πόρισμα των ακόλουθων εικασιών που διετύπωσε ο Weil το 1949. Οι εικασίες αυτές μελετούν σε μεγαλύτερο βάθος την συμπεριφορά των τάξεων των varieties που ορίζονται πάνω από πεπερασμένα σώματα. Για να μπορέσουμε να τις περιγράψουμε πρέπει πρώτα να ορίσουμε την Z συνάρτηση μιας variety, η οποία είναι η εκθετική της γεννήτριας συνάρτησης της ακολουθίας αριθμών $a_n = |V(\mathbb{F}_{q^n})|$

Ορισμός 2.9.4. *Έστω V μια variety που ορίζεται πάνω από ένα πεπερασμένο σώμα $\mathbb{F}_q$, ας πούμε ότι η V ορίζεται ως οι κοινές ρίζες m το πλήθος ομογενών πολυωνύμων, δηλαδή*

$$V = \{P \in \mathbb{P}^N(\mathbb{F}_q) : f_i(P) = 0, \}$$

με $i = 1, 2, ..., m$. Ορίζουμε την Z-συνάρτηση της V να είναι η συνάρτηση:

$$Z(V/\mathbb{F}_q : T) = \exp\left(\sum_{n=1}^{\infty} |V(\mathbb{F}_{q^n})| \frac{T^n}{n}\right)$$

Πρόταση 2.9.5. *Το $|V(\mathbb{F}_{q^n})|$ είναι ίσο με την παράγωγο*

$$\frac{1}{(n-1)!}\frac{d^n}{dT^n}\log Z(V/\mathbb{F}_q : T)$$

υπολογισμένη στο $T = 0$.

Απόδειξη. Άμεση από τον ορισμό της Z-συνάρτησης. □

Παράδειγμα 2.9.6. Αν $V = \mathbb{P}^n$, τότε

$$Z(\mathbb{P}^N/\mathbb{F}_q : T) = \frac{1}{(1-T)(1-qT)(1-q^2T)...(1-q^NT)}$$

Το παράδειγμα αυτό ίσως υποψιάζει κάποιον για τις ακόλουθες εικασίες:

Θεώρημα 2.9.7 (Εικασίες Weil)**.** *Έστω V μια nonsingular προβολική variety διάστασης N που ορίζεται πάνω από ένα πεπερασμένο σώμα $\mathbb{F}_q$. Τότε:*

(i) *Η Z-συνάρτηση της καμπύλης είναι ρητή.*

(ii) *Υπάρχει $\epsilon = \epsilon(V) \in \mathbb{Z}$ ώστε να η V να ικανοποιεί την συναρτησιακή εξίσωση:*

$$Z(V/\mathbb{F}_q : 1/q^NT) = \pm q^{N\epsilon/2}T^\epsilon Z(V/\mathbb{F}_q : T)$$

(iii) *Ισχύει*

$$Z(V/\mathbb{F}_q : T) = \frac{P_1(T)...P_{2N-1}(T)}{P_0(T)...P_{2N}(T)}$$

όπου τα $P_i(T)$ έχουν ακέραιους συντελεστές, $P_0(T) = 1 - T$, $P_{2N}(T) = 1 - q^N(T)$ και κάθε $P_i(T)$, για $i = 1, ..., 2N-1$, γράφεται στην μορφή

$$P_i(T) = \prod_{j=1}^{b_i}(1 - a_{ij}T)$$

με την ιδιότητα κάθε a_{ij} να έχει μέτρο ίσο με $\sqrt{q}$.

Η τρίτη ιδιότητα συχνά καλείται και Υπόθεση Riemann για varieties. Επίσης, ο αριθμός b_i καλείται και i-οστός αριθμός Betti της V.

Οι εντυπωσιακές αυτές εικασίες έχουν εξίσου ενδιαφέρουσα ιστορία: όπως είπαμε, ο ίδιος ο Weil απέδειξε τις εικασίες του για καμπύλες και αργότερα για αβελιανές varieties. Στην γενική περίπτωση, η ρητότητα αποδείχτηκε από τον Dwork το 1960, η συναρτησιακή εξίσωση από τον Grothendieck το 1965, ενώ ο Deligne έδειξε την υπόθεση Riemann το 1974 (ο ίδιος, το 1971, είχε δείξει πως η υπόθεση Riemann για varieties συνεπάγεται την εικασία του Ramanujan για την συνάρτηση τ, την οποία θα μελετήσουμε στην επόμενη παράγραφο). Ο ίδιος ο Deligne έδωσε το 1980 και μια δεύτερη απόδειξη της υπόθεσης Riemann. Στο πέμπτο κεφάλαιο, όταν θα μελετήσουμε τις L-σειρές των ελλειπτικών καμπυλών και των modular μορφών, θα δούμε πως κι εκεί θα μας απασχολήσει η ύπαρξη συναρτησιακής εξίσωσης για αυτές τις L-σειρές.

Προχωράμε τώρα στην απόδειξη των εικασίων του Weil για ελλειπτικές καμπύλες. Πιο συγκεκριμμένα, θα δείξουμε το εξής θεώρημα:

Θεώρημα 2.9.8 (Θεώρημα (Weil))**.** *Έστω $E/\mathbb{F}_q$ μια ελλειπτική καμπύλη. Τότε, υπάρχει $\alpha = \alpha(E) \in \mathbb{Z}$ τέτοιος ώστε:*

$$Z(E/\mathbb{F}_q : T) = \frac{1 - \alpha T + qT^2}{(1-T)(1-qT)}$$

όπου $1 - \alpha T + qT^2 = (1 - aT)(1 - bT)$, με $|a| = |b| = \sqrt{q}$. Άρα ισχύει η συναρτησιακή εξίσωση:

$$Z(E/\mathbb{F}_q : 1/qT) = Z(E/\mathbb{F}_q : T).$$

Ο λόγος που το παραπάνω θεώρημα ονομάζεται υπόθεση Riemann για καμπύλες είναι ο εξής:

Θέτοντας $T = q^{-s}$ στον τύπο της $Z(E/\mathbb{F}_q : T)$ ορίζεται η ζ-συνάρτηση

$$\zeta(s) \equiv \zeta_{E/\mathbb{F}_q}(s) = Z(E/\mathbb{F}_q : q^{-s}) = \frac{1 - \alpha q^{-s} + q^{1-2s}}{(1-q^{-s})(1-q^{1-s})}$$

όπου τώρα η συναρτησιακή εξίσωση που θέλουμε να δείξουμε παίρνει την μορφή

$$\zeta(s) = \zeta(1-s)$$

και η υπόθεση Riemann είναι η παρατήρηση

$$\zeta(s) = 0 \Longrightarrow |q^s| = q^{1/2} \Longrightarrow \Re(s) = \frac{1}{2}$$

Για την απόδειξη του θεωρήματος 2.9.8 θα χρειαστούμε το ακόλουθο θεώρημα, καθώς και την πρόταση 2.6.8, η οποία συνεπάγεται πως τα $\det(\phi_\ell)$ και $\mathrm{tr}(\phi_\ell)$ είναι ακέραιοι, και ανεξάρτητοι του ℓ.

Θεώρημα 2.9.9. *Έστω E μια ελλειπτική καμπύλη που ορίζεται πάνω από το πεπερασμένο σώμα $\mathbb{F}_q$, $\phi : E \to E$ ο συνήθης μορφισμός του Frobenius*

$$\phi(x, y) = (x^q, y^q)$$

και ορίζουμε το

$$\alpha = q + 1 - |E(\mathbb{F}_q)|$$

Τότε, οι συζυγείς μιγαδικές ρίζες a, b του πολυωνύμου $f(x) = x^2 - \alpha x + q$ έχουν μέτρο ίσο με $\sqrt{q}$ και για κάθε φυσικό αριθμό n ισχύει η σχέση

$$|E(\mathbb{F}_{q^n})| = q^n + 1 - a^n - b^n.$$

Επίσης, ο μορφισμός ϕ μηδενίζει το f, δηλαδή ο μορφισμός

$$\phi^2 - \alpha\phi + q$$

είναι ο μηδενικός μορφισμός.

Απόδειξη. Ξέρουμε ότι

$$|E(\mathbb{F}_q)| = \deg(1 - \phi)$$

Από την πρόταση 2.6.8, παίρνουμε $\det(\phi_\ell) = deg(\phi) = q$ και

$$\mathrm{tr}(\phi_\ell) = 1 + \deg(\phi) - \deg(1-\phi) = 1 + q - |E(\mathbb{F}_q)| = \alpha.$$

Καταλήγουμε πως το χαρακτηριστικό πολυώνυμο του ϕ_ℓ είναι το $\det(X - \phi_\ell) = f(X)$. Οι συντελεστές του f ανήκουν στο $\mathbb{Z}$, και το παραγοντοποιούμε ως εξής

$$\det(X - \phi_\ell) = (X - a)(X - b).$$

Για κάθε ρητό m/n έχουμε

$$\det\left(\frac{m}{n} - \phi_\ell\right) \geq 0$$

οπότε το $f(X) \in \mathbb{Z}[X]$ είναι ≥ 0 στο $\mathbb{R}$, άρα έχει μια διπλή ρίζα $a = b$ ή δύο συζυγείς ρίζες μιγαδικές $a \neq b$. Από την σχέση $ab = q$ και το γεγονός ότι $|a| = |b|$ παίρνουμε $|a| = \sqrt{q} = |b|$.

Για κάθε $n \geq 1$, έχουμε

$$|E(\mathbb{F}_{q^n})| = \deg(1 - \phi^n)$$

όπου ϕ^n είναι ο μορφισμός του Frobenius ύψωση εις την q^n δύναμη. Το χαρακτηριστικό πολυώνυμο του ϕ_ℓ^n είναι το

$$\det(X - \phi_\ell^n) = (X - a^n)(X - b^n).$$

Έπεται πως

$$|E(\mathbb{F}_{q^n})| = \deg(1 - \phi^n) = \det(1 - \phi_\ell^n) = q^n + 1 - a^n - b^n.$$

Το δεύτερο συμπέρασμα είναι μια απλή εφαρμογή του Cayley-Hamilton. Ο ϕ_ℓ μηδενίζει το χαρακτηριτικό του πολυώνυμο, και έτσι παίρνουμε

$$\deg(\phi^2 - \alpha\phi + q) = \det(\phi_\ell^2 - \alpha\phi_\ell + q) = \det(0) = 0$$

άρα ο $\phi^2 - \alpha\phi + q$ είναι τετριμμένος. □

Για ευνόητους λοιπόν λόγους, η ποσότητα $\alpha = q + 1 - |E(\mathbb{F}_q)|$ καλείται ίχνος του Frobenius. Μπορούμε τώρα να αποδείξουμε το θεώρημα του Weil (2.9.8):

Απόδειξη. Παρατηρείστε ότι αν αποδείξουμε την ρητή μορφή της συνάρτησης Z, η συναρτησιακή εξίσωση είναι άμεση. Παίρνουμε:

$$\log(Z(E/\mathbb{F}_q : T)) = \sum_{n=1}^{\infty} |E(\mathbb{F}_{q^n})| \frac{T^n}{n}$$

και από το θεώρημα 2.9.9 παίρνουμε

$$\sum_{n=1}^{\infty} |E(\mathbb{F}_{q^n})| \frac{T^n}{n} = \sum_{n=1}^{\infty} (q^n + 1 - a^n - b^n) \frac{T^n}{n}$$

$$= -\log(1 - T) + \log(1 - aT) + \log(1 - bT) - \log(1 - qT)$$

άρα

$$Z(E/\mathbb{F}_q : T) = \frac{(1 - aT)(1 - bT)}{(1 - T)(1 - qT)}$$

όπου τα a, b είναι όπως στο θεώρημα 2.9.9, οπότε ικανοποιούν τα ζητούμενα. □

Είναι απλό τώρα να δει κανείς πως το θεώρημα 2.9.8 δίνει ξανά την Αρχή του Hasse, αφού

$$|E(\mathbb{F}_q)| = q+1-a-b \Longrightarrow ||E(\mathbb{F}_q)| - q - 1| = |a+b| \leq |a| + |b| = \sqrt{q} + \sqrt{q} = 2\sqrt{q}.$$

Πρίν κλείσουμε την παράγραφο αυτήν που αφορά τις ελλειπτικές καμπύλες E που ορίζονται πάνω από πεπερασμένα σώματα, είναι χρήσιμο να αναφέρουμε κάποια αποτελέσματα που αφορούν τους δακτύλιους $\mathrm{End}(E)$ των ενδομορφισμών τους.

Θυμηθείτε πως αν το K είναι χαρακτηριστικής p, τότε, από το θεώρημα 2.6.1, η υποομάδα $E[p^n]$ είναι είτε η τετριμμένη για κάθε n, είτε για κάθε n ισχύει ότι

$$E[p^n] \cong \frac{\mathbb{Z}}{p^n\mathbb{Z}}$$

Η επόμενη πρόταση αποσαφηνίζει αυτόν τον διαχωρισμό:

Πρόταση 2.9.10 (Deuring)**.** *Έστω K ένα σώμα χαρακτηριστικής p (όχι απαραίτητα πεπερασμένο), E/K μια ελλειπτική καμπύλη υπεράνω του σώματος αυτού, οι μορφισμοί του Frobenius και οι δυικοί τους*

$$\phi_n : E \to E^{(p^n)}$$

$$\hat{\phi}_n : E^{(p^n)} \to E$$

(i) *Η $E[p^n]$ είναι τετριμμένη για κάθε $n \iff$ όλοι οι $\hat{\phi}_n$ είναι γνήσια μη διαχωρίσιμοι $\iff$ ο μορφισμός $[p]$: $E \to E$ είναι γνήσια μη διαχωρίσιμος και η $j(E)$ ανήκει στο $\mathbb{F}_p^2 \iff$ ο $\mathrm{End}(E)$ είναι ένας order μιας quaternion άλγεβρας L.*

(ii) *Αν η $E[p^n]$ είναι ισόμορφη για κάθε n με την*

$$\frac{\mathbb{Z}}{p^n\mathbb{Z}}$$

τότε, αν η $j(E)$ ανήκει στην κλειστή θήκη του $\mathbb{F}_p$, ο $\mathrm{End}(E)$ είναι ένας order ενός μιγαδικού τετραγωνικού σώματος αριθμών.

Μπορεί κανείς να δείξει ότι αν είμαστε στην περίπτωση (ii) και η $j(E)$ δεν ανήκει στο $\bar{\mathbb{F}}_p$, τότε ο $\mathrm{End}(E)$ είναι ισόμορφος με το $\mathbb{Z}$.

Ορισμός 2.9.11. *Αν η E είναι όπως στο (i) της πρότασης 2.9.10, τότε καλείται supersingular, ή αλλιώς λέμε ότι έχει αναλλοίωτη Hasse 0. Σε αντίθετη περίπτωση, η E καλείται ordinary , ή λέμε ότι έχει αναλλοίωτη Hasse 1.*

Παρατηρούμε ότι, από τη πρόταση 2.9.10, υπάρχουν πεπερασμένες μόνο supersingular E πάνω απ' το K. Το επόμενο θεώρημα μας εξασφαλίζει έναν γρήγορο τρόπο να αποφασίζει κανείς αν μια καμπύλη είναι supersingular.

Πρόταση 2.9.12. *Έστω E πάνω από το $\bar{\mathbb{F}}_q$, το οποίο έχει χαρακτηριστική $p \geq 3$. Θέτουμε $m = (p-1)/2$ και ορίζουμε το πολυώνυμο Hasse*

$$H_p(t) = \sum_{i=0}^{m} \binom{m}{i}^2 t^i.$$

Θεωρούμε επίσης ότι η E έχει μορφή Legendre

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

όπου $\lambda \in \bar{\mathbb{F}}_q$ και $\lambda \neq 0, 1$.

(i) *(Deuring) Η E είναι supersingular αν και μόνο αν*

$$H_p(\lambda) = 0.$$

(ii) *(Manin)*

$$|E(\mathbb{F}_q)| \equiv 1 - H(\lambda)^{(q-1)(p-1)} \mathrm{mod} p$$

Παρατηρούμε ότι η έννοια της supersingular καμπύλης μοιάζει κάπως να σχετίζεται με τον μιγαδικό πολλαπλασιασμό. Πράγματι, υπάρχουν αποτελέσματα, τα οποία οφείλονται στους Elkies και Serre, τα οποία περιγράφουν το πως σχετίζονται οι $E/\mathbb{Q}$ χωρίς μιγαδικό πολλαπλασιασμό με τις αναγωγές τους πάνω από πεπερασμένα σώματα οι οποίες μπορεί να είναι supersingular.

2.10 Οι Ομάδες $E(\mathbb{C})$ και $E(\mathbb{R})$

Σε αυτήν την παράγραφο, θεωρούμε αρχικά μια ελλειπτική καμπύλη E που ορίζεται πάνω από το $\mathbb{C}$, με σκοπό να περιγράψουμε την δομή της ομάδα $E(\mathbb{C})$. Αμέσως μετά θα θεωρήσουμε μια ελλειπτική καμπύλη E που θα ορίζεται πάνω από το $\mathbb{R}$ και θα μελετήσουμε την $E(\mathbb{R})$.

Πριν προχωρήσουμε όμως στην περιγραφή της $E(\mathbb{C})$ για μια ελλειπτική καμπύλη $E/\mathbb{C}$, θα χρειαστεί να μιλήσουμε πρώτα για lattices και ελλειπτικές συναρτήσεις.

Ορισμός 2.10.1. *Έστω ω_1, ω_2 δύο μιγαδικοί αριθμοί με $\Im(\omega_1/\omega_2) > 0$. Lattice Λ ονομάζεται η ελεύθερη προσθετική αβελιανή υποομάδα που παράγεται από τα ω_1, ω_2. Δηλαδή:*

$$\Lambda = \{n\omega_1 + m\omega_2, n, m \in \mathbb{Z}\}$$

Ορισμός 2.10.2. *Μια ελλειπτική συνάρτηση f στο lattice Λ είναι μία μερόμορφη συνάρτηση στο $\mathbb{C}$ που είναι Λ-περιοδική, δηλαδή:*

$$f(z + \omega) = f(z)$$

για κάθε $\omega \in \Lambda$. Συμβολίζουμε με $\mathbb{C}(\Lambda)$ το σώμα των ελλειπτικών συναρτήσεων που ορίζονται στο Λ. Το θεμελιώδες παραλληλόγραμμο D του Λ ως προς την βάση ω_1, ω_2 είναι το σύνολο

$$D = \{a\omega_1 + b\omega_2 : a, b \in [0, 1)\}.$$

Κάθε μεταφορά $D_u = D + u$ του D κατά $u \in \mathbb{C}$ ονομάζεται επίσης θεμελιώδες παραλληλόγραμμο του Λ. Παρατηρούμε ότι κάθε βάση επάγει και μια διαφορετική άπειρη οικογένεια θεμελιωδών παραλληλογράμμων για το lattice Λ. Επίσης, αν D είναι ένα θεμελιώδες παραλληλόγραμμο για το Λ, η απεικόνιση

$$D \longrightarrow \mathbb{C}/\Lambda$$

είναι 1-1 και επί. Συνηθίζουμε να ταυτίζουμε σαν σύνολο το D με το $\mathbb{C}/\Lambda$.

Ένα lattice $\mathbb{C}/\Lambda$ είναι συμπαγής επιφάνεια Riemann γένους 1. Αν μια $f \in \mathbb{C}(\Lambda)$ είναι ολόμορφη ή αν δεν έχει ρίζες, τότε είναι φραγμένη. Αυτό προκύπτει από το Θεώρημα του Liouville, επειδή η επιφάνεια Riemann $\mathbb{C}/\Lambda$ είναι συμπαγής. Κεντρική για την συνέχεια της μελέτης μας είναι η επόμενη πρόταση:

Θεώρημα 2.10.3. *Για κάθε $f \in \mathbb{C}(\Lambda)$ ισχύει ότι το άθροισμα των residues της f σε εάν παραλληλόγραμμο D είναι 0. Ομοίως, το άθροισμα των τάξεων των ριζών της f σε εάν παραλληλόγραμμο D είναι 0.*

Απόδειξη. Παρατηρείστε ότι επειδή η συνάρτηση είναι Λ-περιοδική, αρκεί να δείξουμε τα ζητούμενα για ένα θεμελιώδες παραλληλόγραμμο του Λ. Πιο συγκεκριμμένα, για τον πρώτο ισχυρισμό, εφαρμόζουμε τον τύπο για τα residues σε ένα θεμελιώδες παραλληλόγραμμο D:

$$\sum_{w \in \mathbb{C}/\Lambda} res_w(f) = \frac{1}{2\pi \mathrm{i}} \int_{\partial D} f(z)dz$$

και επειδή η f είναι Λ-περιοδική το άθροισμα είναι 0.

Εφαρμόζωντας τώρα το τον τύπο για τα residues σε ένα θεμελιώδες παραλληλόγραμμο D για την $f'(z)/f(z)$ αποδεικνύουμε και τον δεύτερο ισχυρισμό. □

Πρόταση 2.10.4. *Αν η f είναι μια ελλειπτική συνάρτηση για το lattice Λ, τότε*

$$\sum_{w\in\mathbb{C}/\Lambda} \mathrm{ord}_w(f)w \in \Lambda.$$

Ορισμός 2.10.5. *Τάξη μιας ελλειπτικής συνάντησης $f \in \mathbb{C}(\Lambda)$ είναι ο αριθμός των ριζών (ισοδύναμα, από το προηγούμενο θεώρημα, των πόλων) σε ένα θεμελιώδες παραλλλόγραμμο D του Λ, μετρώντας και τις πολλαπλότητες.*

Πρόταση 2.10.6. *Μια μη σταθερή ελλειπτική συνάρτηση έχει τάξη τουλάχιστον 2.*

Απόδειξη. Αν έχει απλό πόλο μόνο σε ένα σημείο, τότε, απ' το προηγούμενο θεώρημα το residue εκεί είναι 0, άρα η συνάρτηση είναι ολόμορφη, και άρα σταθερή. □

Με τον ίδιο τρόπο που ορίσαμε πριν divisor ομάδα για τις ελλειπτικές καμπύλες θα ορίσουμε τώρα και divisor ομάδα για lattices.

Ορισμός 2.10.7. *Έστω Λ ένα lattice. Η ομάδα των divisors του $\mathbb{C}/\Lambda$ είναι η ομάδα των τυπικών γραμμικών συνδυασμών*

$$\sum_{w\in\mathbb{C}/\Lambda} n_w(w)$$

όπου οι n_w είναι ακέραιοι και μόνο πεπερασμένοι εξ' αυτών δεν είναι ίσοι με μηδέν. Η ομάδα αυτή συμβολίζεται με $\mathrm{Div}(\mathbb{C}/\Lambda)$. Ως συνήθως, ο βαθμός ενός divisor $D = \sum n_w(w)$ ορίζεται να είναι το άθροισμα

$$\deg D = \sum n_w$$

και το σύνολο των divisors βαθμού 0 είναι υποομάδα της $\mathrm{Div}(\mathbb{C}/\Lambda)$ η οποία συμβολίζεται με $\mathrm{Div}^0(\mathbb{C}/\Lambda)$.

Αν μια $f \in \mathbb{C}(\Lambda)^*$, ο divisor της είναι ο

$$\mathrm{div}(f) = \sum_{w\in\mathbb{C}/\Lambda} \mathrm{ord}_w(f)(w).$$

Από την θεώρημα 2.10.3 έπεται πως ο divisor μιας μη μηδενικής ελλειπτικής f είναι μηδενικός. Η απεικόνιση:

$$\mathrm{div} : \mathbb{C}(\Lambda)^* \longrightarrow \mathrm{Div}^0(\mathbb{C}/\Lambda)$$

είναι ομομορφισμός. Ορίζουμε την συνάρτηση άθροισης

$$S : \mathrm{Div}^0(\mathbb{C}/\Lambda) \longrightarrow \mathbb{C}/\Lambda$$

με

$$S\left(\sum n_w(w)\right) = \sum n_w(w)(\mathrm{mod}\Lambda).$$

Πρόταση 2.10.8. *Η ακολουθία*

$$1 \longrightarrow \mathbb{C}^* \longrightarrow \mathbb{C}(\Lambda)^* \longrightarrow \mathrm{Div}^0(\mathbb{C}/\Lambda) \longrightarrow \mathbb{C}/\Lambda \longrightarrow 0$$

είναι ακριβής. (όπου η τρίτη απεικόνιση είναι η div *και η τέταρτη είναι η S).*

Τα πηλίκα των lattices είναι επιφάνειες Riemann γένους 1, άρα και αλγεβρικές καμπύλες γένους 1 (θεώρημα 3.2.16 παρακάτω), όπως επίσης και οι ελλειπτικές καμπύλες. Η ιδέα λοιπόν είναι ότι κάθε lattice πρέπει να αντιστοιχεί σε μια ελλειπτική καμπύλη (τουλάχιστον μια καμπύλη που να ορίζεται πάνω από το $\mathbb{C}$) και το αντίστροφο. Η ιδέα αυτή είναι σωστή, και στόχος μας σε αυτή την παράγραφο είναι να δούμε πως γίνεται αυτή η ταύτιση. Σκοπός μας είναι, αφ΄ ενός, να κατασκευάσουμε μη σταθερές ελλεπτικές συναρτήσεις, αφ΄ ετέρου οι συναρτήσεις αυτές μας να μας προσφέρουν μια σύνδεση των πηλίκων $\mathbb{C}/\Lambda$ με τις ελλειπτικές καμπύλες.

Η κατασκευή αυτή οφείλεται στον Weierstrass. Η ιδέα της θεώρησης του Weierstrass έγκειται στον ορισμό μιας κατάλληλης ελλειπτικής συνάρτησης $\wp$ πάνω από το Λ. Οι ελλειπτικές συναρτήσεις είναι ουσιαστικά γενίκευση των εκθετικών και των τριγωνομετρικών συναρτήσεων. Αυτό συμβαίνει επειδή οι τριγωνομετρικές είναι περιοδικές ως προς την πραγματική διεύθυνση στο $\mathbb{C}$, ενώ η εκθετική είναι περιοδική στην κατεύθυνση του i. Άρα οι διπλά περιοδικές συναρτήσεις (δηλαδή οι ελλειπτικές), θα πρέπει να κληρονομούν ιδιότητες και των δύο. Πιο συγκεκριμμένα, θα δούμε πως ξεχωριστό ενδιαφέρον έχει η διαφορική εξίσωση που έχει σαν λύση την $\wp$.

Ορισμός 2.10.9. *Η $\wp$-συνάρτηση του Weierstrass για το Λ είναι η*

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

Ορίζουμε επίσης τις σειρές Eisenstein:

$$G_{2k}(\Lambda) = \sum_{\omega\in\Lambda,\omega\neq 0} \omega^{-2k}$$

Πρόταση 2.10.10. *Έστω Λ ένα lattice του $\mathbb{C}$. Τότε:*

(i) *Οι σειρές Eisenstein $G_{2k}(\Lambda)$ συγκλίνουν απόλυτα για κάθε $k \geq 2$.*

(ii) *Η σειρά της συνάρτησης Weierstrass συγκλίνει απόλυτα και ομοιόμορφα στα συμπαγή υποσύνολα του $\mathbb{C} - \Lambda$. Η συνάρτηση $\wp$ έχει πόλους τάξης 2 με residue 0 στα σημεία του lattice Λ, και παντού αλλού είναι ολόμορφη.*

(iii) *Η συνάρτηση $\wp$ είναι μια άρτια ελλειπτική συνάρτηση στο Λ.*

Απόδειξη. (i) Αφού το Λ είναι διακριτό στο $\mathbb{C}$, υπάρχει μια σταθερά $c = c(\Lambda)$ τέτοια ώστε για κάθε $n \geq 1$, για το σύνολο $\{\omega \in \Lambda : n \leq |\omega| < n+1\}$ να ισχύει:

$$|\{\omega \in \Lambda : n \leq |\omega| < n+1\}| < cn.$$

Άρα, παίρνουμε

$$\sum_{\omega\in\Lambda,|\omega|\geq 1} \frac{1}{|\omega|^{2k}} \leq \sum_{n=1}^{\infty} \frac{|\{\omega \in \Lambda : n \leq |\omega| < n+1\}|}{n^{2k}} < \sum_{n=1}^{\infty} \frac{c}{n^{2k-1}} < \infty$$

(ii) Αν $|\omega| > 2|z|$, τότε

$$\left| \frac{1}{(z-\omega)^2} - \frac{1}{(\omega)^2} \right| \leq \frac{10|z|}{|\omega|^2}.$$

Από το πρώτο ερώτημα, έπεται πως η $\wp(z)$ συγκλίνει απολύτως για κάθε $z \in \mathbb{C} - \Lambda$, και συγκλίνει ομοιόμορφα σε κάθε συμπαγές υποσύνολο του $\mathbb{C} - \Lambda$. Άρα η σειρά ορίζει μια ολόμορφη συνάρτηση στο $\mathbb{C} - \Lambda$. Είναι τώρα προφανές πως η $\wp$ έχει έναν διπλό πόλο με residue 0 σε κάθε σημείο του Lattice.

(iii) Βάζοντας όπου ω το $-\omega$ παρατηρούμε ότι $\wp(z) = \wp(-z)$. Άρα η $\wp$ είναι άρτια. Για να δείξουμε ότι είναι ελλειπτική, καταρχάς παραγωγίζουμε κατά όρο την σειρά που ορίζει την $\wp$ (μπορούμε να το κάνουμε εξ΄ αιτίας της ομοιόμορφης σύγκλισης από το (ii)):

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

Ο τύπος αυτός μας δίνει ότι η $\wp'$ είναι ελλειτπική, άρα

$$\wp'(z+\omega) = \wp'(z).$$

Ολοκληρώνοντας συνάγουμε την σχέση

$$\wp(z+\omega) = \wp(z) + c(\omega)$$

όπου το $c(\omega)$ είναι ανεξάρτητο του z. Αντικαθιστώντας όπου z το $-\frac{1}{2}\omega$ και χρησιμοποιώντας το γεγονός ότι η $\wp$ είναι άρτια, συμπεραίνουμε ότι $c(\omega) = 0$, άρα η $\wp$ είναι ελλειπτική.

□

Το επόμενο θεώρημα είναι ένα αναλυτικό ανάλογο της παρατήρησης που κάναμε στην διαδικασία της απόδειξης του θεωρήματος 2.4.1 πως για μια E/K ισχύει $K(E) = K(x, y)$ (όπου $[K(E) : K(x)] = 2$ και $[K(E) : K(y)] = 3$).

Θεώρημα 2.10.11. *Για κάθε lattice Λ του $\mathbb{C}$ ισχύει:*

$$\mathbb{C}(\Lambda) = \mathbb{C}(\wp(z), \wp'(z))$$

Απόδειξη. Έστω $f \in \mathbb{C}(\Lambda)$. Επειδή η f γράφεται σαν άθροισμα μιας άρτιας και μιας περιττής συνάρτησης, αρκεί να αποδείξουμε το ζητούμενο για αυτές. Επίσης, αν η $f(z)$ είναι περιττή, η $f(z)\wp'(z)$ είναι άρτια. Άρα, αρκεί να το δείξουμε μόνο για τις άρτιες.

Αφού η f είναι άρτια, έχουμε

$$\mathrm{ord}_w(f) = \mathrm{ord}_{-w}(f)$$

για κάθε $w \in \mathbb{C}$. Παραγωγίζοντας διαδοχικά την σχέση $f(z) = f(-z)$ παίρνουμε ότι αν $2\omega \in \Lambda$, τότε η $\mathrm{ord}_w f$ είναι άρτια.

Θεωρούμε το H που είναι μια θεμελιώδης περιοχή για το $(\mathbb{C}/\Lambda)/\{\pm 1\}$. Ισοδύναμα, διαλέγουμε το H ώστε να ισχύει

$$\mathbb{C} = (H + \Lambda) \cup (-H + \Lambda).$$

Από τα παραπάνω έπεται ότι ο divisor της f είναι της μορφής

$$\sum_{w \in H} n_w((w) + (-w)).$$

Ορίζουμε την συνάρτηση

$$g(z) = \prod_{\omega \in H - \{0\}} (\wp(z) - \wp(\omega))^{n_\omega}.$$

Ο divisor της $\wp(z) - \wp(\omega)$ είναι ο $(\omega) + (-\omega) - 2(0)$, άρα οι f και g έχουν τις ίδιες ρίζες και τους ίδιους πόλους εκτός ίσως από το $w = 0$. Το θεώρημα 2.10.3 μας λέει ότι έχουν ακριβώς την ίδια τάξη και στο 0. Δηλαδή η συνάρτηση $f(z)/g(z)$ είναι μια ολόμορφη ελλειπτική συνάρτηση στο Λ, και άρα είναι σταθερή. Άρα

$$f(z) = cg(z) \in \mathbb{C}(\wp(z), \wp'(z))$$

και έχουμε το ζητούμενο. □

Ορίζουμε τώρα μια δεύτερη συνάρτηση που εισήγαγε ο Weierstrass, και παραθέτουμε κάποιες χρήσιμες ιδιότητες της.

Ορισμός 2.10.12. *Η σ-συνάρτηση του Weierstrass για το Λ είναι η*

$$\sigma(z; \Lambda) = z \prod_{\omega \in \Lambda, \omega \neq 0} \left(1 - \frac{z}{\omega}\right) e^{z/\omega + \frac{1}{2}(z/\omega)^2}$$

Λήμμα 2.10.13 (ιδιότητες της συνάρτησης σ)**.** (i) *Το γινόμενο της σ ορίζει μια ολόμορφη συνάρτηση στο $\mathbb{C}$, η οποία έχει απλές ρίζες σε κάθε $z \in \Lambda$ και καμία άλλη ρίζα.*

(ii)
$$\frac{d^2}{dz^2} \log \sigma(z) = -\wp(z)$$
για κάθε $z \in \mathbb{C} - \Lambda$.

(iii) *Για κάθε $\omega \in \Lambda$ υπάρχουν σταθερές a και b στο $\mathbb{C}$, οι οποίες εξαρτώνται μόνο από το ω, τέτοιες ώστε*
$$\sigma(z + \omega) = e^{az+b}\sigma(z)$$
για κάθε $z \in \mathbb{C}$.

Λήμμα 2.10.14. *Έστω $n_1, n_2, ...n_r \in \mathbb{Z}$ και $z_1, z_2, ..., z_r \in \mathbb{C}$ τέτοιοι ώστε*

$$\sum n_i = 0$$

και

$$\sum n_i z_i \in \Lambda.$$

Τότε υπάρχει ελλειπτική συνάρτηση $f(z)$ για το Λ τέτοια ώστε

$$\mathrm{div}(f) = \sum n_i(z_i)$$

Επιπλέον, αν διαλέξουμε τα n_i και z_i ώστε να ικανοποιούν την σχέση

$$\sum n_i z_i = 0,$$

τότε μπορούμε να επιλέξουμε για f την

$$f(z) = \prod \sigma(z - z_i)^{n_i}.$$

Πρόταση 2.10.15. *Η σειρά Laurent της $\wp(z)$ στο $z = 0$ δίνεται από τον τύπο*

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

Απόδειξη. Για κάθε $|z| < |\omega|$ έχουμε

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

Αντικαθιστούμε τον παραπάνω τύπο στην σειρά της $\wp(z)$ και επειδή αυτή συγκλίνει ομοιόμορφα εναλλάσουμε σειρά άθροισης για να πάρουμε το ζητούμενο. □

Μπορούμε τώρα να αποδείξουμε την εξής διαφορική εξίσωση που ικανοποιούν οι $\wp$, $\wp'$:

Θεώρημα 2.10.16. *Για κάθε $z \in \mathbb{C} - \Lambda$ ισχύει*

$$\wp'(z)^2 = 4\wp(z)^3 - 60G_4\wp(z) - 140G_6.$$

Απόδειξη. Γράφουμε τους πρώτους όρους των συντελεστών Laurent των $\wp'(z)^2$, $\wp(z)^3$, $\wp(z)$:

$$\begin{aligned}
\wp'(z)^2 &= \frac{4}{z^6} - \frac{24G_4}{z^2} - 80G_6 + \ldots \\
\wp(z)^3 &= \frac{1}{z^6} + \frac{9G_4}{z^2} - 15G_6 + \ldots \\
\wp(z) &= \frac{1}{z^2} + 3G_4z^2 + \ldots
\end{aligned}$$

Συγκρίνοντας αυτές τις σχέσεις, βλέπουμε ότι η συνάρτηση

$$f(z) = \wp'(z)^2 - 4\wp(z)^3 + 60G_4\wp(z) + 140G_6$$

είναι ολόμορφη στο $z = 0$ και $f(0) = 0$. Αλλά η f είναι ελλειπτική στο Λ, άρα η f είναι μια ολόμορφη ελλειπτική συνάρτηση στο Λ. Έπεται πως η f είναι σταθερή, και αφού $f(0) = 0$ συμπεραίνουμε πως $f \equiv 0$. □

Αν έχουμε μια ελλειπτική καμπύλη E πάνω από το $\mathbb{C}$ με εξίσωση Weierstrass

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

τότε το μετασχηματισμός

$$(x, y) \longrightarrow (4x, 4y)$$

μας δίνει μια εξίσωση για την E της μορφής

$$E : y^2 = 4x^3 + Ax + B$$

Αν τώρα χρησιμοποιήσουμε τον συνήθη συμβολισμό

$$g_2 = g_2(\Lambda) = 60G_4(\Lambda), g_3 = g_3(\Lambda) = 140G_6(\Lambda)$$

τότε η εξίσωση του θεωρήματος 2.10.16 γράγεται ως

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3.$$

Την παρατήρηση αυτήν εκμεταλλευόμαστε για να δείξουμε τα επόμενα θεωρήματα.

Ξέρουμε ακόμη ότι αν η $E/\mathbb{C}$ είναι μια ελλειπτική καμπύλη, τότε η πράξη της ομάδας ορίζεται τοπικά από ρητές συναρτήσεις. Άρα, η $E = E(\mathbb{C})$ είναι μια μιγαδική ομάδα Lie, δηλαδή μια μιγαδική πολλαπλότητα εφοδιασμένη με δομή ομάδας της οποίας η πράξη δίνεται τοπικά από μιγαδικές αναλυτικές συναρτήσεις.

Ομοίως, αν το Λ είναι ένα lattice στο $\mathbb{C}$, το πηλίκο $\mathbb{C}/\Lambda$ με την επαγόμενη πράξη της πρόσθεσης, είναι μια μιγαδική ομάδα Lie.

Θεώρημα 2.10.17. *Έστω οι $g_2 = g_2(\Lambda)$ και $g_3 = g_3(\Lambda)$ όπως ορίστηκαν πριν. Τότε:*

(i) *Το πολυώνυμο*

$$f(x) = 4x^3 - g_2x - g_3$$

έχει διακριτές ρίζες, κι άρα

$$\Delta(\Lambda) = g_2^3 - 27g_3^2 \neq 0.$$

(ii) *Έστω $E/\mathbb{C}$ η ελλειπτική καμπύλη*

$$y^2 = 4x^3 - g_2x - g_3$$

(παρατηρούμε ότι η καμπύλη αυτή είναι όντως ελλειπτική εξ΄ αιτίας του ερωτήματος (i)). Τότε η απεικόνιση

$$\phi : \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C})$$

με

$$\phi(z) = [\wp(z), \wp'(z), 1]$$

είναι μιγαδικά αναλυτικός ισομορφισμός μιγαδικών ομάδων Lie, δηλαδή ένας ισομορφισμός επιφανειών Riemann που είναι και ομομορφισμός ομάδων.

Ας σημειώσουμε εδώ πως στο επόμενο κεφάλαιο θα μιλήσουμε αναλυτικά για τις επιφάνειες Riemann. Προς το παρόν, χρησιμοποιούμε εδώ όσα στοιχεία της θεωρίας τους μας χρειάζονται για την διατύπωση και την απόδειξη των θεωρημάτων που σχετίζονται με τις ελλειπτικές καμπύλες.

Απόδειξη. (i) Διαλέγουμε μια βάση $\{\omega_1, \omega_2\}$ για το Λ και θέτουμε $\omega_3 = \omega_1 + \omega_2$. Η $\wp'(z)$ είναι περιττή ελλειπτική συνάρτηση, άρα

$$\wp'\left(\frac{\omega_i}{2}\right) = -\wp'\left(\frac{-\omega_i}{2}\right) = -\wp'\left(\frac{\omega_i}{2}\right),$$

άρα $\wp'(\omega_i/2) = 0$. Άρα το $f(x)$ μηδενίζεται στα τρία σημεία $\wp(\omega_i/2)$, $i = 1, 2, 3$. Για να δείξουμε το ζητούμενο, αρκεί να δείξουμε ότι αυτά τα τρία σημεία ειναι διαφορετικά μεταξύ τους.

Η συνάρτηση

$$\wp(z) - \wp\left(\frac{\omega_i}{2}\right)$$

είναι άρτια, άρα έχει τουλάχιστον μια διπλή ρίζα στο $z = \omega_i/2$. Είναι όμως και ελλειπτική συνάρτηση τάξης 2, άρα υπάρχει ένα θεμελιώδες παραλληλόγραμμο D για το Λ ώστε εκεί αυτές να είναι όλες οι ρίζες της f. Άρα, για $i \neq j$ έχουμε $\wp(\omega_i/2) \neq \wp(\omega_j/2)$.

(ii) Προφανώς, από το θεώρημα 2.10.16, $\mathrm{Im}(\phi) \subset E(\mathbb{C})$. Έστω τώρα ένα $(x, y) \in E(\mathbb{C})$. Η συνάρτηση $\wp(z) - x$ είναι μη σταθερή ελλειπτική συνάρτηση, άρα έχει μια ρίζα, έστω για $z = a$. Από την σχέση $\wp'(a)^2 = y^2$, και βάζοτας όπου a το $-a$, παίρνουμε $\wp'(a) = y$. Έτσι παίρνουμε $\phi(a) = (x, y)$.

Για να δείξουμε ότι η ϕ είναι 1-1, ας υποθέσουμε ότι $\phi(z_1) = \phi(z_2)$.

Αν $2z_1 \notin \Lambda$, τότε η $\wp(z) - \wp(z_1)$ είναι ελλειπτική συνάρτηση τάξης 2 που μηδενίζεται στα z_1, $-z_1$, z_2. Έπεται πως, αναγκαστικά, δύο από τις τρεις αυτές τιμές ταυτίζονται modulo Λ. Εξ' υποθέσεως τα z_1 και $-z_1$ δεν είναι ισοδύναμα modulo Λ, άρα $z_2 \equiv z_1 \pmod{\Lambda}$ ή $z_2 \equiv -z_1 \pmod{\Lambda}$. Επειδή όμως

$$\wp'(z_1) = \wp'(z_2) = \wp'(\pm z_1) = \pm\wp'(z_1)$$

και $\wp'(z_1) \neq 0$ έπεται πως $z_2 \equiv z_1 \pmod{\Lambda}$. Αν $2z_1 \in \Lambda$, τότε η $\wp(z) - \wp(z_1)$ έχι διπλή ρίζα στο z_1 και ρίζα στο z_2, άρα πάλι συμπεραίνουμε ότι $z_2 \equiv z_1 \pmod{\Lambda}$ και η απόδειξη πως η ϕ είναι 1-1 είναι πλήρης.

Θα δείξουμε τώρα ότι είναι ισομορφισμός ομάδων Lie. Σε κάθε σημείο της $E(\mathbb{C})$, η διαφορική μορφή dx/dy είναι ολόμορφη και nonvanishing. Για την εικόνα της μέσω της ϕ^* έχουμε:

$$\phi^*\left(\frac{dx}{dy}\right) = \frac{d\wp(z)}{\wp'(z)} = dz$$

η οποία είναι επίσης ολόμορφη και nonvanishing σε κάθε σημεία του $\mathbb{C}/\Lambda$, δηλαδή η ϕ είναι τοπικά αναλυτικός ισομορφισμός, και το ότι η ϕ είναι επί μας δίνει ότι είναι global ισομορφισμός.

Για να δείξουμε ότι η ϕ είναι ομομορφισμός ομάδων, θεωρούμε δύο σημεία z_1 και z_2 στο $\mathbb{C}$ και, εφαρμόζωντας το λήμμα 2.10.14, βρίσκουμε μια f ελλειπτική στο Λ με divisor

$$\mathrm{div}(f) = (z_1 + z_2) - (z_1) - (z_2) + (0).$$

Αφού $\mathbb{C}(\Lambda) = \mathbb{C}(\wp(z), \wp'(z))$ (θεώρημα 2.10.11), υπάρχει μια $F = F(X, Y)$ στο $\mathbb{C}(X, Y)$, με $f(z) = F(\wp(z), \wp'(z))$. Θεωρούμε την $F(x, y)$ ως στοιχεία του $\mathbb{C}(x, y)$ και υπολογίζουμε

$$\mathrm{div}(F) = (\phi(z_1 + z_2)) + (\phi(z_1)) + (\phi(z_2)) + (\phi(0)).$$

Από το λήμμα 2.4.2 έχουμε πως

$$\phi(z_1 + z_2) = \phi(z_1) + \phi(z_2)$$

και η απόδειξη πως η ϕ είναι ομομορφισμός ομάδων είναι πλήρης.

□

Έστω τώρα δύο lattices Λ_1 και Λ_2 στο $\mathbb{C}$. Έστω ακόμα ένας μιγαδικός αριθμός α τέτοιος ώστε $\alpha\Lambda_1 \subset \Lambda_2$. Τότε, η απεικόνιση «πολλαπλασιασμός επί α»:

$$\phi_\alpha : \mathbb{C}/\Lambda_1 \longrightarrow \mathbb{C}/\Lambda_2$$

με τύπο

$$\phi_\alpha(z) = \alpha z (\mathrm{mod} \Lambda_2)$$

είναι καλά ορισμένη, ολόμορφη και ομομορφισμός. Στην πραγματικότητα, υπάρχουν πολλά περισσότερα πράγματα που μπορούμε να πούμε για αυτήν την απεικόνιση:

Θεώρημα 2.10.18. (i) *Η αντιστοίχιση $\alpha \mapsto \phi_\alpha$ που ορίστηκε παραπάνω από το σύνολο των μιγαδικών αριθμών α με την ιδιότητα $\alpha\Lambda_1 \subset \Lambda_2$ στο σύνολο των ολόμορφων απεικονίσεων*

$$\phi : \mathbb{C}/\Lambda_1 \longrightarrow \mathbb{C}/\Lambda_2$$

με την ιδιότητα $\phi(0) = 0$, είναι 1-1 και επί.

(ii) *Έστω δύο ελλειπτικές καμπύλες E_1 και E_2 οι οποίες αντιστοιχούν στα lattices Λ_1 και Λ_2 αντίστοιχα, σύμφωνα με την απεικόνιση που ορίσαμε στο ερώτημα (ii) του θεωρήματος 2.10.17. Τότε ο φυσικός εγκλεισμός από τις ισογένειες $\phi : E_1 \to E_2$ στο σύνολο των ολόμορφων απεικονίσεων*

$$\phi : \mathbb{C}/\Lambda_1 \longrightarrow \mathbb{C}/\Lambda_2$$

με την ιδιότητα $\phi(0) = 0$, είναι 1-1 και επί.

Απόδειξη. (i) Έστω $\phi_\alpha = \phi_\beta$. Τότε

$$\alpha z \equiv \beta z (\mod \Lambda_2)$$

για κάθε z στο $\mathbb{C}$, δηλαδή, η απεικόνιση $z \to (\alpha - \beta)z$ στέλνει το $\mathbb{C}$ στο Λ_2, το οποίο είναι διακριτό. Άρα η απεικόνιση είναι σταθερή, δηλαδή $\alpha = \beta$.

Για να δείξουμε ότι η αντιστοίχιση είναι επί, θεωρούμε μια ολόμορφη απεικόνιση $\phi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2$ με $\phi(0) = 0$ και θα βρούμε έναν μιγαδικό αριθμό α τέτοιον ώστε $\alpha\Lambda_1 \subset \Lambda_2$ και $\phi = \phi_\alpha$.

Αφού το $\mathbb{C}$ είναι απλά συννεκτικό, η ϕ ανυψώνεται σε μια $f : \mathbb{C} \to \mathbb{C}$ με $f(0) = 0$ τέτοια ώστε, αν $p_i : \mathbb{C} \to \mathbb{C}/\Lambda_i$ η φυσική προβολή, να ισχύει

$$\phi \circ p_1 = p_2 \circ f$$

Συμπεραίνουμε πως θα πρέπει να ισχύει

$$f(z + \omega) \equiv f(z) (\mod \Lambda_2)$$

για κάθε $\omega \in \Lambda_1$ και για κάθε z στο $\mathbb{C}$. Χρησιμοποιώντας και πάλι ότι το Λ_2 είναι διακριτό, συμπεραίνουμε πως η διαφορά $f(z+\omega)-f(z)$ είναι ανεξάρτητη του z. Άρα $f'(z+\omega) = f'(z)$ για κάθε $\omega \in \Lambda_1$ και για κάθε z στο $\mathbb{C}$. Δηλαδή η f' είναι ολόμορφη ελλειπτική καμπύλη, άρα είναι σταθερή, το οποίο σημαίνει πως υπάρχουν μιγαδικοί α και γ τέτοιοι ώστε $f(z) = \alpha z+\gamma$. Όμως $f(0) = 0$ άρα $\gamma = 0$. Επειδή $f(\Lambda_1) \subset \Lambda_2$, συνεπάγεται πως $\alpha\Lambda_1 \subset \Lambda_2$. Άρα ο αριθμός α ικανοποιεί τις συνθήκες που θέλαμε, δηλαδή $\phi = \phi_\alpha$.

(ii) Αφού μια ισογένεια είναι μορφισμός, η απεικόνιση που επάγεται μεταξύ των αντίστοιχων μιγαδικών τόρων είναι ολόμορφη. Έπεται πως η αντιστοίχιση από το $\mathrm{Hom}(E_1, E_2)$ στις ολόμορφες από το $\mathbb{C}/\Lambda_1$ στο $\mathbb{C}/\Lambda_2$ με την ζητούμενη ιδιότητα είναι καλά ορισμένη, και προφανώς είναι 1-1.

Για να δείξουμε ότι είναι επί, από το ερώτημα (i) αρκεί να επιλέξουμε μια απεικόνιση της μορφής ϕ_α, με $\alpha \in \mathbb{C}^*$ και τέτοιον ώστε $\alpha\Lambda_1 \subset \Lambda_2$, και να βρούμε μια ισογένεια $E_1 \to E_2$ που να αντιστοιχεί στον α.

Δοθέντος τέτοιου α λοιπόν, ορίζουμε απεικόνιση $E_1 \to E_2$:

$$[\wp(z, \Lambda_1), \wp'(z, \Lambda_1), 1] \longrightarrow [\wp(\alpha z, \Lambda_2), \wp'(\alpha z, \Lambda_2), 1].$$

Για να ολόκληρώσουμε την απόδειξη, πρέπει να δείξουμε ότι οι $\wp(\alpha z, \Lambda_2)$ και $\wp'(\alpha z, \Lambda_2)$ είναι ρητές εκφράσεις των $\wp(z, \Lambda_1)$ και $\wp'(z, \Lambda_1)$. Χρησιμοποιώντας ότι $\alpha\Lambda_1 \subset \Lambda_2$ βλέπουμε ότι για κάθε $\omega \in \Lambda_1$

$$\wp(\alpha(z + \omega), \Lambda_2) = \wp(\alpha z + \alpha\omega, \Lambda_2) = \wp(\alpha z, \Lambda_2)$$

και ομοίως για το $\wp'(\alpha z, \Lambda_2)$:

$$\wp'(\alpha(z + \omega), \Lambda_2) = \wp'(\alpha z + \alpha\omega, \Lambda_2) = \wp'(\alpha z, \Lambda_2).$$

Οι σχέσεις αυτές μας δίνουν ότι τα $\wp(\alpha z, \Lambda_2)$ και $\wp'(\alpha z, \Lambda_2)$ ανήκουν στο $\mathbb{C}(\Lambda_1)$, και το ζητούμενο έπεται από το θεώρημα 2.10.11.

□

Άμεσο πόρισμα του προηγούμενου θεωρήματος είναι το εξής

Πόρισμα 2.10.19. *Έστω δύο ελλειπτικές καμπύλες E_1 και E_2 που ορίζονται πάνω από το $\mathbb{C}$ και δύο lattices Λ_1, Λ_2 που αντιστοιχούν σε αυτές, σύμφωνα με το θεώρημα 2.10.17. Τότε, οι E_1, E_2 είναι ισόμορφες πάνω από το $\mathbb{C}$, αν και μόνο αν υπάρχει $\alpha \in \mathbb{C}^*$ ώστε $\Lambda_1 = \alpha\Lambda_2$ (σε αυτήν την περίπτωση, τα Λ_1 και Λ_2 λέγονται ομοιόθετα).*

Το τελευταίο μιας σειράς ενδιαμέσων αποτελεσμάτων που μας χρειάζονται για να δείξουμε το κεντρικό θεώρημα είναι το γνωστό

Θεώρημα 2.10.20 (Uniformization Ελλειπτικών Καμπυλών)**.** *Έστω A και B δύο μιγαδικοί αριθμοί τέτοιο ώστε*

$$4A^3 - 27B^2 \neq 0.$$

Τότε υπάρχει μοναδικό lattice $\Lambda \subset \mathbb{C}$ τέτοιο ώστε $g_2(\Lambda) = A$ και $g_3(\Lambda) = B$.

Η απόδειξη του θεωρήματος αυτού δεν είναι δύσκολη, και θα την δώσουμε παρακάτω, ως συνέπεια των ιδιοτήτων της modular συνάρτησης $j(z)$.

Προς το παρόν, για να εκτιμήσουμε την δύναμη των παραπάνω αποτελεσμάτων, δίνουμε ως πόρισμα τους το βασικό αποτέλεσμα στο οποίο στοχεύαμε. Η απόδειξη του είναι άμεση από τα θεωρήματα 2.10.17,2.10.18 και 2.10.20.

Θεώρημα 2.10.21. *Έστω $E/\mathbb{C}$ μια ελλειπτική καμπύλη. Τότε, υπάρχει ένα, μοναδικό ως προς ομοιοθεσία, lattice Λ του $\mathbb{C}$ και ένας μιγαδικός αναλυτικός ισομορφισμός*

$$\phi : \mathbb{C}/\Lambda \longrightarrow E(\mathbb{C})$$

$$\phi(z) = [\wp(z, \Lambda), \wp'(z, \Lambda), 1]$$

μιγαδικών ομάδων Lie.

Μεγάλη σημασία έχει επίσης η αντίστροφη απεικόνιση της ϕ. Για μια εκτενέστερη συζήτηση πάνω σε αυτήν παραπέμπουμε στο [Silverman, [30], κεφ.6]. Παρατηρείστε ότι το επόμενο θεώρημα έπεται άμεσα από τα παραπάνω:

Θεώρημα 2.10.22. *Οι ακόλουθες τρεις κατηγορίες είναι ισοδύναμες:*

(i) *Η κατηγορία με αντικείμενα τις Ελλειπτικές καμπύλες πάνω από το $\mathbb{C}$ και απεικονίσεις τις ισογένειες.*

(ii) *Η κατηγορία με αντικείμενα τις Ελλειπτικές καμπύλες πάνω από το $\mathbb{C}$ και απεικονίσεις τις μιγαδικά αναλυτικές απεικονίσεις που διατηρούν το O.*

(iii) *Η κατηγορία με αντικείμενα τα lattices Λ του $\mathbb{C}$ (μέχρις ομοιοθεσίας) και απεικονίσεις τα $\{\alpha \in \mathbb{C} : \alpha\Lambda_1 \subset \Lambda_2\}$.*

Στην πρόταση 2.5.16 δείξαμε ότι ο μορφισμός $[m] : E \to E$ έχει βαθμό m^2, και στο θεώρημα 2.6.1 δείξαμε ότι, ως αβελιανές ομάδες:

$$E[m] \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \times \frac{\mathbb{Z}}{m\mathbb{Z}}.$$

Τώρα, που έχουμε αποδείξει οτι μια ελλειπτική καμπύλη $E/\mathbb{C}$ είναι ισόμορφη με ένα lattice $\mathbb{C}/\Lambda$, παίρνουμε ξανά τα αποτελέσματα αυτά για το $\mathbb{C}$ ως άμεσα πορίσματα. Στην πραγματικότητα, υπάρχει μια γενικότερη αρχή, η οποία, πολύ αδρά, λέει ότι

Θεώρημα 2.10.23 (Η Αρχή του Lefschetz)**.** *Η αλγεβρική γεωμετρία πάνω από ένα αλγεβρικά κλειστό σώμα K χαρακτηριστικής 0 είναι «η ίδια» με την αλγεβρική γεωμετρία πάνω από το $\mathbb{C}$.*

Για παράδειγμα, χρημοποιώντας την Αρχή του Lefschetz, μπορεί κανείς να αποδείξει ότι αν το αλγερικά κλειστό σώμα K έχει χαρακτηριστική 0 και η E ορίζεται πάνω από το K, τότε ο $\mathrm{End}(E)$ είναι ισόμορφος είτε με το $\mathbb{Z}$ είτε με έναν order ενός μιγαδικού τετραγωνικού σώματος αριθμών K. Η Αρχή του Lefschetz μας λέει ότι για να το δείξουμε αυτό το αποτέλεσμα, «αρκεί» να το δείξουμε για το $\mathbb{C}$. Το αποτέλεσμα αυτό θα το δείξουμε παρακάτω, στην παράγραφο 2.11. Πριν κλείσουμε αυτήν την παράγραφο όμως, δίνουμε την περιγραφή της $E(\mathbb{R})$:

Θεώρημα 2.10.24. *Έστω μια ελλειπτική καμπύλη E που ορίζεται πάνω από το $\mathbb{R}$.*

(i) *Αν η διακρίνουσα Δ της E είναι αρνητική, τότε*

$$E(\mathbb{R}) \cong \frac{\mathbb{R}}{\mathbb{Z}} \cong S^1$$

(ii) *Αν η Δ είναι θετική, τότε*

$$E(\mathbb{R}) \cong \frac{\mathbb{R}}{\mathbb{Z}} \times \frac{\mathbb{Z}}{2\mathbb{Z}} \cong S^1 \times C_2$$

Θα παραλείψουμε την αυστηρή απόδειξη, αλλά δίνουμε έναν διαισθητικό επιχείρημα που εξηγεί την ιδέα, τουλάχιστον στην περίπτωση που $\Delta < 0$.

Αν $\Delta < 0$, τότε η $E(\mathbb{R})$ ως υποσύνολο του $\mathbb{R}$ είναι συνεκτική. Προφανώς είναι συμπαγής, αφού περιέχει το επ΄ άπειρον σημείο, και η πράξη της πρόσθεσης είναι συνεχής. Άρα η $E(\mathbb{R})$ είναι μια μονοδιάστατη ομάδα Lie. Όμως, υπάρχει, μέχρις ισομορφισμού, μόνο μια μονοδιάσταση ομάδα Lie, η S^1.

Είδαμε λοιπόν την δομή που έχουν οι ομάδες $E(\mathbb{C})$ και $E(\mathbb{R})$, μέχρις ισομορφισμού. Η γνώση της δομής της $E(\mathbb{C})$ είναι πολύ σημαντικό εργαλείο. Για παράδειγμα, παρατηρούμε ότι για κάθε lattice του $\mathbb{C}$ μπορούμε να επιλέξουμε (μοναδική) βάση της μορφής $\{z, 1\}$ με $\Im(z) > 0$ (αν $\{\omega_1, \omega_2\}$ είναι μια βάση του Λ, μπορούμε να επιλέξουμε σαν z το ω_1/ω_2). Άρα, σε κάθε καμπύλη E πάνω από τους μιγαδικούς αριθμούς αντιστοιχεί ένας z στο άνω μιγαδικό ημιεπίπεδο. Συμβολίζουμε την E με E_z. Αντίστροφα, κάθε z στο άνω μιγαδικό ημιεπίπεδο το αντιστοιχούμε στο lattice με βάση $\{z, 1\}$, το οποίο αντιστοιχεί σε μια ελλειπτική καμπύλη πάνω από τους μιγαδικούς αριθμούς. Η ταύτιση αυτή παίζει πολύ σημαντικό ρόλο στην σκέψη για το πως πρέπει να προχωρήσει η μελέτη μας · φαίνεται να υπάρχει ουσιώδης λόγος να στραφούμε στην μελέτη του άνω μιγαδικού ημιεπιπέδου $\mathbb{H}$. Επίσης, οι συναρτήσεις

$$G_{2k}(z) = G_{2k}(E_z)$$

$$\Delta(z) \equiv \Delta(E_z)$$

και

$$j(z) \equiv j(E_z)$$

ορίζονται στο $\mathbb{H}$. Θα δούμε παρακάτω πως ανήκουν σε μια ειδική κατηγορία συναρτήσεων που ορίζονται στο άνω μιγαδικό ημιεπίπεδο, και η μελέτη αυτού του είδους των μιγαδικών συναρτήσεων παίζει πολύ σημαντικό ρόλο στην κατανόηση των ελλειπτικών καμπυλών. Θα επανέλθουμε στο άνω μιγαδικό ημιεπίπεδο $\mathbb{H}$, μετά την κάλυψη των θεμάτων που αφορούν την γεωμετρία και την αριθμητική των ελλειπτικών καμπυλών.

2.11 Μιγαδικός Πολλαπλασιασμός

Όπως αναφέραμε και στο θεώρημα 2.7.1, για κάποιες ελλειπτικές καμπύλες μπορεί να ισχύει ότι ο $\mathrm{End}(E)$ είναι γνήσια μεγαλύτερος από το $\mathbb{Z}$. Σχολιάζοντας την Αρχή του Lefschetz, αναφερθήκαμε στο επόμενο θεώρημα:

Θεώρημα 2.11.1. *Έστω E μια ελλειπτική καμπύλη πάνω από το $\mathbb{C}$, και ω_1, ω_2 δύο γεννήτορες για τον lattice που αντιστοιχεί στην E. Τότε, ακριβώς ένα από τα δύο ακόλουθα συμβαίνει:*

(i) *$End(E) = \mathbb{Z}$*

(ii) *Το σώμα $\mathbb{Q}(\omega_1/\omega_2)$ είναι ένα μιγαδικό τετραγωνικό σώμα αριθμών, και ο $\mathrm{End}(E)$ είναι ισόμορφος με έναν order του $\mathbb{Q}(\omega_1/\omega_2)$.*

Απόδειξη. Έστω $\tau = \omega_1/\omega_2$. Πολλαπλασιάζοντας το Λ με τ, παίρνουμε ένα lattice, ομοιόθετο με το Λ, της μορφής $\mathbb{Z} + \tau\mathbb{Z}$. Άρα, αρκεί να δείξουμε το θεώρημα για αυτά τα lattice.

Έστω το σύνολο

$$R = \{\alpha \in \mathbb{C} : \alpha\Lambda \subset \Lambda\}.$$

Από το θεώρημα 2.10.18, για $\Lambda_1 \equiv \Lambda_2 \equiv \Lambda$, έχουμε πως $\mathrm{End}(E) \cong R$ (αφού το Λ είναι μοναδικό μέχρις ομοιοθεσίας, ο R είναι ανεξάρτητος του lattice). Άρα, για κάθε $\alpha \in R$ υπάρχουν ακέραιοι a, b, c, d τέτοιοι ώστε

$$\alpha = a + b\tau$$

$$\alpha\tau = c + d\tau.$$

Απαλλείφουμε το τ από το σύστημα παίρνουμε την εξίσωση

$$\alpha^2 - (a + d)\alpha + (ad - bc) = 0.$$

Αυτό δείχνει ότι ο R είναι ακέραια επέκταση του $\mathbb{Z}$.

Έστω ότι ο R είναι γνήσια μεγαλύτερος του $\mathbb{Z}$, και έστω ένα $\alpha \in R - \mathbb{Z}$. Τότε, $b \neq 0$, οπότε απαλλοίφωντας το α παίρνουμε την δευτεροβάθμια ως προς τ

$$b\tau^2 - (a - d)\tau - c = 0.$$

Άρα, αφού $\tau \notin \mathbb{R}$, το $\mathbb{Q}(\tau)$ είναι μιγαδικό τετραγωνικό σώμα αριθμών. Αφού ο R είναι ακέραια επέκταση του $\mathbb{Z}$ και $R \subset \mathbb{Q}(\tau)$, έχουμε ότι ο R είναι ένας order στο $\mathbb{Q}(\tau)$. □

Το παραπάνω θεώρημα δικαιολογεί και την ονομασία μιγαδικός πολλαπλασιασμός για την ιδιότητα αυτήν.

Οι ελλειπτικές καμπύλες με μιγαδικό πολλαπλασιασμό έχουν πλούσια δομή και πολλές εφαρμογές. Μια εκ των πιο σημαντικών, είναι η σχέση του με την Θεωρία κλάσεως σωμάτων.

Οι ελλειπτικές καμπύλες επεκτείνουν την έννοια του κυκλοτομικού σώματος αριθμών. Στα κυκλοτομικά σώματα, μας ενδιαφέρει η αριθμητική των σημείων πεπερασμένης τάξης του κύκλου S^1. Τα κυκλοτομικά σώματα αντλούν την σημασία τους κυρίως από το θεώρημα Kronecker-Weber:

Θεώρημα 2.11.2 (Kronecker-Weber)**.** *Αν το αλγεβρικό σώμα αριθμών K έχει αβελιανή ομάδα Galois* $\mathrm{Gal}(K/\mathbb{Q})$*, τότε υπάρχει ένα κυκλοτομικό σώμα αριθμών* $\mathbb{Q}(\zeta)$ *τέτοιο ώστε*

$$\mathbb{Q} \subset K \subset \mathbb{Q}(\zeta).$$

Αυτό σημαίνει πως τα σημεία πεπερασμένης τάξης της S^1 «παραμετρικοποιούν» τις αβελιανές επεκτάσεις του $\mathbb{Q}$. Τα n-torsion σημεία της S^1 είναι ισόμορφα με την κυκλική ομάδα C_n τάξης n, ενώ τα n-torsion σημεία μιας ελλειπτικής καμπύλης δείξαμε ότι είναι ισόμορφα με την $C_n \times C_n$. Επίσης, τα σημεία αυτά υπολογίζονται, στην S^1, από τις συναρτήσεις $e^{2\pi \mathrm{i} z}$ στο $\frac{1}{n}\mathbb{Z}$, ενώ στις ελλειπτικές καμπύλες, από τις τιμές των συναρτήσεων $\wp$ και $\wp'$ στα σημεία $1/n\Lambda$. Απά αυτήν την άποψη, είναι φυσιολογικό να ρωτήσει κανείς τι μπορεί να προσφέρει η θεωρία των ελλειπτικών καμπυλών πάνω από το $\mathbb{C}$ στην μελέτη των σωμάτων αριθμών.

Για παράδειγμα, αν μας δοθεί ένα τετραγωνικό σώμα αριθμών F, μπορούμε να βρούμε ένα είδος επεκτάσεων του (κατ΄ αντιστοιχια με τα κυκλοτομικά σώματα

στο $\mathbb{Q}$) που να «παραμετρικοποιούν» με την παραπάνω έννοια όλες τις αβελιανές επεκτάσεις του F (δηλαδή επεκτάσεις με αβελιανή ομάδα Galois); Το ερώτημα αυτό έγινε γνωστό ως το «όνειρο της νιότης» του Kronecker (Kronecker's Jugendtraum).

Θα εφαρμόσουμε την θεωρία των ελλειπτικών καμπυλών με μιγαδικό πολλαπλασιασμό στην περίπτωση του $\mathbb{Q}(\mathrm{i})$, για να εξηγήσουμε εν συντομία πως μπορούμε να ταξινομήσουμε τις αβελιανές επεκτάσεις του, δίνοντας έτσι μια απάντηση στο Jugendtraum για την ειδική αυτήν περίπτωση.

Λήμμα 2.11.3. *Έστω $E/\mathbb{Q}$ μια ελλειπτική καμπύλη, και K μια επέκταση Galois του $\mathbb{Q}$. Για κάθε $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ θεωρούμε την δράση του σ στην $E(K)$ με $\sigma(O) = O$ και, αν $P = (x, y) \in E(K)$, τότε $\sigma(P) = (\sigma(x), \sigma(y))$. Τότε:*

(i) $\sigma(E(K)) \subset E(K)$.

(ii) *Για κάθε $\sigma, \tau \in \mathrm{Gal}(K/\mathbb{Q})$*

$$(\sigma\tau)(P) = \sigma(\tau(P)).$$

(iii) *Το ταυτοτικό στοιχείο της $\mathrm{Gal}(K/\mathbb{Q})$ δρα τετριμμένα.*

(iv)
$$\sigma(P + Q) = \sigma(P) + \sigma(Q)$$
για κάθε $Q \in E(K)$.

(v) *Αν το P έχει τάξη n, τότε και το $\sigma(P)$ έχει τάξη n.*

Για να ορίσουμε τα κυκλοτομικά σώματα επισυνάπτουμε τις ρίζες του ομομορφισμού $\lambda : \mathbb{C} \to \mathbb{C}$ με $\lambda(z) = z^n$. Μιμούμαστε αυτόν τον ορισμό και, αν $P_1 = (x_1, y, 1), ..., P_m = (x_m, y_m)$ είναι τα n-torsion σημεία της $E(\mathbb{Q})$, ορίζουμε το σώμα

$$\mathbb{Q}(E[n]) = \mathbb{Q}(x_i, y_i, i = 1, 2, ..., m).$$

Προφανώς τα x_i, y_i είναι αλγεβρικά (οι πολλαπλασιασμοί επί m είναι οι μορφισμοί $[m]$, δηλαδή δίνονται από ρητές συναρτήσεις, οπότε ένα σημείο είναι m-torsion αν και μόνο αν μηδενίζει το πολυώνυμο στον αριθμητή του $[m]$).

Πρόταση 2.11.4. *Το $K = \mathbb{Q}(E[n])$ είναι Galois επέκταση του $\mathbb{Q}$.*

Απόδειξη. Έστω ένας ομομορφισμος $\sigma : K \to \mathbb{C}$. Η απεικόνιση σ καθορίζεται πλήρως από το που στέλνει τα x_i και y_i. Όμως το P_i ανήκει στην $E[n]$, άρα, από την προηγούμενη πρόταση

$$O = \sigma(O) = \sigma(nP_i) = n\sigma(P_i),$$

δηλαδή το $\sigma(P_i)$ ανήκει στην $E[n]$. Άρα υπάρχει j τέτοιο ώστε $\sigma(P_i) = P_j$, δηλαδή $\sigma(x_i) = x_j \in K$, $\sigma(y_i) = y_j \in K$. Έπεται πως $\sigma(K) \subset K$, το οποίο σημαίνει πως το K είναι Galois επέκταση του $\mathbb{Q}$. □

Το επόμενο βήμα κάποιου είναι να υπολογίσει την ομάδα Galois της επέκτασης $\mathbb{Q}(E[n])/\mathbb{Q}$.

Πρόταση 2.11.5. *Έστω $E/\mathbb{Q}$ και $n \geq 2$. Τότε, υπάρχει ένας 1-1 ομομορφισμός*

$$\rho_n : \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \longrightarrow \mathrm{GL}_2\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)$$

Η αναπαράσταση αυτή καλείται, για ευνόητους λόγους, αναπαράσταση Galois.

Απόδειξη. (Σκιαγράφηση) Η διαδικασία της απόδειξης έγκειται στο να σταθεροποιήσει κανείς δύο γεννήτορες P και Q της $E[n]$ και να εξετάσει με πράξεις τις προυποθέσεις που θα πρέπει να πληρούν οι εικόνες των γεννητόρων. □

Η αναλογία με την θεωρία των κκλοτομικών επεκτάσεων είναι η εξής: Αν διαλέξουμε έναν γεννήτορα ζ της ομάδας των n-οστών ριζών της μονάδας, τότε γνωρίζουμε ότι υπάρχουν $\phi(n)$ στο πλήθος n-οστές αναπαραστάσεις της $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ που δίνονται από τον τύπο

$$t : \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) \longrightarrow \mathrm{GL}_1\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right) = \left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)^*$$

με

$$\sigma(\zeta) = \zeta^{t(\sigma)}.$$

Στην πραγματικότηα, οι αναπαραστάσεις αυτές είναι ισομορφισμοί. Ωστόσο, αυτή η κατάσταση δεν μεταφέρεται στις ελλειπτικές καμπύλες (μπορεί δηλαδή ο ρ_n να μην είναι επί). Ωστόσο, οι ρ_n είναι σχεδόν επί:

Θεώρημα 2.11.6 (Serre)**.** *Έστω $E/\mathbb{Q}$, η οποία δεν έχει μιγαδικό πολλαπλασιασμό. Τότε, υπάρχει ένας ακέραιος $N \geq 1$, που εξαρτάται από την E, τέτοιος ώστε, αν μκδ$(n, N) = 1$, τότε η αναπαράσταση Galois*

$$\rho_n : \mathrm{Gal}(\mathbb{Q}(E[n])/\mathbb{Q}) \longrightarrow \mathrm{GL}_2\left(\frac{\mathbb{Z}}{n\mathbb{Z}}\right)$$

είναι επί(και άρα ισομορφισμός).

Η αναφορά στο θεώρημα αυτό γίνεται απλά για λόγους πληρότητος, μιας και οι ελλειπτικές καμπύλες που μας ενδιαφέρουν στην παρούσα περίπτωση είναι εκείνες που έχουν μιγαδικό πολλαπλασιασμό.

Σημειώνουμε ότι η καμπύλη

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

έχει μιγαδικό πολλαπλασιασμό, την

$$\phi(x, y) = (-x, \mathrm{i}y).$$

Ο λόγος που κάνουμε αναφορά σε αυτήν την συγκεκριμμένη καμπύλη είναι ότι χρησιμοποιώντας τα σημείας στρέψης αυτής της καμπύλης θα ταξινομούνται οι αβελιανές επεκτάσεις του $\mathbb{Q}(\mathrm{i})$. Πιο συγκεκριμμένα:

Θεώρημα 2.11.7. *Έστω η ρητή ελλειπτική καμπύλη E*

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

Για κάθε ακέραιο $n \geq 1$, έστω $K_n = \mathbb{Q}(\mathrm{i})(E[n])$. Τότε το K_n είναι επέκταση Galois του $\mathbb{Q}(\mathrm{i})$ και η ομάδα Galois της επέκτασης αυτής είναι αβελιανή.

Απόδειξη. Αφού οι επεκτάσεις $\mathbb{Q}(E[n])/\mathbb{Q}$ και $\mathbb{Q}(\mathrm{i})/\mathbb{Q}$ είναι Galois, και η $K_n/\mathbb{Q}$ είναι Galois. Άρα η $K_n/\mathbb{Q}(\mathrm{i})$ είναι Galois. Για μια στοιχειώδη απόδειξη του δεύτερου ισχυρισμού, που βασίζεται σε μια σειρά από λήμματα για πίνακες που ανήκουν στην $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$, παραπέμπουμε στο [Silverman-Tate, [32], κεφ.6]. □

Στην πραγματικότητα, ισχύει το εξής ισχυρότερο αποτέλεσμα, το οποίο είναι το Jugendtraum για το $\mathbb{Q}(\mathrm{i})$:

Θεώρημα 2.11.8. *Αν η F είναι αβελιανή επέκταση του $\mathbb{Q}(\mathrm{i})$, τότε υπάρχει $n \geq 1$ τέτοιο ώστε*

$$F \subset K_n = \mathbb{Q}(\mathrm{i})(E[n])$$

Προχωράμε τώρα στην μελέτη της δομής της $E(\mathbb{Q})$, στην οποία βρίσκονται ίσως και οι κυριότερες ιστορικά απαρχές της θεωρίας των ελλειπτικών καμπυλών.

2.12 Οι ομάδες $E(\mathbb{Q})$ και $E(K)$: Το Θεώρημα Mordell-Weil

Μελετώντας κανείς να λύσει πολυώνυμα τρίτου βαθμού σε δύο μεταβλητές, είδαμε πως οδηγείται κανείς φυσιολογικά στην μελέτη των ελλειπτικών καμπυλών. Απ΄ την στιγμή λοιπόν που ενδιαφέρεται κανείς για αριθμοθεωρητικά προβλήματα, οδηγείται στην μελέτη των ελλειπτικών καμπυλών που ορίζονται πάνω από το $\mathbb{Q}$ καθώς και των ρητών λύσεων αυτών. Αναδιατυπώνοντας, χρησιμοποιώντας τον φορμαλισμό που έχουμε εισαγάγει, για την θεωρία αριθμών αποτελεί κεντρικό πρόβλημα, δοσμένης $E/\mathbb{Q}$, η μελέτη της $E(\mathbb{Q})$. Γενικεύοντας ελαφρώς, ενδιαφέρεται κανείς και για την μελέτη της $E(K)$, για μια E που ορίζεται πάνω από ένα σώμα αριθμών K. Βέβαια, για εμάς, ο όρος σώμα αριθμών σημαίνει πάντα, όπως έχουμε ήδη σημειώσει, αλγεβρικό σώμα αριθμών, δηλαδή μια πεπερασμένη επέκταση του $\mathbb{Q}$.

Το πρόβλημα της μελέτης της $E(\mathbb{Q})$ αποδεικνύεται πιο δύσκολο από την μελέτη της $E(\mathbb{C})$ ή της $E(\mathbb{R})$. Ο λόγος που συμβαίνει αυτό είναι ότι πλέον δουλεύουμε πάνω από ένα global σώμα. Το κεντρικό θεώρημα σ΄ αυτήν την περίπτωση είναι το Mordell-Weil. Το 1908 ο Poincare διατύπωσε την εικασία πως για μια ελλειπτική καμπύλη $E/\mathbb{Q}$, η $E(\mathbb{Q})$ είναι πεπερασμένα παραγόμενη. Η απόδειξη της εικασίας δόθηκε το 1922 από τον Mordell. Το 1928 ο Weil κατάφερε να το γενικεύσει για το τυχαίο σώμα αριθμών K:

Θεώρημα 2.12.1 (Mordell-Weil)**.** *Αν K είναι ένα σώμα αριθμών και η ελλειπτική καμπύλη E ορίζεται υπεράνω του K, τότε για την ομάδα Mordell-Weil $E(K)$ ισχύει*

$$E(K) \cong \mathbb{Z}^r \times E(K)_{tors}$$

όπου $r \in \mathbb{N}$ και $|E(\mathbb{K})_{tors}| < \infty$.

Κεντρικό ρόλο στην απόδειξη του θεωρήματος θα παίξει το παρακάτω λήμμα για αβελιανές ομάδες:

Θεώρημα 2.12.2 (Θεώρημα Καθόδου)**.** *Έστω G μια αβελιανή ομάδα, και έστω ότι υπάρχει συνάρτηση $h : G \to \mathbb{R}$ (την οποία θα καλούμε συνάρτηση ύψους ή απλά ύψος) η οποία ικανοποιεί τις εξής ιδιότητες:*

(i) *Αν $\alpha \in \mathbb{R}$ σταθερά, το σύνολο*

$$G_\alpha = \{P \in G : h(P) \leq \alpha\}$$

είναι πεπερασμένο.

(ii) *Αν Q σταθερό σημείο της G, τότε υπάρχει σταθερά $\beta \in \mathbb{R}$, που εξαρτάται μόνο από την ομάδα G και το σημείο Q, τέτοια ώστε:*

$$h(P+Q) \leq 2h(P) + \beta$$

για κάθε σημείο P της G.

(iii) *Υπάρχουν ένας ακέραιος m, $m \geq 2$ και σταθερά $\gamma \in \mathbb{R}$, που εξαρτώνται μόνο από την ομάδα G, με την ιδιότητα:*

$$h(mP) \geq m^2 h(P) - \gamma$$

για κάθε σημείο P της G.

(iv) *Για τον m που ικανοποιεί το (iii) ισχύει ότι $[G : mG] < \infty$.*

Τότε η G είναι πεπερασμένα παραγόμενη.

Μέθοδος απόδειξης του Mordell-Weil: Η διαδικασία της απόδειξης του Mordell-Weil χωρίζεται στα εξής βήματα:

1ο Αποδειχνύουμε το θεώρημα της καθόδου.

2ο Αποδεικνύουμε το Ασθενές Θεώρημα Mordell-Weil: Αν K είναι ένα σώμα αριθμών, E/K μια ελλειπτική καμπύλη και m ένας ακέραιος ≥ 2, τότε η ομάδα

$$E(K)/mE(K)$$

είναι πεπερασμένη.

3ο Κατασκεύαζουμε μια συνάρτηση ύψους για την ομάδα $E(K)$.

Αξίζει σε αυτό το σημείο να κάνουμε κάποια σχόλια πάνω στην μέθοδο αυτήν που θα ακολουθήσουμε. Κατ΄ αρχάς, πρέπει να γίνει σαφές ότι το Ασθενές Mordell-Weil από μόνο του δεν αρκεί για να αποδείξουμε ότι η $E(\mathbb{Q})$ είναι πεπερασμένα παραγόμενη. Για παράδειγμα, $\mathbb{R}/m\mathbb{R} = 0$ για κάθε m, ωστόσο το $\mathbb{R}$ δεν είναι πεπερασμένα παραγόμενο. Μπορεί επίσης να δείξει κανείς ότι για καμπύλες που ορίζονται πάνω από τα p-αδικά σώματα $\mathbb{Q}_p$ ισχύει ότι η ομάδα $E(\mathbb{Q}_p)/mE(\mathbb{Q}_p)$ έχει πεπερασμένη τάξη, ωστόσο η $E(\mathbb{Q}_p)$ δεν είναι πεπερασμένα παραγόμενη.

Το πρόβλημα αυτό το λύνει το θεώρημα της καθόδου, δηλαδή η ύπαρξη μιας συνάρτησης ύψους. Η συνάρτηση ύψους εξασφαλίζει ότι ο μορφισμός $[m]$ αυξάνει αρκετά το «μέγεθος» των σημείων της ομάδας, ενώ υπάρχουν πεπερασμένα σημεία «μικρού μεγέθους».

Για το σώμα $\mathbb{Q}$ είναι σχετικά απλή διαδικασία ο ορισμός της συνάρτησης ύψους, και θέλει κάποια δουλειά η απόδειξη των ιδιοτήτων. Για το τυχόν σώμα αριθμών K απαιτείται κάποια παραπάνω θεωρία, και θα χρειαστεί να μιλήσουμε πρώτα για ύψη σε προβολικούς χώρους.

1ο Βήμα: Απόδειξη του θεωρήματος της καθόδου:

Απόδειξη. Έστω $[G : mG] = r$ και επιλέχουμε $Q_1, Q_2, ..., Q_r$ στοιχεία της G που να αντιστοιχούν σε ένα σύνολο αντιπροσώπων της ομάδας πηλίκο G/mG. Έστω επίσης ένα τυχόν P στοιχείο της G. Γράφουμε το στοιχείο P στην μορφή $P = mT_1 + Q_{i_1}$ για κάποιο i_1. Έπειτα ακολουθούμε την ίδια διαδικασία για το T_1 : $T_1 = mT_2 + Q_{i_2}$, μετά για το T_2 και ούτω καθεξής. Παίρνουμε έτσι μια ακολουθία σημείων $T_1, ...T_n, ...$

Για το ύψος των T_i παίρνουμε:

$$h(T_i) \leq \frac{1}{m^2}(h(mT_i) + \beta) = \frac{1}{m^2}(h(T_{i-1} - Q_{i_j}) + \beta) \leq \frac{1}{m^2}(2h(T_{i-1}) + A + \beta)$$

όπου

$$A = \max\{\alpha : h(Q_i + Q) \leq 2h(Q) + \alpha : Q \in G, i = 1, 2, ..., r\}.$$

δηλαδή τα A, β είναι ανεξάρτητα του P. Επαναλαμβάνοντας την ίδια διαδικασία παίρνουμε:

$$h(T_n) \leq \left(\frac{2}{m^2}\right)^n h(P) + \left(\frac{1}{m^2 - 2}\right)(A + \beta) < \frac{1}{2^n}h(P) + \frac{1}{2}(A + \beta).$$

Άρα, για $n > \log_2(h(P))$ θα έχουμε ότι:

$$h(T_n) \leq 1 + \frac{1}{2}(A + \beta)$$

Τώρα, παρατηρείστε ότι έχουμε γράψει το P σαν γραμμικό συνδυασμό

$$P = m^n T_n + Q_{i_1} + mQ_{i_2} + ... + m^{n-1}Q_{i_n} = m^n T_n + \sum_{k=1}^{n} m^{k-1}Q_{i_k}$$

όπου $Q_{i_j} \in \{Q_1, Q_2, ..., Q_r\}$. Δηλαδή, έχουμε γράψει το τυχαίο σημείο P της ομάδας G ως γραμμικό συνδυασμό των στοιχείων $\{Q_1, Q_2, ..., Q_r\}$ και των $\{T \in G : h(T) \leq 1 + \frac{1}{2}(A + \beta)\}$. Όμως, από την πρώτη ιδιότητα της συνάρτησης ύψους, το τελευταίο σύνολο είναι πεπερασμένο. Άρα η ομάδα G είναι πεπερασμένα παραγόμενη. □

2ο Βήμα: Το Ασθενές Θεώρημα Mordell-Weil: Προχωρούμε τώρα στην απόδειξη του ασθενούς Mordell-Weil, το οποίο ξαναθυμίζουμε εδώ:

Θεώρημα 2.12.3 (Θεώρημα (Ασθενές Θεώρημα Mordell-Weil))**.** *Αν K είναι ένα σώμα αριθμών, E/K μια ελλειπτική καμπύλη και m ένας ακέραιος ≥ 2, τότε η ομάδα:*

$$E(K)/mE(K)$$

είναι πεπερασμένη.

Για την απόδειξη του θεωρήματος αυτού θα χρειαστούμε μερικά λήμματα:

Λήμμα 2.12.4. *Έστω L/K μια πεπερασμένη επέκταση Galois σωμάτων αριθμών, και έστω ένας ακέραιος $m \geq 2$ τέτοιος ώστε η ομάδα $E(L)/mE(L)$ να είναι πεπερασμένη. Τότε και η $E(K)/mE(K)$ είναι πεπερασμένη.*

Απόδειξη. Ο εγκλεισμός $E(K) \to E(L)$ επάγει απεικόνιση

$$\phi : \frac{E(K)}{mE(K)} \longrightarrow \frac{E(L)}{mE(L)}$$

με πυρήνα

$$\ker\phi = \Phi = \frac{E(K) \cap mE(L)}{mE(K)}$$

Για κάθε $P(\mathrm{mod} mE(K))$ στο πυρήνα της ϕ διαλέγουμε ένα $Q = Q_P$ στην $E(L)$, το οποίο εξαρτάται από την κλάση του P, τέτοιο ώστε να ισχύει

$$[m]Q = P$$

και ορίζουμε την απεικόνιση του P

$$\lambda_P : \mathrm{Gal}(L/K) \longrightarrow E[m]$$

όπου

$$\lambda_P(\sigma) = Q^\sigma - Q.$$

Ελέγχουμε ότι

$$[m]\lambda_P(\sigma) = [m](Q^\sigma - Q) = ([m]Q)^\sigma - [m]Q = P^\sigma - P = O$$

όπου η τελευταία ισότητα επεται από το γεγονός ότι το σ σταθεροποιεί το K, άρα και την $E(K)$. Άρα το $\lambda_P(\sigma)$ ανήκει όντως στην $E[m]$, δηλαδή η λ_P είναι καλά ορισμένη (παρατηρείστε ότι η τιμή του $\lambda_P(\sigma)$ δεν εξαρτάται από την επιλογή του Q).

Αν πάρουμε δύο σημεία P, P' στην $E(K) \cap mE(L)$ με $\lambda_p = \lambda_{P'}$, θα έχουμε

$$(Q_P - Q_{P'})^\sigma = Q_P - Q_{P'}$$

για κάθε σ στην $\mathrm{Gal}(L/K)$, το οποίο συνεπάγεται ότι το $Q_P - Q_{P'} \in E(K)$. Έτσι έχουμε ότι

$$P - P' \in mE(K)$$

κι έτσι

$$P \equiv P'(\mathrm{mod} mE(K).$$

Έτσι λοιπόν, η παραπάνω κατασκυευή μας δίνει μια 1-1 απεικόνιση από τον πυρήνα Φ της ϕ στις απεικονίσεις από την $\mathrm{Gal}(L/K)$ στην $E[m]$. Επειδή οι ομάδες $\mathrm{Gal}(L/K)$ και $E[m]$ είναι πεπερασμένες, έπεται ότι και ο Φ είναι πεπερασμένος. Για να έχουμε το ζητούμενο, αρκεί να παρατηρήσουμε ότι η ακολουθία

$$0 \longrightarrow \Phi \longrightarrow \frac{E(K)}{mE(K)} \longrightarrow \frac{E(L)}{mE(L)}$$

είναι ακριβής. □

Το παραπάνω λήμμα μας δείχνει ότι για να αποδείξουμε το Ασθενές Mordell-Weil, αρκεί να υποθέσουμε ότι

$$E[m] \subset E(K).$$

Αν K είναι ένα σώμα αριθμών, ορίζουμε την επέκταση L που αντιστοιχεί στο K ως εξής:

$$L = K([m]^{-1}E(K))$$

Παρατηρούμε πως η επέκταση αυτή είναι το ελλειπτικό ανάλογο της κλασσικής επέκτασης Kummer, όπου στο σώμα αριθμών K επισυνάπτουμε τις m-οστές ρίζες της μονάδας (επίσης, ο ορισμός αυτός επεκτείνει τον ορισμό της $\mathbb{Q}(E[n])$ που δώσαμε στην προηγούμενη παράγραφο). Η επέκταση αυτή θα παίξει σημαντικό ρόλο στην απόδειξη του Ασθενούς Mordell-Weil. Για να μπορέσουμε να την χειριστούμε καλύτερα, θα χρειαστεί να ορίσουμε την αντιστοιχία του Kummer. Η αντιστοιχία του Kummer είναι ένα συνομολογιακό εργαλείο που μας επιτρέπει να μελετήσουμε εκτενέστερα την συμπεριφορά των ελλειπτικών καμπυλών και των torsion υποομάδων τους σε σχέση με τις επεκτάσεις σωμάτων αριθμών.

Ορισμός 2.12.5. *Ορίζουμε την αντιστοιχία Kummer*

$$\kappa : E(K) \times \mathrm{Gal}(\bar{K}/K) \longrightarrow E[m]$$

ως εξής: αν P είναι ένα σημείο της $E(K)$ και Q ένα οποιοδήποτε σημείο στην $E(\bar{K})$ τέτοιο ώστε να ισχύει ότι $[m]Q = P$, τότε η αντιστοιχία Kummer του (P, σ) ορίζεται να είναι η

$$\kappa(P, \sigma) = Q^\sigma - Q.$$

Υπενθυμίζουμε ότι, αν τα M, N και L είναι R-πρότυπα, μια διγραμμική αντιστοιχία $e : M \times N \to L$ λέγεται τέλεια αν και μόνο αν ο ομομορφισμός

$$M \longrightarrow \mathrm{Hom}(N, L)$$

που επάγει η αντιστοιχία είναι ισομορφισμός.

Οι ακόλουθες ιδιότητες της αντιστοιχίας τους Kummer, και ιδιαίτερα η τέλεια αντιστοιχία που αυτή επάγει, θα μας χρησιμεύσουν στην απόδειξη του θεωρήματος 2.12.3.

Πρόταση 2.12.6. (i) *Η αντιστοιχία Kummer είναι καλά ορισμένη.*

(ii) *Η αντιστοιχία Kummer είναι διγραμμική.*

(iii) *Ο αριστερός πυρήνας της αντιστοιχίας Kummer είναι η $mE(K)$.*

(iv) *Ο δεξιός πυρήνας της αντιστοιχίας Kummer είναι η $\mathrm{Gal}(\bar{K}/L)$, όπου το L είναι όπως ορίστηκε παραπάνω.*

(v) *Η αντιστοιχία Kummer επάγει μιά τέλεια διγραμμική αντιστοιχία*

$$E(K)/mE(K) \times \mathrm{Gal}(L/K) \longrightarrow E[m]$$

Απόδειξη. (i) Έχουμε

$$[m]\kappa(P, \sigma) = [m](Q^\sigma - Q) = [m]Q^\sigma - [m]Q = P^\sigma - P = O$$

όπου η τελευταία ισότητα έπεται από το γεγονός ότι $P \in E(K)$ και η σ σταθεροποιεί το K άρα και την $E(K)$. Άρα το $\kappa(P, \sigma)$ ανήκει στην $E[m]$. Αν τώρα πάρουμε ένα άλλο S στην $E(\bar{K})$ με $[m]S = P$, τότε το S είναι της μορφής $Q + T$ για κάποιο $T \in E[m]$, και παίρνουμε

$$(S)^\sigma - S = (Q+T)^\sigma - (Q+T) = Q^\sigma + T^\sigma - Q - T = Q^\sigma + T - Q - T = Q^\sigma - Q$$

όπου η προτελευταία ισότητα έπεται επειδή έχουμε κάνει την υπόθεση ότι $E[m] \subset E(K)$.

(ii) Προφανώς αν $[m]Q = P$ και $[m]Q' = P'$, τότε $[m](Q+Q') = P+P'$, άρα

$$\kappa(P+P',\sigma) = (Q+Q')^\sigma - (Q+Q')$$
$$= Q^\sigma - Q + Q'^\sigma - Q' = \kappa(P,\sigma) + \kappa(P',\sigma)$$

Αν τώρα θεωρήσουμε δύο στοιχεία σ, τ της $\mathrm{Gal}(\bar{K},K)$, έχουμε

$$\kappa(P,\sigma\tau) = Q^{\sigma\tau} - Q = Q^{\sigma\tau} - Q^\tau + Q^\tau - Q$$
$$= (Q^\sigma - Q)^\tau - (Q^\tau - Q) = \kappa(P,\sigma)^\tau + \kappa(P,\tau) = \kappa(P,\sigma) + \kappa(P,\tau)$$

όπου η τελευταία ισότητα έπεται από το γεγονός ότι $\kappa(P,\sigma) \in E[m] \subset E(K)$.

(iii) Αν το P ανήκει στην $mE(K)$, δηλαδή υπάρχει Q στην $E(K)$ με $P = [m]Q$,τότε το Q σταθεροποιείται από κάθε $\sigma \in \mathrm{Gal}(\bar{K},K)$, άρα

$$\kappa(P,\sigma) = Q^\sigma - Q = O.$$

Αντίστροφα, αν $\kappa(P,\sigma) = 0$ για κάθε $\sigma \in \mathrm{Gal}(\bar{K}/K)$. Τότε, επιλέγοντας ένα Q στην $E(\bar{K})$ με $[m]Q = P$, έχουμε ότι $Q^\sigma = Q$ για κάθε $\sigma \in \mathrm{Gal}(\bar{K}/K)$. Αυτό τώρα μας δίνει ότι $Q \in E(K)$, δηλαδή $P \in mE(K)$.

(iv) Αν ένα σ ανήκει στην $\mathrm{Gal}(\bar{K}/L)$, τότε

$$\kappa(P,\sigma) = Q^\sigma - Q = O,$$

αφού, εξ' ορισμού, το Q ανήκει στο $E(L)$. Αντίστροφα, αν το σ ανήκει στην $\mathrm{Gal}(\bar{K}/K)$ και $\kappa(P,\sigma) = O$, για κάθε P στην $E(K)$, τότε για κάθε Q στην $E(\bar{K})$ με $[m]Q \in E(K)$ θα έχουμε

$$O = \kappa([m]Q,\sigma) = Q^\sigma - Q.$$

Άρα το σ σταθεροποιεί το L, δηλαδή ανήκει στην $\mathrm{Gal}(\bar{K}/L)$.

(v) Αφού τα στοιχεία της $\mathrm{Gal}(\bar{K}/K)$ σταθεροποιούν το $[m]^{-1}E(K)$, έπεται πως η L/K είναι Galois. Το ζητούμενο τώρα έπεται από τα (ii) και (iii).

□

Η πρόταση 2.12.6 μας δίνει σαν πόρισμα ότι η ομάδα πηλίκο $E(K)/mE(K)$ είναι πεπερασμένη αν και μόνο αν η επέκταση L/K είναι πεπερασμένη. Για να αποδείξουμε ότι η L/K είναι πεπερασμένη επέκταση, θα χρειαστεί να μελετήσουμε τις αναγωγές της ελλειπτικής καμπύλης.

Στα επόμενα, με M_K συμβολίζουμε ένα πλήρες σύνολο από μη ισοδύναμες απόλυτες τιμές, ή ισοδύναμα εκτιμήσεις, στο K. Με M_K^∞ συμβολίζουμε τα Αρχιμήδεια στοιχεία του M_K, ενώ τα μη Αρχιμήδεια στοιχεία του τα συμβολίζουμε με M_K^0. Αν η εκτίμηση $\upsilon \in M_K^0$, γράφουμε ord_υ για την αντίστοιχη κανονικοποιημένη εκτίμηση της υ (δηλαδή $\mathrm{ord}_\upsilon(K^*) = \mathbb{Z}$).

Ο δακτύλιος των ακεραίων R και η ομάδα των μονάδων R^* ορίζονται όπως και προηγουμένως, στην παράγραφο 2.8, με την διαφορά ότι τώρα απαιτούμε τα στοιχεία του R (αντίστοιχα του R^*) να ικανοποιούν την σχέση $\upsilon(x) \geq 0$ (αντίστοιχα $\upsilon(x) = 0$) για κάθε εκτίμηση υ στον M_K^0.

Τέλος, αν $\upsilon \in M_K$, με K_υ συμβολίζουμε την πλήρωση του σώματος K ως προς την μετρική που επάγει η εκτίμηση υ, ενώ, αν $\upsilon \in M_K^0$, με R_υ θα συμβολίζουμε τον δακτύλιων των ακεραίων του K_υ, με M_υ το μέγιστο ιδεώδες του R_υ και με k_υ το πηλίκο R_υ/M_υ.

Ορισμός 2.12.7. *Έστω E/K μια ελλειπτική καμπύλη πάνω από ένα σώμα αριθμών K, και υ μια διακριτή εκτίμηση στο M_K^0. Η E έχει καλή (αντίστοιχα κακή) αναγωγή στην υ αν η E έχει καλή (αντίστοιχα, κακή) αναγωγή στο K_υ. Θεωρώντας μια ελάχιστη εξίσωση Weierstrass για την E πάνω από το K_υ, συμβολίζουμε την αναγωγή της E στο k_υ με $\tilde{E}_\upsilon/k_\upsilon$.*

Δεν είναι πάντα εφικτό να επιλέξουμε μια ελάχιστη εξίσωση Weierstrass για την E πάνω από το K που να είναι ταυτόχρονα ελάχιστη για κάθε K_υ. Ωστόσο, για το $\mathbb{Q}$, αυτό είναι εφικτό.

Τέτοιες ελάχιστες εξισώσεις Weierstrass λέγονται global. Μπορεί κανείς να δείξει ότι μια ελλειπτική καμπύλη πάνω από ένα σώμα αριθμών K έχει πάντα global ελάχιστη εξίσωση Weierstrass αν και μόνο αν το K έχει τετριμμένη class group (δηλαδή έχει class number ίσο με 1). Έστω E/K μια ελλειπτική καμπύλη πάνω από ένα σώμα αριθμών K. Επιλέγουμε μια εξίσωση Weierstrass

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

η οποία έχει διακρίνουσα Δ. Τότε, για σχεδόν όλες τις εκτιμήσεις υ στο M_K^0 (εκτός από πεπερασμένες) έχουμε

$$\upsilon(a_i) \geq 0$$

για κάθε $i = 1, 2, ..., 6$, και $\upsilon(\Delta) = 0$. Για κάθε υ που ικανοποιεί τα παραπάνω, η αρχική εξίσωση είναι ελάχιστη, και η αναγωγή $\tilde{E}_\upsilon/k_\upsilon$ είναι nonsingular. Άρα, η E έχει καλή αναγωγή για σχεδόν κάθε $\upsilon \in M_K^0$ (εκτός από το πολύ πεπερασμένες). Ο συμβολισμός που έχουμε εισαγάγει μας επιτρέπει να αναδιατυπώσουμε το (ii) της πρότασης 2.8.8 ως εξής:

Πρόταση 2.12.8. *Έστω $\upsilon \in M_K^0$ μια διακριτή εκτίμηση, με $\upsilon(m) = 0$. Έστω ακόμη ότι η E έχει καλή αναγωγή στην υ. Τότε, η απεικόνιση αναγωγής*

$$E(K)[m] \longrightarrow \tilde{E}_\upsilon(k_\upsilon)$$

είναι 1-1.

Οι επόμενες τρεις προτάσεις είναι τα τελευταία ενδιάμεσα αποτελέσματα που θα χρειαστούμε για να αποδείξουμε το θεώρημα 2.12.3.

Πρόταση 2.12.9. *Έστω το $L = K([m]^{-1}E(K))$ όπως προηγουμένως. Η επέκταση L/K είναι αβελιανή και έχει εκθέτη m (δηλαδή η $\mathrm{Gal}(L/K)$ είναι αβελιανή και η τάξη κάθε στοιχείου της διαιρεί το m).*

Απόδειξη. Η πρόταση 2.12.6 μας δίνει μια εμφύτευση

$$\mathrm{Gal}(L/K) \longrightarrow \mathrm{Hom}(E(K), E[m])$$

με

$$\sigma \longrightarrow \kappa(\cdot, \sigma),$$

και το ζητούμενο έπεται. □

Πρόταση 2.12.10. *Έστω E/K με ελάχιστη διακρίνουσα Δ και L, K όπως πριν. Αν θέσουμε*

$$S = \{v \in M_K^0 : v(\Delta) > 0\} \cup \{v \in M_K^0 : v(m) \neq 0\} \cup M_K^\infty,$$

τότε, αν $v \in M_K$ και $v \notin S$, η L/K είναι αδιακλάδιστη στην v.

Για την επόμενη πρόταση, θα χρειαστούμε τα εξής τρία βασικά θεωρήματα από την αλγεβρική θεωρία αριθμών:

Θεώρημα 2.12.11. *Έστω K ένα σώμα αριθμών. Τότε, η class qroup του K είναι πεπερασμένη (η τάξη της ονομάζεται class number του K).*

Θεώρημα 2.12.12. *Έστω ένα σώμα K χαρακτηριστικής 0 το οποίο περιέχει τις m-οστές ρίζες της μονάδας. Τότε, η μέγιστη αβελιανή επέκταση του με εκθέτη m επιτυγχάνεται επισυνάρτοντας στο K τις m-οστές ρίζες όλων των στοιχείων του.*

Θεώρημα 2.12.13 (Θεώρημα των S-μονάδων του Dirichlet)**.** *Έστω K ένα σώμα αριθμών και S ένα πεπερασμένο σύνολο από εκτιμήσεις στο K που περιέχει τις Αρχιμήδειες εκτιμήσεις. Τότε, η ομάδα R_S^* των S-ακεραίων είναι πεπερασμένα παραγόμενη.*

Πρόταση 2.12.14. *Έστω K ένα σώμα αριθμών, $S \subset M_K$ ένα πεπερασμένο σύνολο από εκτιμήσεις, το οποίο περιέχει το M_K^∞, και ένας ακέραιος $m \geq 2$. Έστω L/K η μέγιστη αβελιανή επέκταση του K με εκθέτη m, η οποία είναι αδιακλάδιστη έξω από το S. Τότε, η L/K είναι πεπερασμένη.*

Απόδειξη. Έστω ότι η πρόταση αληθεύει για κάποια πεπερασμένη επέκταση K' του K, και έστω S' το σύνολο το σύνολο των εκτιμήσεων στο K' που επεκτείνουν το S. Τότε, η επέκταση LK'/K' θα είναι πεπερασμένη, ως αβελιανή, με εκθέτη m και αδιακλάδιστη έξω από το S'. Από αυτό όμως έπεται πως η L/K θα είναι επίσης πεπερασμένη. Άρα, μπορούμε να υποθέσουμε πως το K περιέχει τις m-οστές ρίζες της μονάδας.

Επίσης, μπορούμε να μεγαλώσουμε το S, εφόσον αυτό θα έχει επίπτωση μόνο στο L. Χρησιμοποιώντας ότι η class qroup του K είναι πεπερασμένη, επισυνάπτουμε στο S πεπερασμένο πλήθος εκτιμήσεων, ούτως ώστε ο δακτύλιος

$$R_S = \{\alpha \in K : v(\alpha) \geq 0 \forall v \in M_K : v \notin S\}$$

των S-ακεραίων να είναι περιοχή κύριων ιδεωδών. Για παράδειγμα, μπορεί κανείς να επισυνάψει εκτιμήσεις που αντιστοιχούν στου πρώτους που διαιρούν το γινόμενο ενός πλήρους συνόλου αντιπροσώπων της class group. Επίσης, επεκτείνουμε το S ούτως ώστε να ισχύει ότι $v(m) = 0$ για κάθε $v \notin S$.

Χρησιμοποιώντας το θεώρημα 2.12.12, συμπεραίνουμε ότι το L είναι το μέγιστο υπόσωμα του

$$K(a^{1/m} : a \in K)$$

που μένει αδιακλάδιστο έξω από το S.

Αν τώρα v είναι ένα στοιχείο του M_K που δεν ανήκει στο S, και θεωρήσουμε την εξίσωση

$$X^m - a = 0$$

πάνω από το K_v, τότε, αφού $v(m) = 0$ και η διακρίσουσα του πολυωνύμου $X^m - a$ είναι $\pm m^m a^{m-1}$, συμπεραίνουμε ότι η επέκταση

$$K_v(a^{1/m})/K_v$$

είναι αδιακλάδιστη αν και μόνο αν

$$\mathrm{ord}_v(a) \equiv 0(\mathrm{mod} m).$$

Όμως, όταν επισυνάπτουμε τις m-οστές ρίζες της μονάδας, πρέπει να επιλέγουμε μόμον έναν αντιπρόσωπο για κάθε κλάση στην $K^*/(K^*)^m$. Θέτοντας

$$T_S = \{a \in K^*/(K^*)^m : \mathrm{ord}_v(a) \equiv 0(\mathrm{mod} m) \forall v \in M_K : v \notin S\},$$

παρατηρούμε ότι παίρνουμε

$$L = K(a^{1/m} : a \in T_S).$$

Για να δείξουμε λοιπόν ότι η L/K είναι πεπερασμένη αρκεί να δείξουμε ότι το σύνολο T_S είναι πεπερασμένο.

Θεωρούμε την φυσική απεικόνιση

$$R_S^* \longrightarrow T_S.$$

Έστω ένα $a \in K^*$ που αντιπροσωπεύει ένα στοιχείο του T_S. Το ιδεώδες aR_S είναι η m-οστή δύναμη ενός ιδεώδους στον R_S, αφού τα πρώτα ιδεώδη του R_S αντιστοιχούν σε εκτιμήσεις που δεν ανήκουν στο S. Όμως ο R_S είναι περιοχή κύριων ιδεωδών, και άρα μπορούμε να βρούμε ένα $b \in K^*$ τέτοιο ώστε $aR_S = b^m R_S$. Αυτό σημαίνει πως υπάρχει ένα $u \in R_S^*$ τέτοιο ώστε να ισχύει $a = ub^m$. Τότε, τα a και u δίνουν το ίδιο στοιχείο στο T_S, δηλαδή η φυσική απεικόνιση απ΄ τον R_S^* στο T_S είναι επί. Ο πυρήνας της περιέχει τον $(R_S^*)^m$, άρα υπάρχει μια απεικόνιση

$$R_S^*/(R_S^*)^m \longrightarrow T_S$$

η οποία είναι επί. Όμως, το θεώρημα 2.12.13 δίνει σαν πόρισμα ότι το πηλίκο $R_S^*/(R_S^*)^m$ είναι πεπερασμένο. Άρα, το T_S είναι πεπερασμένο, και έχουμε δείξει το ζητούμενο. □

Μπορούμε τώρα να αποδείξουμε το θεώρημα 2.12.3, του οποίου την απόδειξη την έχουμε ήδη περιγράψει.

Απόδειξη. (του Ασθενούς Θεωρήματος Mordell-Weil) Έστω K ένα σώμα αριθμών. Θεωρούμε την επέκταση

$$L = K([m]^{-1}E(K)).$$

Η ομάδα $E[m]$ είναι πεπερασμένη, και η τέλεια αντιστοιχία που επάγει η αντιστοιχία Kummer (Πρόταση 2.12.6) αποδεικνύουν ότι η $E(K)/mE(K)$ είναι πεπερασμένη αν και μόνο αν η L/K είναι πεπερασμένη. Από τις προτάσεις 2.12.9, 2.12.10 και 2.12.14 έπεται ότι η L/K είναι πεπερασμένη. □

3ο Βήμα: α) Κατασκευή της συνάρτησης ύψους για το $\mathbb{Q}$:

Κατασκευάζουμε τώρα μια συνάρτηση ύψους. Όπως έχουμε δείξει, αυτό είναι το τελευταίο βήμα που χρειάζεται για την απόδειξη του θεωρήματος 2.12.1. Σε πρώτη φάση, θέλουμε να αποδείξουμε το θεώρημα για το $\mathbb{Q}$. Η απόδειξη του κάνει χρήση της ακόλουθης συνάρτησης ύψους:

Ορισμός 2.12.15. *Αν $a = p/q$ είναι ένας ρητός αριθμός σε ανάγωγη μορφή, τότε ορίζουμε το ύψους του ως*

$$H(a) = \max\{|p|, |q|\}$$

και το λογαριθμικό του ύψος να είναι το

$$h(a) = \log(H(a))$$

Ορισμός 2.12.16 (συνάρτησης ύψους για το $\mathbb{Q}$)**.** *Έστω μια ελλειπτική καμπύλη $E/\mathbb{Q}$. Η συνάρτηση ύψους για την $E(\mathbb{Q})$ είναι η συνάρτηση*

$$h : E(\mathbb{Q}) \longrightarrow \mathbb{R}$$

όπου εξ΄ ορισμού

$$h(P) \equiv h(x(P))$$

για $P \neq O$, και 0 για $P = O$. Μερικές φορές συμβολίζουμε την h και με h_x (επειδή εξαρτάται από την x συντεταγμένη).

Πρέπει ασφαλώς να εξασφαλίσουμε ότι η συνάρτηση $h(P)$ που ορίσαμε ικανοποιεί τις ιδιότητες που απαιτεί το θεώρημα της Καθόδου και άρα η h είναι όντως ύψος:

Πρόταση 2.12.17. *Έστω μια ρητή ελλειπτική καμπύλη $E : y^2 = x^3 + Ax + B$ με $A, B \in \mathbb{Z}$ (υπενθυμίζουμε ότι κάθε ελλειπτική καμπύλη $E/\mathbb{Q}$ έχει μια τέτοια ελάχιστη εξίσωση Weierstrass). Τότε:*

(i) *Αν $\alpha \in \mathbb{R}$ σταθερά, το σύνολο*

$$E(\mathbb{Q})_\alpha = \{P \in E(\mathbb{Q}) : h(P) \leq \alpha\}$$

είναι πεπερασμένο.

(ii) *Αν Q σταθερό σημείο της $E(\mathbb{Q})$, τότε υπάρχει σταθερά $\beta \in \mathbb{R}$, που εξαρτάται μόνο από τα A, B, δηλαδή την $E(\mathbb{Q}$, και το σημείο Q, τέτοια ώστε:*

$$h(P + Q) \leq 2h(P) + \beta$$

για κάθε σημείο P της $E(\mathbb{Q})$.

(iii) *Υπάρχει σταθερά $\gamma \in \mathbb{R}$ που εξαρτάται μόνο από τα A και B, δηλαδή την $E(\mathbb{Q})$, με την ιδιότητα:*

$$h([2]P) \geq 4h(P) - \gamma$$

για κάθε σημείο P της $E(\mathbb{Q})$.

Παρατηρούμε ότι για το Mordell-Weil στο $\mathbb{Q}$ μας αρκεί το Ασθενές Mordell-Weil, για $m = 2$, μιας και για αυτό το m δουλεύει η συνάρτηση ύψους που ορίσαμε.

Απόδειξη. (i) Είναι προφανές ότι το σύνολο

$$\{x \in \mathbb{Q} : h(x) \leq \alpha\}$$

είναι πεπερασμένο. Επειδή για κάθε ρητό x_0, η $E(\mathbb{Q})$ περιέχει το πολύ δύο σημεία με x-συντεταγμένη το x_0 το ζητούμενο έπεται.

(ii) Μπορούμε να υποθέσουμε ότι $\beta > \max\{h(Q), h([2]Q)\}$, ούτως ώστε το ζητούμενο να ισχύει για $Q = O$ και για $P \in \{O, \pm Q\}$. Γενικότερα, γράφουμε

$$P = (x, y) = \left(\frac{a}{d^2}, \frac{b}{d^3}\right)$$

και

$$Q = (x_0, y_0) = \left(\frac{a_0}{d_0^2}, \frac{b_0}{d_0^3}\right)$$

όπου τα κλάσματα είναι όλα ανάγωγα (είναι απλό να εξακριβώσει κανείς ότι αυτή η γραφή είναι εφικτή). Η πρόσθεση στην ομάδα μας δίνει

$$x(P + Q) = \left(\frac{y - y_0}{x - x_0}\right)^2 - x - x_0.$$

Κάνοντας πράξεις, και χρησιμοποιώντας το γεγονός ότι τα P και Q ανήκουν στην E, παίρνουμε

$$x(P + Q) = \frac{(xx_0 + A)(x + x_0) + 2B - 2yy_0}{(x - x_0)^2}$$

$$= \frac{(aa_0 + Ad^2d_0^2)(ad_0^2 + a_0d^2) + 2Bd^4d_0^4 - 2bdb_0d_0}{(ad_0^2 - a_0d^2)^2}.$$

Η απαλλοιφή κοινού παράγοντα σε αριθμητή και παρανομαστή ενός ρητού κατεβάζει το ύψος του, οπότε υπολογίζουμε

$$H(x(P + Q)) \leq \beta' max\{|a|^2, |d|^4, |bd|\},$$

όπου η β' είναι μια σταθερά που εξαρτάται μόνο από τα A, B, a_0, b_0 και d_0. Αφού $H(x(P)) = \max\{|a|, |d|^2\}$, αν μπορέσουμε να διώξουμε κατάλληλα το $|bd|$ που εμφανίζεται στην ανισότητα (δηλαδή να το αντικαταστήσουμε με μία βολική έκφραση των $|a|$ και $|d|$) θα έχουμε τελειώσει. Όμως, αφού το $P \in E$, οι συντεταγμένες του ικανοποιούν την εξίσωση της, δηλαδή παίρνουμε

$$b^2 = a^3 + Aad^4 + Bd^6.$$

Άρα

$$|b| \leq \beta'' max\{|a|^{3/2}, |d|^3\},$$

Συνεκτιμώντας και το προηγούμενο φράγμα, έχουμε

$$H(x(P + Q)) \leq \beta'\beta'' max\{|a|^2, |d|^4\} = \beta'\beta'' H(x(P))^2.$$

Λογαριθμώντας παίρνουμε το ζητούμενο.

(iii) Μπορούμε να επιλέξουμε εξ΄ αρχής την σταθερά $\gamma \geq 4\max\{h(T) : T \in E(\mathbb{Q})[2]\}$, ούτως ώστε να εξασφαλίσουμε από την αρχή ότι το ζητούμενο ισχύει για το μηδενικό σημείο και τα 2-torsion σημεία της E. Γράφουμε $P = (x, y)$, οπότε από τους τύπους για την πράξη της ομάδας (πρόταση 2.2.4) θα έχουμε

$$x([2]P) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4x^3 + 4Ax + 4B}.$$

Ο τύπος αυτός μας προτρέπει να μελετήσουμε τα πολυώνυμα:

$$F(X,Z) = X^4 - 2AX^2Z^2 - 8BXZ^3 + A^2Z^4,$$

$$g(X,Z) = 4X^3Z + 4AXZ^3 + 4BZ^4.$$

Αν $x = x([2]P) = a/b$ ως ανάγωγο κλάσμα, τότε

$$x([2]P) = \frac{F(a,b)}{G(a,b)}.$$

Εδώ όμως, ψάχνουμε, σε αντίθεση με την απόδειξη του προηγούμενου ερωτήματος, για ένα κάτω φράγμα για το $H(x([2]P))$. Αυτό σημαίνει ότι θα πρέπει να φράξουμε την «ποσότητα της απαλλοιφής» μεταξύ αριθμητή και παρανομαστή.

Τα πολυώνυμα $F(X,1)$, $G(X,1)$ είναι σχετικά πρώτα μεταξύ τους. Αυτό μας οδηγεί στο εξής λήμμα:

Λήμμα 2.12.18. *Έστω $\Delta = 4A^3 + 27B^2$ και τα πολυώνυμα F και G όπως παραπάνω. Ορίζουμε επίσης τα πολυώνυμα*

$$\begin{aligned}
f_1(X,Z) &= 12X^2Z + 16AZ^3,\\
g_1(X,Z) &= 3X^3 - 5AXZ^2 - 27BZ^3,\\
f_2(X,Z) &= 4(4A^3+27B^2)X^3 - 4A^2BX^2Z + 4A((3A^3+22B^2)XZ^2\\
&\quad +12B(A^3+8B^2)Z^3,\\
g_2(X,Z) &= A^2bX^2 + A(5A^3+32B^2)X^2Z + 2B(13A^3+96B^2)XZ^2\\
&\quad -3A^2(A^3+8B^2)Z^3.
\end{aligned}$$

Τότε, στο $\mathbb{Z}[A,B,X,Z]$, ισχύουν οι εξής ταυτότητες:

$$f_1(X,Z)F(X,Z) - g_1(X,Z)G(X,Z) = 4\Delta Z^7,$$

$$f_2(X,Z)F(X,Z) - g_2(X,Z)G(X,Z) = 4\Delta X^7.$$

Λόγω του ότι τα $F(X,Z)$ και $G(X,Z)$ είναι σχετικά πρώτα ομογενή πολυώνυμα, έπεται ότι κάποιες ταυτότητες αυτού του είδους θα πρέπει να υπάρχουν. Για την ακριβή εύρεση των f_i και g_i πρέπει κανείς να εφαρμόσει τον ευκλείδιο αλγόριθμο.

Ορίζουμε τώρα την δ ως τον μκδ$(F(a,b), G(a,b))$. Η δ δηλαδή είναι η ποσότητα που απαλλοίφουμε στο κλάσμα του $x([2]P)$ για να το κάνουμε ανάγωγο. Από τις σχέσεις

$$f_1(a,b)F(a,b) - g_1(a,b)G(a,b) = 4\Delta b^7,$$

και

$$f_2(a,b)F(a,b) - g_2(a,b)G(a,b) = 4\Delta a^7,$$

έπεται ότι $\delta | 4\Delta$. Ειδικότερα, $|\delta| \leq |4\Delta|$. Άρα

$$H(x([2]P)) \geq \frac{\max\{|F(a,b)|, |G(a,b)|\}}{|4\Delta|}.$$

Οι ίδιες ταυτότητες μας δίνουν όμως κι ότι

$$|4\Delta b^7| \leq 2\max\{|f_1(a,b)|, |g_1(a,b)|\}\max\{|F(a,b)|, |G(a,b)|\},$$

$$|4\Delta a^7| \leq 2\max\{|f_2(a,b)|, |g_2(a,b)|\}\max\{|F(a,b)|, |G(a,b)|\}.$$

Από τους τύπους για τα f_i και g_i (λήμμα 2.12.19), παίρνουμε το φράγμα

$$\max\{|f_1(a,b)|, |g_1(a,b)|, |f_2(a,b)|, |g_2(a,b)|\} \leq \gamma' \max\{|a|^3, |b|^3\},$$

για κάποια σταθερά γ' που εξαρτάται μόνον από τα A και B. Συνδυάζοντας τις τρεις τελευταίες ανισότητες έχουμε την ανισότητα

$$\max\{|4\Delta a^7||4\Delta b^7|\} \leq 2\gamma' \max\{|a|^3, |b|^3\}\max\{|F(a,b)|, |G(a,b)|\}.$$

Απαλλοίφωντας κατά μέλη το $\max\{|a|^3, |b|^3\}$, παίρνουμε

$$\frac{1}{2\gamma'}\max\{|a|^4, |b|^4\} \leq \frac{\max\{|F(a,b)|, |G(a,b)|\}}{|4\Delta|}.$$

Χρησιμοποιώντας τώρα ότι $\max\{|a|, |b|\} = H(x(P))$, και σε συνδυασμό με την ανισότητα

$$H(x([2]P)) \geq \frac{\max\{|F(a,b)|, |G(a,b)|\}}{|4\Delta|}$$

που δείξαμε προηγουμένως, παίρνουμε ότι

$$\frac{1}{2\gamma'}H(x(P))^4 \leq H(x([2]P)),$$

οπότε λογαριθμούμε για να έχουμε το ζητούμενο. □

Απόδειξη. (του θεωρήματος 2.12.1 για $K = \mathbb{Q}$) Έχουμε κατασκευάσει μια συνάρτηση ύψους για το $\mathbb{Q}$ που ικανοποιεί τις απαιτήσεις του θεωρήματος της Καθόδου, το οποίο μας δίνει ότι η $E(\mathbb{Q})$ είναι πεπερασμένα παραγόμενη. □

3ο Βήμα: β) Κατασκευή της συνάρτησης ύψους για το K:

Προχωράμε τώρα στην κατασκευή της συνάρτησης ύψους για το τυχόν σώμα αριθμών K. Για να μπορέσουμε να την κατασκευάσουμε θα χρειαστεί πρώτα να αναφέρουμε κάποια αποτελέσματα σχετικά με την κατασκευή υψών σε στον προβολικό χώρο $\mathbb{P}^n(\bar{\mathbb{Q}})$.

Αν P είναι ένα σημείο στον προβολικό χώρο $\mathbb{P}^n(\mathbb{Q})$, μπορούμε να βρούμε ομογενείς συντεταγμένες για το P

$$P = [x_0, x_1, ...x_n]$$

τέτοιες ώστε x_i όλες ακέραιες και μκδ$(x_0, x_1, .., x_n) = 1$ (αυτό μπορούμε να το πετύχουμε επειδή ο $\mathbb{Z}$ είναι περιοχή κύριων ιδεωδών), οπότε ορίζουμε το ύψος του P να είναι η ποσότητα

$$H(P) = \max\{|x_0|, |x_1|, ..., |x_n|\}.$$

Είναι άμεσο ότι αν το C είναι σταθερά, τότε το σύνολο

$$\{P \in \mathbb{P}^n(\mathbb{Q}) : H(P) \leq C\}$$

είναι πεπερασμένο.

Θέλουμε να γενικεύσουμε την κατασκευή για το ύψος που ορίσαμε στο $\mathbb{Q}$ σε κάθε σώμα αριθμών. Το ουσιαστικό πρόβλημα εδώ είναι ότι ο δακτύλιος των ακεραίων του σώματος μπορεί να μην είναι περιοχή κύριων ιδεωδών. Για να αντιμετωπίσουμε αυτήν την δυσκολία, χρησιμοποιούμε και πάλι τις εκτιμήσεις του σώματος.

Ορισμός 2.12.19. *Το σύνολο $M_{\mathbb{Q}}$ των στάνταρ απολύτων τιμών στο $\mathbb{Q}$ αποτελείται από:*

(i) *Την Αρχιμήδεια απόλυτη τιμή*

$$|x|_\infty = \max\{x, -x\}$$

(ii) *Τις μη Αρχιμήδειες p-αδικές απόλυτες τιμές, όπου p πρώτος, που ορίζονται ως εξής: αν p δεν διαιρεί το ab, τότε:*

$$|p^n \frac{a}{b}| = p^{-n}.$$

Το σύνολο των στάνταρ απόλυτων τιμών στο σώμα αριθμών K είναι το σύνολο των απόλυτων τιμών M_K που αποτελείται από τις απόλυτες τιμές στο K που ο περιορισμός τους στο $\mathbb{Q}$ ταυτίζεται με κάποια από τις απόλυτες τιμές στο $M_{\mathbb{Q}}$.

Είναι σαφές ότι όταν αναφερόμαστε στο M_K, μπορούμε να θεωρούμε είτε τις απόλυτες τιμές, είτε ισοδύναμα τις εκτιμήσεις που αυτές επάγουν.

Ορισμός 2.12.20. *Έστω $\upsilon \in M_K$. Ο τοπικός βαθμός της υ είναι ο βαθμός*

$$n_\upsilon = [K_\upsilon : \mathbb{Q}_\upsilon]$$

όπου, όπως και πριν, τα K_υ και Q_υ είναι οι πληρώσεις των K και $\mathbb{Q}$ ως προς την υ.

Υπάρχουν δύο βασικά θεωρήματα της αλγεβρικής θεωρίας αριθμών σχετικά με τους τοπικούς βαθμούς των στοιχείων του M_K:

Πρόταση 2.12.21. *Αν έχουμε $L/K/\mathbb{Q}$ μια ακολουθία από σώματα αριθμών, και $\upsilon \in M_K$, τότε:*

$$\sum_{w \in M_L, w|\upsilon} n_w = [L : K] n_\upsilon,$$

όπου $w|\upsilon$ σημαίνει ότι η w περιορισμένη στο K ταυτίζεται με την υ.

Πρόταση 2.12.22 (Τύπος γινομένου)**.** *Αν $x \in K^*$ τότε*

$$\prod_{\upsilon \in M_K} |x|_\upsilon^{n_\upsilon} = 1.$$

Ορισμός 2.12.23. *Έστω $P \in \mathbb{P}^n(K)$ με $P = [x_0, x_1, ..., x_n]$, όπου $x_0, x_1, ..., x_n \in K$. Το ύψος του P (στο K) ορίζεται να είναι το*

$$H_K(P) = \prod_{\upsilon \in M_K} max\{|x_0|_\upsilon, |x_1|_\upsilon, ..., |x_n|_\upsilon\}^{n_\upsilon}.$$

Οι βασικές ιδιότητες του ύψους $H_K(P)$ συνοψίζονται στην παρακάτω πρόταση:

Πρόταση 2.12.24. *Αν $P \in \mathbb{P}^n(K)$, τότε:*

(i) *Το $H_K(P)$ δεν εξαρτάται από την επιλογή των ομογενών συντεταγμένων του P.*

(ii) *Για κάθε P στον $\mathbb{P}^n(K)$ ισχύει*

$$H_K(P) \geq 1.$$

(iii) *Αν η L/K είναι πεπερασμένη, τότε*

$$H_L(P) = H_K(P)^{[L:K]}.$$

Απόδειξη. (i) Αν μια επιλογή συντεταγμέων για το P είναι η $P = [x_0, x_1, ..., x_n]$, τότε κάθε άλλη επιλογή είναι της μορφής $[\lambda x_0, \lambda x_1, \lambda x_n]$ για κάποιο $\lambda \in K^*$, οπότε

$$\begin{aligned}
&\prod_{v \in M_K} max\{|\lambda x_0|_v, |\lambda x_1|_v, ..., |\lambda x_n|_v\}^{n_v} \\
&= \prod_{v \in M_K} |\lambda|^{n_v} max\{|x_0|_v, |x_1|_v, ..., |x_n|_v\}^{n_v} \\
&= \prod_{v \in M_K} max\{|x_0|_v, |x_1|_v, ..., |x_n|_v\}^{n_v}
\end{aligned}$$

όπου η τελευταία ισότητα έπεται από την πρόταση 2.12.22.

(ii) Προφανές, από το γεγονός ότι για κάθε σημείο στον προβολικό χώρο μπορούμε πάντα να βρούμε συντεταγμένες που η μία τουλάχιστον εξ΄ αυτών να είναι ίση με 1.

(iii) Υπολογίζουμε

$$\begin{aligned}
H_L(P) &= \prod_{w \in M_L} max\{|x_0|_w, |x_1|_w, ..., |x_n|_w\}^{n_w} \\
&= \prod_{v \in M_K} \prod_{w \in M_L, w|v} max\{|x_0|_v, |x_1|_v, ..., |x_n|_v\}^{n_w} \\
&= \prod_{v \in M_K} max\{|x_0|_v, |x_1|_v, ..., |x_n|_v\}^{[L:K]n_v} \\
&= H_K(P)^{[L:K]}.
\end{aligned}$$

□

Το ύψος $H_{\mathbb{Q}}$ που ορίσαμε ταυτίζεται βέβαια με το ύψος που ορίσαμε για την απόδειξη του Mordell-Weil για το $\mathbb{Q}$.

Θέλουμε τώρα να ορίσουμε ένα ύψος στον $\mathbb{P}^n(\bar{\mathbb{Q}})$ που να μην εξαρτάται από ένα συγκεκριμμένο σώμα αριθμών.

Ορισμός 2.12.25. *Έστω ένα σημείο P στον προβολικό χώρο $\mathbb{P}^n(\bar{\mathbb{Q}})$. Το απόλυτο ύψος του P ορίζεται ως εξής: αν K είναι ένα σώμα αριθμών με $P \in \mathbb{P}^n(K)$, ορίζουμε το απόλυτο ύψος $H(P)$ του P ως*

$$H(P) = H_K(P)^{1/[K:\mathbb{Q}]},$$

όπου επιλέγουμε την θετική ρίζα.

Η προηγούμενη πρόταση αποδεικνύει ότι το $H(P)$ είναι καλά ορισμένο, ανεξάρτητο απ΄ το K και $H(P) \geq 1$. Το επόμενο θεώρημα είναι αρκετά γενικό, αλλά εμείς θα χρειαστούμε ένα απλό πόρισμα του.

Θεώρημα 2.12.26. *Αν $F : \mathbb{P}^n(\bar{\mathbb{Q}}) \to \mathbb{P}^m(\bar{\mathbb{Q}})$ είναι ένας μορφισμός βαθμού d (δηλαδή δίνεται τοπικά από ομογενή πολυώνυμα βαθμού d), τότε υπάρχουν σταθερές C_1 και C_2, που εξαρτώνται μόνο από τον F, τέτοιες ώστε*

$$C_1 H(P)^d \leq H(F(P)) \leq C_2 H(P)^d$$

για κάθε $P \in \mathbb{P}^n(\bar{\mathbb{Q}})$.

Για την απόδειξη του θεωρήματος 2.12.26 παραπέμπουμε στην βιβλιογραφία ([Silverman, [30], κεφ.8]).

Πόρισμα 2.12.27. *Αν ο A είναι ένα στοιχείο της $GL_{n+1}(\bar{\mathbb{Q}})$ (οπότε ο A επάγει έναν αυτομορφισμό στον $\mathbb{P}^n(\bar{\mathbb{Q}})$), τότε υπάρχουν σταθερές C_1 και C_2, που εξαρτώνται μόνο από τον A, τέτοιες ώστε*

$$C_1 H(P) \leq H(AP) \leq C_2 H(P)$$

για κάθε $P \in \mathbb{P}^n(\bar{\mathbb{Q}})$.

Απόδειξη. Άμεσο πόρισμα του προηγούμενου θεωρήματος για μορφισμούς βαθμού 1. □

Για ένα $x \in \bar{\mathbb{Q}}$, θα συμβολίζουμε με $H(x)$ το $H([x,1])$ και, αν $x \in K$, με $H_K(x)$ το $H_K([x,1])$. Το επόμενο θεώρημα δίνει φράγματα για το μέγεθος των συντελεστών ενός πολυωνύμου συναρτήσει των υψών των ριζών του.

Θεώρημα 2.12.28. *Έστω*

$$f(T) = a_0 T^d + a_1 T^{d-1} + ... + a_d = a_0(T - b_1)...(T - b_d) \in \bar{\mathbb{Q}}[T].$$

Τότε

$$2^{-d} \prod_{j=1}^{d} H(b_j) \leq H([a_0, ..., a_d]) \leq 2^{d-1} \prod_{j=1}^{d} H(b_j)$$

Το θεώρημα 2.12.28, σε συνδυασμό με το επόμενο, δίνει σαν πόρισμα ότι υπάρχουν πεπερασμένα προβολικά σημεία φραγμένου ύψους (θεώρημα 2.12.30).

Θεώρημα 2.12.29. *Έστω $P \in \mathbb{P}^n(\bar{\mathbb{Q}})$ και $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Τότε:*

$$H(P^\sigma) = H(P).$$

Απόδειξη. Έστω $K/\mathbb{Q}$ με $P \in \mathbb{P}^n(K)$. Η επέκταση $K/\mathbb{Q}$ μπορεί να μην είναι Galois, αλλά, σε κάθε περίπτωση, η σ επάγει έναν ισομορφισμό

$$\sigma : K \longrightarrow K^\sigma$$

και, με φυσικό τρόπο, η σ ταυτίζει τις απόλυτες τιμές στα K και K^σ

$$M_K \longrightarrow M_{K^\sigma}$$

μέσω της απεικόνισης

$$\upsilon \longrightarrow \upsilon^\sigma,$$

όπου η υ^σ ορίζεται έτσι ώστε να ισχύει $|x^\sigma|_{\upsilon^\sigma} = |x|_\upsilon$ για κάθε $x \in K$ και $\upsilon \in M_K$. Η σ επάγει επίσης έναν ισομορφισμό

$$K_\upsilon \longrightarrow K^\sigma_{\upsilon^\sigma}$$

έτσι ώστε, εξ' ορισμού, να ισχύει η ισότητα $n_\upsilon = n_{\upsilon^\sigma}$ για τους τοπικούς βαθμούς. Παίρνουμε λοιπόν ότι

$$\begin{aligned} H_{K^\sigma}(P^\sigma) &= \prod_{w \in M_{K^\sigma}} \max\{|x_0^\sigma|_w, |x_1^\sigma|_w, ..., |x_n^\sigma|_w\}^{n_w} \\ &= \prod_{\upsilon \in M_K} \max\{|x_0^\sigma|_{\upsilon^\sigma}, |x_1^\sigma|_{\upsilon^\sigma}, ..., |x_n^\sigma|_{\upsilon^\sigma}\}^{n_{\upsilon^\sigma}} \\ &= \prod_{\upsilon \in M_K} \max\{|x_0|_\upsilon, |x_1|_\upsilon, ..., |x_n|_\upsilon\}^{n_\upsilon} \\ &= H_K(P). \end{aligned}$$

Αφού $[K : \mathbb{Q}] = [K^\sigma : \mathbb{Q}]$, έπεται το ζητούμενο. □

Θεώρημα 2.12.30. *Έστω C και d σταθερές. Τότε το σύνολο*

$$\{P \in \mathbb{P}^n(\bar{\mathbb{Q}}) : H(P) \leq C, [\mathbb{Q}(P) : \mathbb{Q}] \leq d\}$$

είναι πεπερασμένο (όπου με $\mathbb{Q}(P)$ συμβολίζουμε το ελάχιστο σώμα στο οποίο ορίζεται το P). Ειδικότερα, αν K είναι ένα σώμα αριθμών, το σύνολο

$$\{P \in \mathbb{P}^n(K) : H_K(P) \leq C\}$$

είναι πεπερασμένο.

Απόδειξη. Έστω $P \in \mathbb{P}^n(\bar{\mathbb{Q}})$. Επιλέγουμε συντεταγμένες για το P

$$P = [x_0, x_1, ..., x_n]$$

έτσι ώστε κάποια εξ' αυτών να είναι ίση με 1. Τότε έχουμε ότι

$$\mathbb{Q}(P) = \mathbb{Q}(x_0, x_1, ..., x_n),$$

και παίρνουμε την εκτίμηση

$$H_{\mathbb{Q}(P)}(P) = \prod_{\upsilon \in M_{\mathbb{Q}(P)}} \max_{0 \leq i \leq n}\{|x_i|_\upsilon\}^{n_\upsilon}$$

$$\geq \max_{0\leq i\leq n}\left(\prod_{v\in M_{\mathbb{Q}(P)}}\max\{|x_i|_v,1\}^{n_v}\right)$$

$$=\max_{0\leq i\leq n}H_{\mathbb{Q}(P)}(x_i).$$

Άρα, αν $H(P)\leq C$ και $[\mathbb{Q}(P):\mathbb{Q}]\leq d$, τότε θα έχουμε τις ανισότητες

$$\max_{0\leq i\leq n}H_{\mathbb{Q}(P)}(x_i)\leq C$$

και

$$\max_{0\leq i\leq n}[\mathbb{Q}(x_i):\mathbb{Q}]\leq d.$$

Συμπεραίνουμε λοιπόν, πως, για να αποδείξουμε το θεώρημα, αρκεί να το δείξουμε για την περίπτωση $n=1$, δηλαδή αρκεί να δείξουμε την ασθενέστερη πρόταση ότι το σύνολο

$$\{x\in\bar{\mathbb{Q}}:H(x)\leq C,[\mathbb{Q}(x):\mathbb{Q}]\leq d\}$$

είναι πεπερασμένο.

Έστω λοιπόν ένα x στον $\bar{\mathbb{Q}}$, το οποίο ανήκει σε αυτό το σύνολο. Ορίζουμε

$$e=[\mathbb{Q}(x):\mathbb{Q}]\leq d.$$

Επίσης, ορίζουμε $x_1=x$, x_2,..., $x_e\in\bar{\mathbb{Q}}$ τα συζυγή στοιχεία του x. Τότε, το ελάχιστο πολυώνυμο του x πάνω απ΄ το $\mathbb{Q}$ είναι το

$$f_x(T)=\prod_{i=1}^{e}(T-x_i)=T^e+a_1T^{e-1}+...+a_e\in\mathbb{Q}[T].$$

Χρησιμοποιώντας τώρα διαδοχικά τα θεωρήματα 2.12.28 και 2.12.29, και χρησιμοποιώντας επίσης το γεγονός ότι $e\leq d$ και $H(x)\leq C$, παίρνουμε τις εκτιμήσεις:

$$H([1,a_1,a_2,...,a_e])\leq 2^{e-1}\prod_{j=1}^{e}H(x_j)$$

$$=2^{e-1}H(x)^e\leq(2C)^d.$$

Αφού $a_i\in\mathbb{Q}$, έπεται πως για κάθε ζεύγος σταθερών C και d υπάρχουν πεπερασμένες επιλογές για το πολυώνυμο $f_x(T)$ (σε αυτό το βήμα χρησιμοποιούμε το θεώρημα που θέλουμε να δείξουμε για $K=\mathbb{Q}$, το οποίο άμεσα επαληθεύεται πως ισχύει). Όμως, αφού κάθε $f_x(T)$ έχει το πολύ d ρίζες στο K, και αυτές συνεισφέρουν το πολύ d στοιχεία στο σύνολο που έχουμε ορίσει, συμπεραίνουμε ότι το σύνολο αυτό είναι πεπερασμένο. Η απόδειξη είναι πλήρης. □

Θα χρησιμοποιήσουμε λοιπόν τώρα την θεωρία για τα ύψη στον n-διάστατο προβολικό χώρο του $\bar{\mathbb{Q}}$ για να ορίσουμε τις συναρτήσεις ύψους που θέλουμε για τις ελλειπτικές καμπύλες που ορίζονται πάνω από σώματα αριθμών. Έστω λοιπόν K ένα σώμα αριθμών και E/K μια ελλειπτική καμπύλη. Κάθε μη σταθερή συνάρτηση f στον $\bar{K}(E)$ ορίζει ένα μορφισμό επί, τον οποίο συμβολίζουμε επίσης με f

$$f:E\longrightarrow\mathbb{P}^1$$

με $P\to[1,0]$ αν το P είναι πόλος για την f και $P\to[f(P),1]$ αλλιώς.

Ορισμός 2.12.31. *Το (απόλυτο λογαριθμικό) ύψος στον προβολικό χώρο* $\mathbb{P}^n(\bar{\mathbb{Q}})$ *ορίζεται να είναι η συνάρτηση*

$$h : \mathbb{P}^n(\bar{\mathbb{Q}}) \longrightarrow \mathbb{R}$$

με τύπο

$$h(P) = \log(H(P)).$$

Φυσικά, $h(P) \geq 0$ (από την πρόταση 2.12.24).

Ορισμός 2.12.32. *Έστω* E/K *μια ελλειπτική καμπύλη, και μια συνάρτηση* f *στον* $\bar{K}(E)$*. Το ύψος της της* E *ως προς την* f *είναι η συνάρτηση*

$$h_f : E(\bar{K}) \longrightarrow \mathbb{R}$$

που δίνεται από τον τύπο

$$h_f(P) = h(f(P)).$$

Πρόταση 2.12.33. *Έστω* E/K *μια ελλειπτική καμπύλη, και μια συνάρτηση* f *στον* $K(E)$*, μη σταθερή. Τότε, για κάθε σταθερά* C*, το σύνολο*

$$\{P \in E(K) : h_f(P) \leq C\}$$

είναι πεπερασμένο.

Απόδειξη. Η συνάρτηση $f \in K(E)$ ορίζεται πάνω από το K, άρα ένα σημείο $P \in E(K)$ το απεικονίζει σε ένα σημείο $f(P) \in \mathbb{P}^1(K)$. Άρα η f είναι «πεπερασμένα -προς -ένα» απεικόνιση από το σύνολο

$$\{P \in E(K) : h_f(P) \leq C\}$$

στο σύνολο

$$\{Q \in \mathbb{P}^1(K) : H(Q) \leq e^C\}.$$

Όμως, από το θεώρημα 2.12.30, το σύνολο αυτό είναι πεπερασμένο, και το ζητούμενο έπεται. □

Το επόμενο θεώρημα, το οποίο εκφράζει έναν «σχεδόν» κανόνα παραλληλογράμμου (δηλαδή με $O(1)$-απόκλιση), περιγράφει μια θεμελιώδη σχέση μεταξύ των συναρτήσεων της μορφής h_f (που ονομάζονται συναρτήσεις ύψους) και της πράξης της ομάδας στην ελλειπτική καμπύλη.

Υπενθυμίζουμε πως ο συμβολισμός $f \geq g + O(1)$ σημαίνει ότι η συνάρτηση διαφοράς $f - g$ είναι κάτω φραγμένη, ενώ ο συμβολισμός $f \leq g + O(1)$ σημαίνει ότι η συνάρτηση διαφοράς $f - g$ είναι άνω φραγμένη. Αν ισχύουν και οι δύο συνθήκες, γράφουμε $f = g + O(1)$.

Θεώρημα 2.12.34 (κανόνας παραλληλογράμμου)**.** *Έστω* E/K *μια ελλειπτική καμπύλη, και* $f \in K(E)$ *μια άρτια συνάρτηση (δηλαδή μια* f *τέτοια ώστε* $f \circ [-1] = f$*). Τότε, για κάθε* P *και* Q *στην* $E(\bar{K})$ *ισχύει*

$$h_f(P + Q) + h_f(P - Q) = 2h_f(P) + 2h_f(Q) + O(1),$$

όπου η σταθερά στο $O(1)$ *εξαρτάται μόνον από τις* E *και* f*.*

Απόδειξη. Διαλέγουμε μια εξίσωση Weierstrass της μορφής

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

για την καμπύλη E/K (τέτοια εξίσωση υπάρχει επειδή είμαστε σε σώμα χαρακτηριστικής 0). Θα δείξουμε πρώτα το ζητούμενο για την άρτια συνάρτηση $f = x$.

Αφού $h_x(O) = 0$ και $h_x(-P) = h_x(P)$, το ζητούμενο είναι προφανές για $P = O$ ή $Q = O$. Αν $P \neq O$ και $Q \neq O$, έχουμε

$$x(P) = [x_1, 1],$$

$$x(Q) = [x_2, 1],$$

$$x(P + Q) = [x_3, 1],$$

$$x(P - Q) = [x_4, 1],$$

για κάποια x_i (όπου μπορεί το x_3 ή το x_4 να απειρίζονται αν $P = \pm Q$). Οι τύποι για την πράξη της ομάδας $E(K)$ δίνουν τις σχέσεις

$$x_3 + x_4 = \frac{2(x_1 + x_2)(A + x_1x_2) + 4B}{(x_1 + x_2)^2 - 4x_1x_2},$$

$$x_3x_4 = \frac{(x_1x_2 - A)^2 - 4B(x_1 + x_2)}{(x_1 + x_2)^2 - 4x_1x_2}.$$

Ορίζουμε την απεικόνιση $g : \mathbb{P}^2 \to \mathbb{P}^2$ με

$$g([t, u, v]) = [u^2 - 4tv, 2u(At + v) + 4Bt^2, (v - At)^2 - 4Btu].$$

Έστω $G : E \times E \to E \times E$ με $G(P, Q) = (P + Q, P - Q)$ και $\sigma : E \times E \to \mathbb{P}^2$ η σύνθεση των απεικονίσεων

$$E \times E \to \mathbb{P}^1 \times \mathbb{P}^1, (P, Q) \to (x(P), x(Q)),$$

και

$$\mathbb{P}^1 \times \mathbb{P}^1 \to \mathbb{P}^2, ([a_1, b_1], [a_2, b_2]) \to [b_1b_2, a_1b_2 + a_2b_1, a_1a_2].$$

Οι εκφράσεις για τα x_3+x_4 και x_3x_4 μας δίνουν ότι $\sigma \circ G = g \circ \sigma$. Αν τώρα δούμε τα 1, $x_1 + x_2$ και x_1x_2 ως t, u και v, τότε παίρνουμε $g([t, u, v]) = [1, x_3 + x_4, x_3x_4]$. Θέλουμε τώρα να δείξουμε ότι η g είναι μορφισμός. Είναι απλό να δει κανείς ότι μια ρητή απεικόνιση $\phi = [\phi_0, ..., \phi_n]$ από τον m-διάστατο προβολικό χώρο στον n-διάστατο χώρο είναι μορφισμός (υποθέτωντας ότι τα ϕ_i δεν έχουν κοινούς παράγοντες) αν και μόνον αν τα ϕ_i δεν έχουν κοινές ρίζες στον $\mathbb{P}^m$. Για να δείξουμε λοιπόν το ζητούμενο, αρκεί να δείξουμε ότι τα ομογενή πολυώνυμα που ορίζουν την g δεν έχουν κοινές ρίζες εκτός των $t = u = v = 0$.

Έστω λοιπόν $g([t, u, v]) = 0$. Αν $t = 0$, τότε, απ΄ τον τύπο της g έπεται ότι $u = v = 0$. Αν $t \neq 0$, ορίζουμε την μεταβλητή $x = u/2t$, οπότε η εξίσωση $u^2 = 4tv$ γίνεται $x^2 = v/t$. Διαιρούμε με t^2 τις εξισώσεις

$$2u(At + v) + 4Bt^2 = 0$$

$$(v - At)^2 - 4Btu = 0$$

και, αντικαθιστώντας το x σε αυτές, παίρνουμε τις εξισώσεις

$$\psi(x) = 4x^3 + 4Ax + 4B = 0,$$

$$\phi(x) = x^4 - 2Ax^3 - 8Bx + A^2 = 0.$$

Σε αυτό το σημείο, παρατηρεί κανείς ότι, από την πρόταση 2.2.4, $x([2]P) = \phi(x)/\psi(x)$. Για να δείξουμε ότι τα $\phi(x)$ και $\psi(x)$ δεν έχουν κοινές ρίζες, χρησιμοποιούμε την σχέση

$$(12X^2 + 16A)\phi(X) - (3X^3 - 5AX - 27B)\psi(X) = 4(4A^3 + 27B^2) \neq 0,$$

την οποία έχουμε ήδη χρησιμοποιήσει στο λήμμα 2.12.18. Η σχέση αυτή μας δίνει ότι τα $\phi(x)$ και $\psi(x)$ δεν έχουν κοινές ρίζες, και άρα η g είναι μορφισμός. Χρησιμοποιούμε τώρα την σχέση $\sigma \circ G = g \circ \sigma$, και υπολογίζουμε

$$h(\sigma(P+Q, P-Q)) = h(\sigma \circ G(P,Q)) = h(g \circ \sigma(P,Q))$$

το οποίο, από το θεώρημα 2.12.26 (για μορφισμούς βαθμού 2), ισούται με

$$2h(\sigma(P,Q)) + O(1).$$

Αν τώρα $R_1 = O$ ή $R_2 = O$, τότε είναι προφανές ότι

$$h(\sigma(R_1, R_2)) = h_x(R_1) + h_x(R_2).$$

Διαφορετικά, γράφουμε $x(R_1) = [a_1, 1]$ και $x(R_2) = [a_2, 1]$, και έχουμε τις σχέσεις

$$h(\sigma(R_1, R_2)) = h([1, a_1 + a_2, a_1 a_2]),$$

$$h_x(R_1) + h_x(R_2) = h(a_1) + h(a_2).$$

Εφαρμόζουμε το θεώρημα 2.12.28 στο πολυώνυμο $(T+a_1)(T+a_2)$, το οποίο δίνει

$$h(a_1) + h(a_2) - \log 4 \leq h([1, a_1 + a_2, a_1 a_2]) \leq h(a_1) + h(a_2) + \log 2$$

ή, ισοδύναμα,

$$h(\sigma(R_1, R_2)) = h_x(R_1) + h_x(R_2) + O(1).$$

Εφαρμόζωντας αυτήν την σχέση στην εξίσωση

$$h(\sigma(P+Q, P-Q)) = 2h(\sigma(P,Q)) + O(1)$$

έχουμε το ζητούμενο.

Για την γενική περίπτωση, δηλαδή για την τυχαία άρτια συνάρτηση στον $K(E)$, θα χρησιμοποιήσουμε το ακόλουθο λήμμα:

Λήμμα 2.12.35. *Αν οι f, $g \in K(E)$ είναι άρτιες, τότε*

$$(\deg g) h_f = (\deg f) h_g + O(1).$$

Απόδειξη. Έστω x και $y \in K(E)$ οι Weierstrass συντεταγμένες συναρτήσεις για την E/K. Από το πόρισμα 2.2.6, ξέρουμε ότι τα άρτια στοιχεία του $K(E)$ είναι αριβώς τα στοιχεία του $K(x)$, κι έτσι, μπορούμε να βρούμε μια συνάρτηση $r(x) \in K(x)$, έτσι ώστε, $x \circ r \equiv f$ ως συναρτήσεις από την E στο $\mathbb{P}^1$. Από την πρόταση 1.2.5, έπεται ότι η r είναι μορφισμός. Εφαρμόζωντας το θεώρημα 2.12.26, παίρνουμε ότι

$$h_f = h_x \circ r = (\deg r) h_x + O(1).$$

Όμως, από την σχέση $x \circ r \equiv f$, έχουμε επίσης ότι

$$\deg f = (\deg x)(\deg r) = 2 \deg r,$$

άρα

$$2h_f = (\deg f)h_x + O(1).$$

Ομοίως λαμβάνουμε ότι

$$2h_g = (\deg g)h_x + O(1).$$

Συνδυάζοντας τις δύο αυτές σχέσεις, έχουμε το ζητούμενο. □

Για να ολοκληρώσουμε την απόδειξη του θεωρήματος 2.12.34, εφαρμόζουμε το λήμμα 2.12.35 για $g \equiv x$. Αφού $\deg x = 2$, παίρνουμε

$$h_f = \frac{1}{2}(\deg f)h_x + O(1).$$

Πολλαπλασιάζουμε τώρα την σχέση

$$h_x(P+Q) + h_x(P-Q) = 2h_x(P) + 2h_x(Q) + O(1),$$

που δείξαμε πριν, με $\frac{1}{2}\deg f$, και παίρνουμε

$$h_f(P+Q) + h_f(P-Q) = 2h_f(P) + 2h_f(Q) + O(1),$$

η οποία είναι η σχέση που θέλαμε να αποδείξουμε. □

Η επόμενη πρόταση δείχνει ότι οι συναρτήσεις ύψους που ορίσαμε ικανοποιούν τις βασικές ιδιότητες που θέλουμε να ικανοποιούν τα ύψη.

Πόρισμα 2.12.36. *Έστω E/K μια ελλειπτική καμπύλη, και μια άρτια $f \in K(E)$. Τότε:*

(i) *Έστω $Q \in E(\bar{K})$. Τότε:*

$$h_f(P+Q) \le 2h_f(P) + O(1),$$

για κάθε P στην $E(\bar{K})$, όπου η σταθερά στο $O(1)$ εξαρτάται μόνο από τις E, f και το Q.

(ii) *Έστω m ένας ακέραιος αριθμός. Τότε*

$$h_f([m]P) = m^2 h_f(P) + O(1),$$

για κάθε P στην $E(\bar{K})$, όπου η σταθερά στο $O(1)$ εξαρτάται μόνο από τις E, f και το m.

Απόδειξη. (i) Άμεσο από το θεώρημα 2.12.34 και το γεγονός ότι $h_f(P-Q) \ge 0$.

(ii) Λόγω της αρτιότητας της f, αρκεί να δείξουμε το ζητούμενο για $m \geq 0$. Η απόδειξη θα γίνει με επαγωγής στο m. Για $m = 0$ και $m = 1$, το ζητούμενο είναι προφανές. Έστω λοιπόν ότι το ζητούμενο είναι αληθές για $m - 1$ και m. Εφαρμόζωντας το θεώρημα για $[m]P$ και P, θα έχουμε:

$$h_f([m+1]P) = -h_f([m-1]P) + 2h_f([m]P) + 2h_f(P) + O(1)$$

$$= (-(m-1)^2 + 2m^2 + 2)h_f(P) + O(1)$$

$$= (m+1)^2 h_f(P) + O(1),$$

και αυτό ολοκληρώνει την επαγωγή.

□

Είμαστε τώρα σε θέση να αποδείξουμε το θεώρημα Mordell-Weil για το τυχόν σώμα αριθμών K. Στην πραγματικότητα, έχουμε αναπτύξει όλα τα εργαλεία που χρειαζόμαστε, και η απόδειξη συνίσταται, όπως και στο Mordell-Weil για το $\mathbb{Q}$, απλώς στο να συνδέσει κανείς όλα τα επιμέρους βήματα, ορίζοντας την συνάρτηση ύψους που θα δουλέψει για να δώσει το ζητούμενο και εφαρμόζωντας στην συνέχεια το θεώρημα της Καθόδου.

Απόδειξη. Αποδεικνύουμε το θεωρήμα Mordell-Weil (2.12.1) για τυχόν σώμα αριθμών K. Επιλέγουμε μια οποιαδήποτε άρτια συνάρτηση f στον $K(E)$, π.χ. μπορούμε να επιλέξουμε την συνάρτηση x της εξίσωσης Weierstrass. Θεωρούμε την συνάρτηση ύψους h_f. Η h_f έχει τις εξής ιδιότητες:

(i) Έστω $Q \in E(K)$. Τότε, υπάρχει μια σταθερά C_1, που εξαρτάται μόνο από τις E, f και το Q, τέτοια ώστε:

$$h_f(P+Q) \leq 2h_f(P) + C_1,$$

για κάθε P στην $E(K)$ (Πόρισμα 2.12.36, ισχυρισμός (i).

(ii) Υπάρχει σταθερά C_2, που εξαρτάται μόνο από τις E και f, τέτοια ώστε:

$$h_f([2]P) \geq 4h_f(P) - C_2,$$

για κάθε P στην $E(K)$ (Πόρισμα 2.12.36, ισχυρισμός (ii) για $m = 2$).

(iii) Για κάθε σταθερά C_3, το σύνολο

$$\{P \in E(K) : h_f(P) \leq C_3\}$$

είναι πεπερασμένο (Πρόταση 2.12.33).

Εφαρμόζουμε τώρα το Ασθενές θεώρημα Mordell-Weil και το θεώρημα της Καθόδου, και το ζητούμενο έπεται. □

2.13 Περαιτέρω θέματα αριθμητικής των ελλειπτικών καμπυλών

2.13α΄ Η δομή της torsion υποομάδας

Πριν τελειώσουμε την μελέτη των ελλειπτικών καμπυλών, είναι ίσως χρήσιμο να σημειώσουμε κάποια θεωρήματα που αφορούν την δομή και τον υπολογισμό της $E(\mathbb{Q})$, και εν γένει της $E(K)$.

Όπως δείξαμε, υπάρχει ένας ισομορφισμός αβελιανών ομάδων:

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \times E(\mathbb{Q})_{tors}$$

και, όπως σημειώσαμε, ο αριθμός r ονομάζεται rakn (τάξη) της $E(\mathbb{Q})$, και τα σημεία της $E(\mathbb{Q})_{tors}$ ονομάζονται torsion σημεία της $E(\mathbb{Q})$ (ή σημεία στρέψης). Ο υπολογισμός της δομής που μπορεί να έχει η υποομάδα στρέψης της $E(\mathbb{Q})$ και τι τάξης στοιχεία μπορεί να περιέχει αποτελούσε για χρόνια γόνιμο πεδίο έρευνας. Το 1935 και το 1937, οι Nagell και Lutz έδειξαν ανεξάρτητα το εξής:

Θεώρημα 2.13.1 (Nagell-Lutz)**.** *Έστω μια ελλειπτική καμπύλη $E/\mathbb{Q}$ με εξίσωση Weierstrass $y^2 = x^3 + Ax + B$, όπου $A, B \in \mathbb{Z}$. Υποθέτουμε ότι η $E(\mathbb{Q})$ έχει ένα μη μηδενικό σημείο στρέψης P. Τότε:*

(i) *$x(P), y(P) \in \mathbb{Z}$.*

(ii) *Αν $[2]P \neq O$ τότε το $y(P)^2$ διαιρεί την διακρίνουσα $4A^3 + 27B^2$.*

Για να το αποδείξουμε, θα χρειαστούμε το εξής θεώρημα, το οποίο αποτελεί μια αναδιατύπωση του θεωρήματος 2.8.10 του Cassels για την περίπτωση των σωμάτων αριθμών:

Θεώρημα 2.13.2 (Αναδιατύπωση του 2.8.10 για σώματα αριθμών)**.** *Έστω K ενα σώμα αριθμών και μια ελλειπτική καμπύλη E/K με εξίσωση Weierstrass*

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

ούτως ώστε ολα τα a_i να ανήκουν στους ακέραιους R του K. Έστω P ένα σημείο της $E(K)$ με τάξη $m \geq 2$. Τότε:

(i) *Αν το m δεν είναι δύναμη πρώτου, τότε $x(P), y(P) \in R$.*

(ii) *Αν $m = p^n$, τότε, για κάθε $\upsilon \in M_K^0$, ορίζουμε*

$$r_\upsilon = \left[\frac{\mathrm{ord}_\upsilon(p)}{p^n - p^{n-1}} \right],$$

όπου $[x]$ είναι, ως συνήθως, το ακέραιο μέρος του x. Τότε:

$$\mathrm{ord}_\upsilon(x(P)) \geq -2r_\upsilon$$

και

$$\mathrm{ord}_\upsilon(y(P)) \geq -3r_\upsilon.$$

Ιδιαίτερα, αν $\mathrm{ord}_\upsilon(p) = 0$, τότε τα $x(P)$ και $y(P)$ είναι υ-ακέραια.

Αποδεικνύουμε τώρα το Nagell-Lutz.

Απόδειξη. (i) Έστω m η τάξη του P. Αν $m = 2$, τότε $y(P) = 0$, τότε το $x(P)$ είναι ακέραιος, επειδή είναι λύση μονικού πολυωνύμου με ακέραιους συντελεστές. Αν $m > 2$, τότε, αν ο m δεν είναι δύναμη πρώτου, το ζητούμενο έπεται από το ερώτημα (i) του θεωρήματος 2.13.2, ενώ αν ο m είναι δύναμη πρώτου, θα έχουμε $r_v = 0$ για την ποσότητα του ερωτήματος (ii) του θεωρήματος 2.13.2, το οποίο αποδεικνύει το ζητούμενο.

(ii) Έστω ότι $[2]P \neq O$, δηλαδή $y(P) \neq 0$. Εφαρμόζωντας το (i) για τα σημεία P και $[2]P$, παίρνουμε ότι $x(P)$, $y(P)$ και $x([2]P) \in \mathbb{Z}$. Θεωρούμε τα πολυώνυμα

$$\phi(X) = X^4 - 2AX^2 - 8BX + A^2$$

και

$$\psi(X) = X^3 + AX + B.$$

Σύμφωνα με τους τύπους που ξέρουμε ότι δίνουν τις συντεταγμένες του $[2]P$,

$$x([2]P) = \frac{\phi(x(P))}{4\psi(x(P))}.$$

Ξέρουμε όμως και την γνωστή σχέση μεταξύ των ϕ και ψ την οποία έχουμε χρησιμοποιήσει και προηγουμένως, την οποία υπενθυμίζουμε εδώ:

$$f(X)\phi(X) - g(X)\psi(X) = 4A^3 + 27B^2$$

όπου $f(X) = 3X^2+4A$ και $g(X) = 3X^3-5AX-27B$. Θέτουμε $X = x(P)$ και χρησιμοποιούμε τον τύπο για το $x([2]P)$ καθώς και το ότι $y(P)^2 = \psi(x(P))$, οπότε η προηγούμενη εξίσωση παίρνει την μορφή

$$y(P)^2\,(4f(x(P))x([2]P) - g(x(P))) = 4A^3 + 27B^2,$$

και από το γεγονός ότι όλοι οι αριθμοί στην εξίσωση είναι ακέραιοι έπεται ότι $y(P)^2 | 4A^3 + 27B^2$.

□

Το Nagell-Lutz μας δίνει έναν (όχι γρήγορο) αλγόριθμο για τον υπολογισμό της υποομάδας στρέψης μιας ελλειπτικής καμπύλης (παρατηρείστε ότι το P έχει τάξη 2 αν και μόνο αν $x(P) = 0$). Ωστόσο, παρέμενε για χρόνια ανοικτό ερώτημα οι δυνατές δομές της $E(\mathbb{Q})_{tors}$. Για παράδειγμα, το 1940 οι Billing και Mahler έδειξαν ([3]) ότι η $E(\mathbb{Q})$ δεν μπορεί να έχει στοιχείο τάξης 11. Μια σειρά απο αποτελέσματα ενοποιηθήκαν από τον Mazur ([18]), ο οποίος το 1978 έδειξε το εξής θεώρημα:

Θεώρημα 2.13.3 (Mazur)**.** *Έστω μια ελλειπτική καμπύλη $E/\mathbb{Q}$. Τότε η $E(\mathbb{Q})_{tors}$ είναι ισόμορφη είτε με μια εκ των*

$$\mathbb{Z}/n\mathbb{Z}$$

όπου $n = 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$ ή 12, είτε με μια εκ των

$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z}$$

όπου $n = 1, 2, 3,$ ή 4. Επίσης, κάθε μια απ΄ αυτές τις διαφορετικές δυνατές υποομάδες εμφανίζεται ως υποομάδα στρέψης κάποιας $E/\mathbb{Q}$.

Μια σειρά από εργασίες του Kamienny και άλλων γενικεύθηκαν στο εξής αποτέλεσμα:

Θεώρημα 2.13.4 (Merel). *Έστω d ένας φυσικός αριθμός. Τότε, υπάρχει μια σταθερά N που εξαρτάται μόνο από τον d τέτοια ώστε αν το σώμα αριθμών K έχει βαθμό επέκτασης $\leq d$ τότε να ισχύει*

$$|E(K)_{tors}| \leq N$$

Για μια εκτενέστερη συζήτηση πάνω στα torsion σημεία μιας ελλειπτικής καμπύλης καθώς και πιο γρήγορους τρόπους υπολογισμού της $E(\mathbb{Q})_{tors}$ παραπέμπουμε στους [Silverman, [30], κεφ.8], [Hindry-Silverman, [11]] ή [Silverman-Tate, [32], κεφ.2].

2.13β′ Η rank μιας ελλειπτικής καμπύλης

Το έτερον πρόβλημα που σχετίζεται με την ομάδα Mordell-Weil είναι αυτό του υπολογισμού της τάξης της ελευθέρας στρέψης υποομάδας της. Το πρόβλημα αυτό είναι σαφώς πιο δύσκολο. Είναι ανοιχτό ερώτημα κατα πόσον υπάρχει ένα άνω φράγμα στις τάξεις ή εάν μπορούμε να βρίσκουμε καμπύλη με οσοδήποτε μεγάλη τάξη. Το 1992, ο Mestre κατασκεύασε μια ελλειπτική καμπύλη με τάξη 15, και περαιτέρω τεχνικές που αναπτύχθηκαν από τον Mestre και άλλους έχουν οδηγήσει σε παραδείγματα μεγαλύτερης τάξης. Η καμπύλη

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

όπου

$$A = 20067762415575526585033208209338542750930230312178956502$$

$$B = 3448161179503055646703298569039072037485594435931918 03$$

$$612660082962919394487322434 29$$

έχει αποδειχθεί, από τον Elkies, ότι έχει τάξη τουλάχιστον 28. Η rank μιας ελλειπτικής καμπύλης συνδέεται με την διάσημη Εικασία των Birch-Swinnerton-Dyer, για την οποία θα πούμε περισσότερα στο κεφάλαιο 5.

2.13γ′ Ακέραια σημεία

Το θεώρημα Mordell-Weil είναι ένα από τα σημαντικότερα θεωρήματα για την δομή των ομάδων $E(K)$. Ένα εξίσου σημαντικό είναι το Θεώρημα του Siegel:

Θεώρημα 2.13.5 (Siegel). *Έστω E/K. Τότε η $E(K)$ έχει πεπερασμένα ακέραια σημεία.*

Πιο γενικά, το θεώρημα του Siegel ισχύει για καμπύλη C οποιουδήποτε γένους. Σε αυτό το σημείο παρατηρούμε την διαφορά των ελλειπτικών καμπυλών σε σχέση με τις δευτεροβάθμιες εξισώσεις, όπου μπορεί μια κωνική τομή να έχει άπειρες ακέραιες λύσεις, όπως συμβαίνει για παράδειγμα στις εξισώσεις του Pell:

$$X^2 - DY^2 = 0$$

οι οποίες έχουν άπειρες ακέραιες λύσεις όταν το D δεν είναι τετράγωνο.

2.13δ΄ Γενικεύσεις

Τέλος, αξίζει πριν κλείσουμε αυτό το κεφάλαιο να αναφερθούμε σε δύο γενικεύσεις, προς διαφορετική κατεύθυνση, του θεωρήματος Mordell-Weil. Η πρώτη είναι το φημισμένο Θεώρημα του Faltings σχετικά με την δομή των καμπυλών μεγαλύτερου γένους:

Θεώρημα 2.13.6 (Faltings)**.** *Έστω C/K μια nonsingular πλήρης καμπύλη γένους $g \geq 2$. Τότε, η $C(K)$ είναι πεπερασμένη.*

Το εντυπωσιακό αυτό θεώρημα αυτό, για το οποίο ο Faltings τιμήθηκε με το μετάλλιο Fields το 1983, ήταν ανοιχτή εικασία από την δεκαετία του 1920, γνωστή ως Εικασία του Mordell. Σαν πόρισμα προκύπτει π.χ. ότι η εξίσωση του Fermat

$$x^n + y^n = 1$$

έχει το πολύ πεπερασμένες λύσεις (η εξίσωση του Fermat έχει γένος $\frac{n^2-n}{2}$). Επίσης, το θεώρημα του Faltings συνεπάγεται το θεώρημα του Siegel για $g > 1$.

Μια δεύτερη σημαντική κατεύθυνση γενίκευσης έγκειται στην γενίκευση του Mordell-Weil για αβελιανές varieties. Σε γενικές γραμμές, μια variety λέγεται αβελιανή αν μπορεί να εφοδιαστεί με μια δομή ομάδας (η οποία προκύπτει να είναι αβελιανή). Ο λόγος που το Mordell-Weil φέρει αυτό το όνομα είναι επειδή ο Weil, το 1928, έδειξε, στην διδακτορική του διατριβή, την παρακάτω γενίκευση του θεωρήματος του Mordell (και του θεωρήματος Mordell-Weil που δείξαμε για τις $E(K)$):

Θεώρημα 2.13.7 (Mordell-Weil για αβελιανές varieties)**.** *Έστω A μια αβελιανή variety που ορίζεται πάνω από ένα σώμα αριθμών K. Τότε, η ομάδα $A(K)$ των K-ρητών σημείων της είναι πεπερασμένα παραγόμενη.*

Η διαδικασία της απόδειξης, η οποία γενικεύει την μέθοδο που εφαρμόσαμε για την απόδειξη του Mordell-Weil για ελλειπτικές καμπύλες, βασίζεται επίσης στο λήμμα της καθόδου και την κατασκευή μιας συνάρτησης ύψους. Μια απόδειξη του αποτελέσματος αυτού, όπως επίσης και μια απόδειξη του θεωρήματος του Siegel και μια απλουστευμένη απόδειξη του θεωρήματος του Faltings από τους Vojta και Bombieri, υπάρχει στο [Hindry-Silverman, [11], κεφ. 3, 4, 5].

Κεφάλαιο 3

Ομάδες Fuchs και Επιφάνειες Riemann

Αρχικά, θα αναφερθούμε σε κάποια γενική θεωρία σχετικά με τις τοπολογικές ομάδες και τις δράσεις τους σε τοπολογικούς χώρους, καθώς και σε κάποια βασικά στοιχεία από την θεωρία των επιφανειών Riemann. Σταδιακά, θα αρχίσουμε να μελετάμε κυρίως χώρους πηλίκα του άνω μιγαδικού επιπέδου, οπότε και το πλαίσιο αναφοράς μας θα γίνει πιο συγκεκριμμένο. Στην παρούσα παράγραφο ακολουθούμε κυρίως την έκθεση στον [Milne, [22], κεφ.1,2] και στους [Diamond-Shurman, [8], κεφ.2]. Καθώς κι αυτό το κεφάλαιο είναι, όπως και το πρώτο, εισαγωγικό, μικρή έμφαση δίνεται στις αποδείξεις, καθώς στόχος μας είναι κυρίως μια εισαγωγή στις βασικές έννοιες. Για τις αποδείξεις που λείπουν παραπέμπουμε στους [Milne, [22], κεφ.1,2], [Silverman, [31], κεφ. 1], [Apostol, [2], κεφ. 1,2] και [Diamond-Shurman, [8], κεφ. 1,2].

3.1 Τοπολογικές ομάδες

Σ′ αυτήν την εισαγωγή, υποθέτουμε πως κάθε τοπικά συμπαγής τοπολογικός χώρος είναι Hausdorff.

Ορισμός 3.1.1. *Μια ομάδα G εφοδιασμένη με μια τοπολογία ώστε οι απεικονίσεις*

$$(g,h) \in G \times G \to gh \in G$$
$$g \in G \to g^{-1} \in G$$

να είναι συνεχείς λέγεται τοπολογική ομάδα.

Ορισμός 3.1.2. *Έστω ότι η G δρα σε έναν τοπολογικό χώρο X, μέσω μιας δράσης*

$$\phi : G \times X \to X : (g,x) \to \phi(g,x) = gx.$$

Αν η απεικόνιση αυτή είναι συνεχής, τότε λέμε ότι η G δρα συνεχώς στον X.

Παρατηρούμε ότι ο πολλαπλασιασμός με g, όπου $g \in G$, είναι ομοιομορφισμός. Έστω τώρα ένα $x \in X$. Ως συνήθως, ορίζουμε τα σύνολα:

$$Gx = \{gx, g \in G\},$$
$$\mathrm{stab}(x) = \{g \in G : gx = x\}.$$

Ορισμός 3.1.3. *Το $Gx \subseteq X$ ονομάζεται τροχιά του x. Ισοτροπική ομάδα στο x ονομάζουμε την σταθεροποιούσα* $\mathrm{stab}(x) \leq G$ *του x.*

Παρατηρούμε ότι η ισοτροπική ομάδα είναι η αντίστροφη εικόνα του x για την συνεχή απεικόνιση:

$$G \longrightarrow X : g \longrightarrow gx$$

Αυτό μας δίνει ότι αν ο X είναι Hausdorff , τότε η $\mathrm{stab}(x)$ είναι κλειστή υποομάδα.

Υενθυμίζουμε την γνωστή (από την θεωρία ομάδων) 1-1 και επί απεικόνιση

$$G/\mathrm{stab}(x) \longrightarrow Gx$$

$$g \cdot \mathrm{stab}(x) \longrightarrow gx.$$

Συμβολίζουμε με $G\backslash X$ τον χώρο (πηλίκο) των τροχιών με την επαγόμενη τοπολογία. Τότε, ως γνωστόν, η απεικόνιση πηλίκο

$$p : X \longrightarrow G\backslash X$$

είναι συνεχής και ανοιχτή.

Έστω H μια υποομάδα της G. Η H δρα στην G από αριστερά και από δεξιά με προφανή τρόπο, και με $H\backslash G$ και G/H συμβολίζουμε τους χώους πηλίκα των αριστερών και των δεξιών συμπλόκων αντίστοιχα.

Λήμμα 3.1.4. *Ο χώρος G/H είναι Hausdorff αν και μόνο αν η H είναι κλειστή υποομάδα της G.*

Αν η G δρα μεταβατικά στον X τότε $Gx = X$ για κάθε x στον X, και αν η δράση είναι συνεχής, έχουμε:

Πρόταση 3.1.5. *Αν μια τοπικά συμπαγής και Hausdorff τοπολογική ομάδα G δρα συνεχώς και μεταβατικά στον τοπικά συμπαγή και Hausdorff τοπολογικό χώρο X και η G έχει αριθμήσιμη βάση για την τοπολογία της, τότε η απεικόνιση*

$$\phi : G/\mathrm{stab}(x) \longrightarrow X$$

$$g \cdot \mathrm{stab}(x) \longrightarrow gx$$

είναι ομομορφισμός.

Αν η G δρα στον X και ο χώρος $G\backslash X$ είναι Hausdorff τότε οι τροχιές είναι κλειστές, αλλά όπως είναι αναμενόμενο η αντίστροφη συνεπαγωγή δεν ιχύει αυτόματα. Αναζητούμε συνθήκες για τον τρόπο που δρα η G που να μας εξασφαλίζουν ότι το πηλίκο θα είναι Hausdorff.

Ορισμός 3.1.6. *Η δράση της G στον X λέγεται ασυνεχής αν για κάθε $x \in X$ και ακολουθία (g_i) στην G, η ακολουθία $(g_i x)$ δεν έχει σημεία συσσώρευσης στον X, και λέγεται γνήσια ασυνεχής αν για κάθε x και y στον X υπάρχουν περιοχές τους U_x και U_y αντίστοιχα ώστε το σύνολο*

$$G_{xy} = \{\gamma \in G : \gamma U_x \cap U_y \neq \emptyset\}$$

να είναι πεπερασμένο.

Πρόταση 3.1.7. *Έστω μια τοπικά συμπαγής ομάδα G που δρα στον τοπολογικό χώρο X τέτοια ώστε για κάθε $x \in X$ η σταθεροποιούσα K του x στην G να είναι συμπαγής και η απεικόνιση*

$$G/K \longrightarrow X : gK \longrightarrow gx$$

να είναι ομοιομορφισμός. Τότε, για μια υποομάδα Γ της G τα ακόλουθα είναι ισοδύναμα:

(i) *Η Γ δρα ασυνεχώς στον X.*

(ii) *Η Γ δρα γνήσια ασυνεχώς στον X.*

(iii) *Για κάθε δύο συμπαγή υποσύνολα A και B του X το σύνολο $\Gamma_{AB} = \{\gamma \in \Gamma : \gamma A \cap B \neq \emptyset\}$ είναι πεπερασμένο.*

(iv) *Η Γ είναι διακριτή υποομάδα της G*

Πρόταση 3.1.8. *Αν οι G, K, X είναι όπως στην προηγούμενη πρόταση και η Γ είναι μια διακριτή υποομάδα της G, τότε ισχύουν τα εξής:*

(i) *Για κάθε $x \in X$ το $\{g \in \Gamma : gx = x\}$ είναι πεπερασμένο.*

(ii) *Για κάθε $x \in X$ υπάρχει μια περιοχή του U_x τέτοια ώστε αν $\gamma \in \Gamma$ και $U_x \cap \gamma U_x \neq \emptyset$ τότε $\gamma x = x$.*

(iii) *Για κάθε x, y που δεν ανήκουν στην ίδια τροχιά της Γ υπάρχουν περιοχές U_x, U_y των x και y αντίστοιχα τέτοιες ώστε $\gamma U_x \cap U_y = \emptyset$ για κάθε $\gamma \in \Gamma$.*

Το σημαντικό των παραπάνω αποτελεσμάτων είναι ότι μας δίνουν μια συνθήκη για να είναι ο χώρος πηλίκο Huasdorff.

Πόρισμα 3.1.9. *Αν οι G, X, K και Γ είναι όπως στις υποθέσεις της πρότασης 3.1.8, τότε ο χώρος πηλίκο $\Gamma\backslash X$ είναι Hausdorff.*

Απόδειξη. Διαλέγουμε x και y που να μην ανήκουν στην ίδια τροχιά της Γ. Αν διαλέξουμε περιοχές U_x και U_y των x και y όπως στην προηγούμενη πρόταση, τότε οι εικόνες τους στον χώρο πηλίκο είναι ξένες περιοχές των Γx και Γy. □

Ορισμός 3.1.10. *Μια δράση λέγεται ελεύθερη αν* $\mathrm{stab}(x) = 1_G$ *για κάθε $x \in X$.*

Τα παραπάνω γενικά αποτελέσματα θα τα χρησιμοποιήσουμε παρακάτω για να μελετήσουμε την δράση των Fuchsian ομάδων στο άνω μιγαδικό επίπεδο. Πρώτα όμως θα δούμε κάποια στοιχεία από την θεωρία των επιφανειών Riemann που θα μας φανούν επίσης χρήσιμα στην μελέτη των χώρων πηλίκο που θα προκύψουν από τις δράσεις αυτές.

3.2 Επιφάνειες Riemann

Σε αυτήν την παράγραφο αναπτύσουμε σύντομα τα στοιχεία από την θεωρία των επιφανειών Riemann που θα χρειαστούμε για την εργασία αυτήν. Θα παρατηρήσει κάποιος πως από ένα σημείο και μετά η θεωρία για τις συμπαγείς επιφάνειες Riemann που θα παρουσιάζουμε εδώ θα ταυτίζεται ουσιαστικά με την θεωρία που παρουσιάσαμε στο κεφάλαιο 1 για τις καμπύλες. Αυτό το γεγονός υποψιάζει κάποιον πως οι συμπαγείς επιφάνειες Riemann πρέπει να είναι αλγεβρικές καμπύλες. Αυτό είναι σωστό. Πιο συγκεκριμμένα, μπορεί κανείς να δείξει ότι κάθε συμπαγής επιφάνεια Riemann δέχεται με φυσιολογικό τρόπο δομή λείας καμπύλης. Θα δούμε εν συντομία πως προκύπτει αυτό το θεώρημα για συγκεκριμμένες περιπτώσεις παρακάτω. Προς το παρόν, αφιερώνουμε λίγες σελίδες παραπάνω για την ακριβή διατύπωση και τον φορμαλισμό των αποτελεσμάτων που θέλουμε στο πλαίσιο των επιφανειών Riemann. Αφού έχουμε ήδη δει κάποιες επιφάνειες Riemann στο κεφάλαιο 2, δεν θα πρέπει να εκπλήσσεται κάποιος που αυτές εμφανίζονται ξανά παρακάτω στην θεωρία των ελλειπτικών καμπυλών.

Ορισμός 3.2.1. *Έστω X ένας συνεκτικός χώρος Hausdorff. Έστω ότι υπάρχει μια κάλυψη (U_i, z_i) του X, δηλαδή $z_i : U_i \to A_i \subseteq \mathbb{C}, i \in I$, με*

$$X = \bigcup_{i \in I} U_i,$$

τα A_i ανοικτά, οι z_i ομοιομορφισμοί και οι απεικονίσεις μεταφοράς

$$z_i \circ z_j^{-1} : z_j(U_i \cap U_j) \to z_i(U_i \cap U_j)$$

ολόμορφες με πουθενά μηδενιζόμενες παραγώγους. Δύο καλύψεις του X είναι ισοδύναμες αν η ένωση του είναι κάλυψη με την παραπάνω έννοια. Μια κλάση ισοδυναμίας καλύψεων λέμε ότι ορίζει μια μιγαδική δομή στον X.

Ορισμός 3.2.2. *Μια επιφάνεια Riemann X είναι μια ένα συνεκτικός Hausdorff τοπολογικός χώρος X με μια μιγαδική δομή. Ισοδύναμα, μια επιφάνεια Riemann είναι μια μιγαδική πολλαπλότητα διάστασης 1.*

Ορισμός 3.2.3. *Έστω μια επιφάνεια Riemann X όπως παραπάνω, και U ένα ανοικτό σύνολο της X. Τότε, μια απεικόνιση $f : U \to \mathbb{C}$ λέγεται ολόμορφη (σε σχέση με την κάλυψη (U_i, z_i)) αν και μόνο αν η*

$$f \circ z_i^{-1} : z_i(U \cap U_i) \to \mathbb{C}$$

είναι ολόμορφη για κάθε $i \in I$.

Ολομορφία σε μία κάλυψη συνεπάγεται ολομορφία για κάθε ισοδύναμη της κάλυψη. Έτσι, ορίζεται μια ολόμορφη συνάρτηση σε μια επιφάνεια Riemann να είναι μια συνάρτηση ολόμορφη ως προς μία κάλυψη που να ορίζει την μιγαδική δομή της. Μια μερόμορφη συνάρτηση σε ένα ανοικτό U της X είναι μια συνάρτηση που είναι ολόμορφη στο συμπλήρωμα ενός διακριτού υποσυνόλου του U και έχει πόλο σε κάθε σημείο του διακριτού συνόλου.

Εν μέρει, η μεγάλη σημασία των επιφανειών Riemann έγκειται στο ότι μπορούμε να ορίσουμε ολόμορφες συναρτήσεις ανάμεσα τους.

Ορισμός 3.2.4. *Έστω X, Y δύο επιφάνειες Riemann. Μια $f : X \to Y$ λέγεται ολόμορφη αν για κάθε σημείο P στην X υπάρχουν καλύψεις (U_P, z_P) του P και $(U_{f(P)}, z_{f(P)})$ του $f(P)$ τέτοιες ώστε η*

$$z_{f(P)} \circ f \circ z_P^{-1} : z_P(U_P) \longrightarrow z_{f(P)}\left(U_{f(P)}\right)$$

να είναι ολόμορφη.

Παραδείγματα επιφανειών Riemann είναι η σφαίρα του Riemann $\bar{\mathbb{C}} = \mathbb{C} \cup \infty$, κάθε ανοιχτό υποσύνολο του $\mathbb{C}$ καθώς και ο τόρος $\mathbb{C}/\mathbb{Z}^2$.

Όπως και με τις αλγεβρικές καμπύλες, μας ενδιαφέρει να μελετήσουμε συναρτήσεις και διαφορικά πάνω σε επιφάνειες Riemann.

Ορισμός 3.2.5. *Το σύνολο των μερόμορφων συναρτήσεων που ορίζονται πάνω σε μια επιφάνεια Riemann X συμβολίζεται με $M(X)$. Προφανώς, το $M(X)$ είναι σώμα.*

Ορισμός 3.2.6. *Έστω U ένα ανοικτό υποσύνολο του $\mathbb{C}$. Μια διαφορική μορφή (ή διαφορικό) στο U είναι μια τυπική έκφραση της μορφής $f(z)dz$, όπου η f είναι μερόμορφη στο U και το σύμβολο dz είναι ένα τυπικό σύμβολο που υπακούει στους συνήθεις κανόνες που δώσαμε στον ορισμό 1.3.8. Για κάθε τέτοια f ορίζουμε μια διαφορική μορφή*

$$df \equiv \frac{df}{dz}dz.$$

Έστω τώρα μια απεικόνιση $g : U \to U'$, όπου το U' είναι ένα ανοικτό υποσύνολο του $\mathbb{C}$. Ορίζουμε $\omega = f(g(z))dg(z)$ μια διαφορική μορφή στο U'. Τότε, η

$$g^*(\omega) = f(g(z))\frac{dg(z)}{dz}dz$$

είναι μια διαφορική μορφή στο U. Αν τώρα η X είναι μια επιφάνεια Riemann και (U_i, z_i) μια κάλυψη της X, μια διαφορική μορφή στην X ως προς την κάλυψη (U_i, z_i) είναι μια οικογένεια διαφορικών μορφών $\omega_i = f(z_i)dz_i$ στα $z_i(U_i)$ για κάθε $i \in I$ ώστε να συμφωνούν στις αλληλοκαλύψεις: αν $g_{ij}(z_j) = z_i$ τότε $g_{ij}^*(\omega_i) = \omega_j$, δηλαδή

$$f_j(z_j)dz_j = f_i(g_{ij}(z_j))g_{ij}^{'}(z_j)dz_j.$$

Το σύνολο των διαφορικών μορφών πάνω στην επιφάνεια Riemann X το συμβολίζουμε με Ω_X.

Αξίζει να συγκριθεί αυτός ο ορισμός με τον ορισμό των μερόμορφων συναρτήσεων στην X, όπου μια μερόμορφη f δίνεται από μια οικογένεια μερόμορφων $f_i(z_i)$ στα $z_i(U_i)$ τέτοια ώστε για κάθε i και j να έχουμε την ακόλουθη συμφωνία στις αλληλοκαλύψεις:

$$f_j(z_j) = f_i(g_{ij}(z_j)).$$

Ορισμός 3.2.7. *Μια διαφορική μορφή στην X λέγεται ολόμορφη ή πρώτου είδους, αν δεν έχει πόλους στην X. Αν έχει residue 0 σε κάθε πόλο της, τότε λέγεται δευτέρου είδους, και λέγεται τρίτου είδους αλλιώς.*

Όμοια με τις αλγεβρικές καμπύλες, ξεχωριστό ενδιαφέρον για εμάς παρουσιάζουν τα ολόμορφα διαφορικά που ορίζονται πάνω σε μια επιφάνεια Riemann. Την επόμενη πρόταση την έχουμε ήδη δει για επιφάνειες Riemann γένους 1.

Πρόταση 3.2.8. (i) *Αν ω είναι ένα ολόμορφο διαφορικό στην συμπαγή επιφάνεια Riemann X, το άθροισμα των residues του ω στους πόλους του είναι* 0.

(ii) *Για μια μερόμορφη συνάρτηση f στην X το πλήθος των ριζών της ισούται με το πλήθος των πόλων της, λαμβάνοντας υπ' όψην τις πολλαπλότητες.*

Απόδειξη. (i) Θεωρούμε το ολόμορφο διαφορικό $\omega = f dz$ σε ένα ανοικτό υποσύνολο του $\mathbb{C}$ και ένα κλειστό μονοπάτι του γ που δεν περνά από τους πόλους της f. Έχουμε

$$\int_C \omega = 2\pi \mathrm{i} \left(\sum_{\mathrm{P}} \mathrm{res}_{\mathrm{P}}(\omega) \right)$$

όπου το άθροισμα είναι υπεράνω όλων των πόλων της f. Η X είναι συμπαγής, μπορούμε να θεωρήσουμε μία πεπερασμένη κάλυψη της (U_i, z_i) και διαλέγουμε έναν τριγωνισμό της τέτοιον ώστε κάθε τρίγωνο να είναι εξ' ολοκλήρου εντός κάποιου U_i. Τότε, το δεξιό μέλος ισούται με το άθροισμα των ολοκληρωμάτων κατά μήκος των τριγώνων, τα οποία αλληλοαναιρούνται.

(ii) Θεωρούμε το $\omega = df/f$ στο (i).

□

Πόρισμα 3.2.9. *Αν η f είναι μια μη σταθερή μερόμορφη συνάρτηση ορισμένη πάνω σε μια συμπαγή επιφάνεια Riemann X, τότε υπάρχει ένας ακέραιος $n > 0$ με την ιδιότητα η f να παίρνει κάθε τιμή της n ακριβώς φορές, μετρώντας πολλαπλότητες.*

Απόδειξη. Για κάθε τιμή $z_0 \in \bar{\mathbb{C}}$ εφαρμόζουμε το παραπάνω θεώρημα για την απεικόνιση $f(z) - z_0$. □ □

Ορισμός 3.2.10. *Ο ακέραιος αριθμός n που ορίζεται από το παραπάνω πόρισμα ονομάζεται βαθμός της συνάρτησης f.*

Ορισμός 3.2.11. *Μια απεικόνιση βαθμού n είναι μια απεικόνιση $f{:}X \to \bar{\mathbb{C}}$ που είναι n προς 1. Ένα σημείο z_0 ονομάζεται σημείο διακλάδωσης (ramification point) της συμπαγούς επιφάνειας Riemann X αν το σύνολο $f^{-1}(z_0)$ περιέχει λιγότερα από n διακριτά σημεία.*

Πρόταση 3.2.12. *Έστω $\bar{\mathbb{C}} = \mathbb{C} \cup \infty$ η σφαίρα του Riemann . Τότε $M(\bar{\mathbb{C}}) = \mathbb{C}(z)$ (οι μερόμορφες συναρτήσεις πάνω στην $\bar{\mathbb{C}}$ είναι ακριβώς οι ρητές).*

Δεν είναι προφανές ότι για κάθε συμπαγή επιφάνεια Riemann X υπάρχει τουλάχιστον μία μερόμορφη συνάρτηση για την X. Αυτό μας το εγγυάται το επόμενο θεώρημα:

Θεώρημα 3.2.13 (Ύπαρξης)**.** *Έστω X μια συμπαγή επιφάνεια Riemann X. Τότε το $M(X)$ είναι μη κενό σύνολο, και η επέκταση σωμάτων $M(X)/\mathbb{C}$ έχει βαθμό υπερβατικότητας* 1.

Ομοίως με τις καμπύλες, ορίζουμε την ομάδα των divisors της X να είναι η ελεύθερη αβελιανή ομάδα που γεννάται από τα σημεία της X, δηλαδή αποτελείται από τα τυπικά πεπερασμένα αθροίσματα της μορφής $\sum n_P(P)$, $P \in X$, όπου $n_P \in \mathbb{Z}$ και συμβολίζουμε την ομάδα αυτήν με $\mathrm{Div}(X)$. Ο βαθμός τους $D = \sum n_P(P)$ ορίζεται να είναι η ποσότητα

$$\deg D = \sum n_P$$

και αν $n_P \geq 0$ για κάθε n_P, τότε ο divisor λέγεται θετικός. Αν η f είναι μια μερόμορφη συνάρτηση στην συμπαγή επιφάνεια Riemann X, ορίζουμε

$$\mathrm{div}(f) = \sum_{P \in X} \mathrm{ord}_P(f) P$$

κι επειδή η X είναι συμπαγής, το άθροισμα αυτό είναι πεπερασμένο. Παρατηρούμε ότι ο $\mathrm{div}(f)$ έχει βαθμό 0. Οι έννοιες πρωταρχικός divisor και γραμμική ισοδυναμία ορίζονται ομοίως με το κεφάλαιο 1. Ορίζουμε ο βαθμός μιας κλάσης ισοδυναμίας να είναι ο βαθμός ενός αντιπροσώπου της.

Αν ω είναι ένα διαφορικό της X, τότε σε κάθε U_i της πεπερασμένης κάλυψης (U_i, z_i) της X το ω γράφεται ως $f_i dz_i$, και ορίζουμε την τάξη του ω στο $P \in U_i$ να είναι η τάξη της f_i στο P. Ο divisor του ω είναι ο

$$\mathrm{div}(\omega) = \sum_{P \in X} \mathrm{ord}_P(\omega) P.$$

Για κάθε μερόμορφη συνάρτηση έχουμε $\mathrm{div}(f\omega) = \mathrm{div}(f) + \mathrm{div}(\omega)$. Αν ω' είναι ένα άλλο διαφορικό της X, τότε $\omega' = f\omega$ για κάποια μερόμορφη f, άρα η κλάση των $\mathrm{div}(\omega)$ είναι καλά ορισμένη, και καλείται κανονικός divisor.

Αν για κάθε divisor ορίσουμε τον χώρο

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

τότε αυτός είναι ένας $\mathbb{C}$-διανυσματικός χώρος και η διάσταση του εξαρτάται μόνο από την κλάση ισοδυναμίας του D. Την διάσταση του $L(D)$ την συμβολίζουμε με $\ell(D)$.

Θεώρημα 3.2.14 (Riemann-Roch για επιφάνειες Riemann). *Έστω X μια συμπαγής επιφάνεια Riemann, και έστω K ένας κανονικός divisor της. Τότε, υπάρχει ένας ακέραιος $g \geq 0$, που εξαρτάται μόνο από την X, τέτοιος ώστε για κάθε divisor D της X να ισχύει:*

$$\ell(D) - \ell(K - D) = \deg D - g + 1$$

Τα πορίσματα του Riemann-Roch για καμπύλες ισχύουν φυσικά κι εδώ. Σε αυτό το πλαίσιο, το θεώρημα του Hurwitz είναι ως εξής:

Θεώρημα 3.2.15 (Hurwitz για επιφάνειες Riemann). *Έστω X και Y δύο συμπαγείς επιφάνειες Riemann με γένη $g(X)$ και $g(Y)$ αντίστοιχα, και $f : X \to Y$ μια ολόμορφη απεικόνιση βαθμού m, και $e(P)$ ο δείκτης διακλάδωσης στο P Τότε, ισχύει ο τύπος:*

$$2g(Y) - 2 = (2g(X) - 2) \deg f + \sum_{P \in X} (e(P) - 1)$$

Έχουμε διατυπώσει το Riemann-Roch στην γλώσσα των αλγεβρικών καμπυλών, που μας χρειάστηκε για την μελέτη των ελλειπτικών καμπυλών, και στην γλώσσα των επιφανειών Riemann, που θα μας χρειαστεί για την μελέτη των modular forms. Η μέχρις εδώ λοιπόν θεωρία υποδεικνύει πως πρέπει να υπάρχει κάποια συσχέτιση ανάμεσα στις συμπαγείς επιφάνειες Riemann και τις αλγεβρικές καμπύλες. Το επόμενο θεώρημα μας λέει πως αυτό είναι σωστό.

Θεώρημα 3.2.16. *Κάθε συμπαγής επιφάνεια Riemann έχει μοναδική δομή ως πλήρης nonsingular αλγεβρική καμπύλη.*

Δεν θα δώσουμε την απόδειξη του θεωρήματος αυτού. Για μια σκιαγράφηση της απόδειξης παραπέμπουμε στον [Milne, [22], κεφ.7]. Η παραπάνω συζήτηση δικαιολογεί το όνομα modular καμπύλες για τις επιφάνειες Riemann που θα ορίσουμε στις επόμενες παραγράφους. Τα παραπάνω θα γίνουν πιο σαφή στο 4ο κεφάλαιο, όταν θα επιστρέψουμε στην μελέτη των modular καμπυλών. Επίσης, παραπέμπουμε στον [Hartshorne, [10], appendix A] για την απόδειξη ενός γενικευμένου θεωρήματος Riemann-Roch που οφείλεται στον Grothendieck.

3.3 Το άνω μιγαδικό επίπεδο $\mathbb{H}$

Ορισμός 3.3.1. *Ορίζουμε το άνω μιγαδικό ημιεπίπεδο να είναι ο χώρος*

$$\mathbb{H} = \{z : \Im(z) > 0\}$$

Το Θεώρημα σύμμορφης απεικόνισης του Riemann (Riemann mapping theorem) μας λέει ότι οι απλά συνεκτικές επιφάνειες Riemann είναι πολύ συγκεκριμμένες:

Θεώρημα 3.3.2. *Κάθε απλά συνεκτική επιφάνεια Riemann είναι ισόμορφη με ακριβώς μία εκ των $\mathbb{H}$ (ισοδύναμα τον μοναδιαίο δίσκο $\mathbb{D}$), $\mathbb{C}$ και $\bar{\mathbb{C}} = P^1(\mathbb{C})$.*

Είναι γνωστό ότι οι αυτομορφισμοί της σφαίρας του Riemann $\bar{\mathbb{C}} = \mathbb{C} \cup \infty$ είναι η ομάδα των μετασχηματισμών Möbius:

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

όπου οι $a, b, c, d \in \mathbb{C}$. Επειδή κάθε πίνακας δρα όπως και κάθε πολλαπλάσιο του και αλλάζοντας το πρόσημο στον πίνακα δεν αλλάζει ο μετασχηματισμός, έχουμε ως επιπλέον συνθήκες την $ad - bc = 1$ και την άγνοια του προσήμου του πίνακα, δηλαδή η ομάδα αυτομορφισμών της $\bar{\mathbb{C}}$ είναι ισόμορφη με την ομάδα $\mathrm{PSL}_2(\mathbb{C})$. Η ομάδα αυτομορφισμών του $\mathbb{C}$ είναι τα πρωτοβάθμια πολυώνυμα με μιγαδικούς συντελεστές. Οι χώροι που κυρίως θα μελετήσουμε είναι, για λόγους που σχετίζονται με τις ελλειπτικές καμπύλες, πηλίκα του $\mathbb{H}$, άρα θα έχουν σαν καθολικό χώρο επικάλυψης το $\mathbb{H}$. Οπότε είναι λογικό να ρωτήσει κανείς ποιοί είναι οι αυτομορφισμοί του $\mathbb{H}$. Καταρχάς, ένα πρώτο βήμα προς τον καθορισμό των αυτομορφισμών του $\mathbb{H}$ είναι η εξής παρατήρηση: αν $\gamma \in \mathrm{SL}_2(\mathbb{R})$ και $z \in \mathbb{H}$ τότε έχουμε ότι $\gamma(z) \in \mathbb{H}$, δηλαδή η $\mathrm{SL}_2($ $mathbbR$) δρα στο $\mathbb{H}$. Πράγματι, αν:

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

τότε

$$\Im(\gamma(z)) = \frac{\Im(z)}{|cz+d|^2}.$$

Δίνοντας τώρα στην $\mathrm{SL}_2(\mathbb{R})$ και στο $\mathbb{H}$ τις συνήθεις τοπολογίες, η δράση αυτή είναι συνεχής. Ορίζουμε επίσης την ειδική ορθογώνια ομάδα:

$$\mathrm{SO}_2(\mathbb{R}) = \left\{ \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix}, \theta \in \mathbb{R} \right\}.$$

Παρατηρούμε ότι η $\mathrm{SO}_2(\mathbb{R})$ είναι κλειστή υποομάδα της $\mathrm{SL}_2(\mathbb{R})$, άρα από το λήμμα 3.1.4 έπεται ότι το πηλίκο $\mathrm{SL}_2(\mathbb{R})/\mathrm{SO}_2(\mathbb{R})$ είναι Hausdorff.

Θεώρημα 3.3.3. (i) *Η $\mathrm{SL}_2(\mathbb{R})$ δρα μεταβατικά στο $\mathbb{R}$: για κάθε $z_1, z_2 \in \mathbb{H}$ υπάρχει $\gamma \in \mathrm{SL}_2(\mathbb{R})$ τέτοιο ώστε $\gamma(z_1) = z_2$.*

(ii) *Η δράση της $\mathrm{SL}_2(\mathbb{R})$ στο $\mathbb{H}$ επάγει ισομορφισμό:*

$$\mathrm{SL}_2(\mathbb{R})/\pm I \longrightarrow \mathrm{Aut}(\mathbb{H})$$

(iii) *Η σταθεροποιούσα του* i *είναι η $\mathrm{SO}_2(\mathbb{R})$*

(iv) *Η απεικόνιση*

$$\phi : \mathrm{SL}_2(\mathbb{R})/\mathrm{SO}_2(\mathbb{R}) \to \mathbb{H}$$

με

$$\phi(\gamma \mathrm{SO}_2(\mathbb{R})) = \gamma(\mathrm{i})$$

είναι ομοιομορφισμός.

Απόδειξη. (i) Ο πίνακας

$$\begin{pmatrix} y & x \\ 0 & 1 \end{pmatrix}$$

απεικονίζει το i στο $z = x + y\mathrm{i}$. Αν γ_1, γ_2 είναι οι πίνακες που απεικονίζουν το i στα z_1 και z_2 αντίστοιχα, τότε ο $\gamma_2\gamma_1^{-1}$ απεικονίζει το z_1 στο z_2.

(ii) Αν ένας πίνακας της $\mathrm{SL}_2(\mathbb{R}$ δρα ταυτοτικά στο $\mathbb{H}$ τότε είναι άμεσο να ότι θα πρέπει να είναι διαγώνιος, και αφού θα έχει ορίζουσα έπεται ότι θα είναι ένας εκ των $\pm I$. Έστω τώρα ένας αυτοορφισμός γ του $\mathbb{H}$. Απ'ο το προηγούμενο ερώτημα, υπάρχει $\alpha \in \mathrm{SL}_2(\mathbb{R}$ τέτοιο ώστε $\alpha(\mathrm{i}) = \gamma(\mathrm{i})$, άρα μπορούμε να υποθέσουμε πως $\gamma(\mathrm{i}) = \mathrm{i}$. Η απεικόνιση

$$f : \mathbb{H} \longrightarrow \mathbb{D} : f(z) = \frac{z - \mathrm{i}}{z + \mathrm{i}}$$

είναι ισομορφισμός με $f(\mathrm{i}) = 0$. Άρα, η απεικόνιση $f \circ \gamma \circ f^{-1}$ είναι ισομορφισμός του $\mathbb{D}$ που σταθεροποιεί το 0. Οι αυτομορφισμοί του $\mathbb{D}$ που σταθεροποιούν το 0 είναι, ως γνωστόν, της μορφής $z \to \lambda z$ με $|\lambda| = 1$. Άρα, $f \circ \gamma \circ f^{-1}(z) = e^{2\theta\mathrm{i}}$, το οποίο σημαίνει ότι

$$\gamma(z) = \begin{pmatrix} \cos\theta & \sin\theta \\ -\sin\theta & \cos\theta \end{pmatrix} z,$$

δηλαδή $\gamma \in \mathrm{SO}_2(\mathbb{R})$.

(iii) Παρατηρούμε ότι

$$\gamma(\mathrm{i}) = \frac{\mathrm{ai}+\mathrm{b}}{\mathrm{ci}+\mathrm{d}} = \mathrm{i} \Longleftrightarrow \mathrm{a} = \mathrm{d}, \mathrm{b} = -\mathrm{c}$$

δηλαδή, επειδή η ορίζουσα είναι 1, αν και μόνο αν $\gamma \in \mathrm{SO}_2(\mathbb{R})$.

(iv) Έπεται από την πρόταση 3.1.5.

□

Αφού η σταθεροποιούσα του i στην $\mathrm{SL}_2(\mathbb{R})/\pm I$ δεν είναι η τετριμένη υποομάδα της, η δράση δεν είναι ελεύθερη. Πριν προχωρήσουμε στην μελέτη της δράσης συγκεκριμμένων υποομάδων της $\mathrm{SL}_2(\mathbb{R})/\pm I$ στο $\mathbb{H}$, θα δώσουμε ένα λήμμα το οποίο θα μας φανεί επίσης χρήσιμο για την μελέτη των χώρων πηλίκο των δράσεων αυτών.

Λήμμα 3.3.4. *Έστω Γ μια διακριτή υποομάδα της $\mathrm{SL}_2(\mathbb{R})$ τέτοια ώστε η Γ (όπου μπορούμε, αν $-I \in \Gamma$, να διαλέξουμε την Γ / $\pm I$) να δρα ελεύθερα στο $\mathbb{H}$. Τότε, μπορούμε να ορίσουμε μιγαδική δομή με μοναδικό τρόπο στο πηλίκο $\Gamma\backslash\mathbb{H}$ ώστε να ισχύει ότι μια f είναι ολόμορφη σε ένα ακοικτό υποσύνολο του πηλίκου αν και μόνο αν η $f \circ p$ είναι ολόμορφη (όπου $p : \mathbb{H} \longrightarrow \Gamma\backslash\mathbb{H}$ η φυσική προβολή).*

3.4 Ομάδες Fuchsian και η δράση τους στο $\mathbb{H}$

Ορισμός 3.4.1. *Μια διακριτή υποομάδα της $\mathrm{SL}_2(\mathbb{R})$ ονομάζεται ομάδα Fuchsian. Η (full) modular group είναι η ομάδα των 2×2 πινάκων με ακέραια στοιχεία και διακρίνουσα* 1*,*

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} , a, b, c, d \in \mathbb{Z}, ad - bc = 1 \right\}.$$

Συχνά, ορίζουμε τα παραπάνω με τον ίδιο τρόπο modulo $\pm I$ (γιατί είδαμε ότι αυτό απαιτείται για την δράση στο άνω μιγαδικό επίπεδο). Οι αντίστοιχες ομάδες συμβολίζονται με $\mathrm{PSL}_2(\mathbb{R})$ και $\mathrm{PSL}_2(\mathbb{Z})$.

Θεώρημα 3.4.2. *Η modular group παράγεται από τα στοιχεία $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ και $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.*

Απόδειξη. Έστω

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Μπορούμε, χωρίς βλάβη της γενικότητας, να υποθέσουμε ότι $c \geq 0$. Επίσης, μπορούμε να υποθέσουμε ότι $|c| \leq |d|$ (αν όχι, πολλαπλασιαστε με S για να το πετύχετε). Η απόδειξη θα γίνει με επαγωγή στο c:

Αν $c = 0$, τότε είτε $a = d = 1 \Longrightarrow \gamma = T^b$, είτε $a = d = -1 \Longrightarrow \gamma = T^{-b}$.

Αν $c = 1$, τότε $\gamma = T^a S T^d$.

Έστω τώρα ένας φυσικός $c \geq 2$ και έστω ότι ισχύει για κάθε ακέραιο $< c$. Αφού $ad - bc = 1$ έπεται ότι μκδ(c, d)=1. Διαιρώντας το d με c έχουμε $d = qc + r$, όπου $0 < r < c$ (μπορούμε να το πετύχουμε επειδή $c \geq 2$).

Τότε

$$AT^{-q}S = \begin{pmatrix} -aq+b & -a \\ r & -c \end{pmatrix},$$

ο οποίος παράγεται από τους πίνακες T, S από επαγωγική υπόθεση. □

Οι Fuchsian ομάδες είναι πολλών ειδών, αλλά για εμάς ξεχωριστή σημασία θα έχει η κατανόηση του τρόπου που δρούν στο $\mathbb{H}$ τόσο η modular group όσο και συγκεκριμένες υποομάδες της.

Ορισμός 3.4.3. *Για κάθε $N \in \mathbb{N}$ ορίζουμε την ομάδα*

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a \equiv d \equiv 1 \mathrm{mod} N, b \equiv c \equiv 0 \mathrm{mod} N \right\}.$$

Η $\Gamma(N)$ ονομάζεται πρωταρχική ομάδα ισοτιμίας ύψους N. Μια υποομάδα της modular group ονομάζεται υποομάδα ισοτιμάς ύψους N αν περιέχει την $\Gamma(N)$.

Για παράδειγμα, ορίζουμε τις:

$$\begin{aligned}
\Gamma_0(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : c \equiv 0 \mathrm{mod} N \right\} \\
\Gamma^0(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : b \equiv 0 \mathrm{mod} N \right\} \\
\Gamma_1(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a \equiv d \equiv 1 \mathrm{mod} N, c \equiv 0 \mathrm{mod} N \right\} \\
\Gamma^1(N) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a \equiv d \equiv 1 \mathrm{mod} N, b \equiv 0 \mathrm{mod} N \right\}
\end{aligned}$$

Υιοθετούμε τον συμβολισμό $H \leq_f G$ για να δηλώσουμε ότι μια υποομάδα H της G έχει πεπερασμένο δείκτη στην G.

Ορισμός 3.4.4. *Δύο υποομάδες H_1, H_2 της G λέγονται commensurable αν $H_1 \cap H_2 \leq_f H_1$ και $H_1 \cap H_2 \leq_f H_2$.*

Παρατηρήσεις:

(i) Η ιδιότητα να είναι δύο υποομάδες της G commensurable είναι σχέση ισοδυναμίας.

(ii) Αν H_1 και H_2 είναι δύο commensurable υποομάδες της τοπολογικής ομάδας G και η μία είναι διακριτή, τότε και η άλλη είναι διακριτή.

(iii) Αν οι Γ_1 και Γ_2 είναι commensurable υποομάδες της $\mathrm{SL}_2(\mathbb{R})$ και το πηλίκο $\Gamma_1\backslash\mathbb{H}$ είναι συμπαγές, τότε και το $\Gamma_2\backslash\mathbb{H}$ είναι συμπαγές.

Ορισμός 3.4.5. *Μια υποομάδα την $\mathrm{SL}_2(\mathbb{Q})$ που είναι commensurable με την $\mathrm{SL}_2(\mathbb{Z})$ καλείται αριθμητική Fuchsian ομάδα.*

Άρα μια υποομάδα της $\mathrm{SL}_2(\mathbb{Z})$ είναι αριθμητική αν είναι πεπερασμένου δείκτη στην $\mathrm{SL}_2(\mathbb{Z})$. Έχουμε ήδη ορίσει κάποιες αριθμητικές Fuchsian ομάδες:

Πρόταση 3.4.6. *Οι πρωταρχικές ομάδες ισοτιμίας είναι αριθμητικές Fuchsian ομάδες.*

Απόδειξη. Η φυσική απεικόνιση

$$\mathrm{SL}_2(\mathbb{Z}) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$$

επάγει έναν ισομορφισμό

$$\mathrm{SL}_2(\mathbb{Z})/\Gamma(N) \longrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Οπότε παίρνουμε

$$[\mathrm{SL}_2(\mathbb{Z}) : \Gamma(N)] = |\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})| = N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right)$$

και έχουμε το ζητούμενο. □

Από την παραπάνω πρόταση έπεται ότι όλες οι ομάδες ισοτιμίας είναι αριθμητικές. Το αντίστροφο δεν ισχύει. Μάλιστα, αν A_m και B_m είναι το πλήθος των υποομάδων ισοτιμίας της $\mathrm{SL}_2(\mathbb{Z})$ δείκτη $\leq m$ και το πλήθος των υποομάδων της $\mathrm{SL}_2(\mathbb{Z})$ δείκτη $\leq m$ αντίστοιχα, τότε

$$\lim_{m\to\infty} \frac{A_m}{B_m} = 0$$

Θέλουμε τώρα να εξετάσουμε πιο ενδελεχώς τους αυτομορφισμούς του $\mathbb{H}$. Η ομάδα $\mathrm{SL}_2(\mathbb{C})$ δρα στο $\mathbb{P}^1(\mathbb{C}) = \bar{\mathbb{C}}$. Οι βαθμωτοί πίνακες (δηλαδή τα πολλαπλάσια του ταυτοτικού) δρουν σαν το ταυτοτικό στοιχείο. Γνωρίζουμε ότι κάθε 2×2 πίνακας που δεν είναι βαθμωτός έχει κανονική μορφή Jordan μια εκ των εξής δύο:

$$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}, a \in \mathbb{C}, \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}, a \neq b, a, b \in \mathbb{C}$$

Στην πρώτη περίπτωση ο πίνακας είναι συζυγής με μια απεικόνιση μεταφοράς κατά a^{-1}, και ο πίνακας ονομάζεται παραβολικός. Στην δεύτερη περίπτωση, ο πίνακας αντιστοιχεί σε πολλαπλασιασμό με έναν έναν αριθμό $c \neq 1$. Αν έχουμε ότι $|c| = 1$, ο πίνακας ονομάζεται ελλειπτικός, αν είναι θετικός πραγματικός αριθμός ονομάζεται υπερβολικός, ενώ αλλιώς ονομάζεται λοξοδρομικός. Η επόμενη πρόταση κατατάσσει τους μετασχηματισμούς με βάση το ίχνος τους.

Πρόταση 3.4.7. *Έστω ένας πίνακας*

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{C}).$$

Τότε, ο γ είναι:

(i) *παραβολικός* $\iff Tr(\gamma) = \pm 2$

(ii) *ελλειπτικός* $\iff Tr(\gamma) \in \mathbb{R}$ *και* $|Tr(\gamma)| < 2$

(iii) *υπερβολικός* $\iff Tr(\gamma) \in \mathbb{R}$ *και* $|Tr(\gamma)| > 2$

(iv) *λοξοδρομικός* $\iff Tr(\gamma) \in \mathbb{C}$ - $\mathbb{R}$.

Αν ένας τέτοιος πίνακας ανήκει στην $\mathrm{SL}_2(\mathbb{R})$ και δεν είναι λοξοδρομικός, τότε μπορούμε να κάνουμε την εξής διάκριση για τα σταθερά του σημεία:

(i) *Αν ο γ είναι παραβολικός και δεν είναι ένας εκ των $\pm I$, τότε έχει ακριβώς ένα σταθερό σημείο, το οποίο ανήκει στο $\mathbb{R} \cup \{\infty\}$.*

(ii) *Αν ο γ είναι ελλειπτικός, τότε έχει ένα σταθερό σημείο στο $\mathbb{H}$ και ένα συμμετρικό του στο κάτω μιγαδικό ημιεπίπεδο.*

(iii) *Αν ο γ είναι υπερβολικός, τότε έχει ακριβώς δύο σταθερά σημεία στο $\mathbb{R} \cup \{\infty\}$.*

Ορισμός 3.4.8. *Έστω Γ μια ομάδα Fuchsian. Τότε, ένα $z \in \mathbb{H}$ λέγεται ελλειπτικό αν μένει σταθερό από κάποιο ελλειπτικό σημείο της Γ, και ένα σημείο $z \in \mathbb{R} \cup \{\infty\}$ λέγεται cusp αν μένει σταθερό από κάποιο παραβολικό στοιχείο της Γ.*

Πρόταση 3.4.9. *Αν το z είναι ελλειπτικό σημείο μιας Γ τότε η υποομάδα της $\Gamma_z = \{\gamma \in \Gamma : \gamma(z) = z\}$ είναι πεπερασμένη κυκλική.*

Απόδειξη. Έστω ένα $\alpha \in \mathrm{SL}_2(\mathbb{R})$ τέτοιο ώστε $\alpha(\mathrm{i}) = \mathrm{z}$. Τότε η συζυγία

$$\gamma \longrightarrow \alpha^{-1}\gamma\alpha$$

επάγει ισομορφισμό

$$\Gamma_z = (\gamma \in \Gamma : \gamma(z) = z) \longrightarrow \mathrm{SO}_2(\mathbb{R}) \cup (\alpha^{-1}\Gamma\alpha).$$

Η ομάδα $\mathrm{SO}_2(\mathbb{R}) \cup (\alpha^{-1}\Gamma\alpha)$ είναι διακριτή και συμπαγής, άρα πεπερασμένη. Έχουμε τους ισομορφισμούς

$$\mathbb{R}/\mathbb{Z} \cong S^1 \cong \mathrm{SO}_2(\mathbb{R})$$

άρα

$$\mathbb{Q}/\mathbb{Z} \cong \mathrm{SO}_2(\mathbb{R})_{tors}$$

Άρα η Γ_z είναι ισόμορφη με κάποια πεπερασμένη υποομάδα της $\mathbb{Q}/\mathbb{Z}$ και άρα κυκλική. □

Παράδειγμα: Μας ενδιαφέρει να κατατάσσουμε τα cusps και τα ελλειπτικά σημεία της Γ μέχρις Γ-ισοδυναμίας. Τα cusps της modular ομάδας είναι το $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{\infty\}$, και όλα αυτά τα σημεία είναι $\mathrm{SL}_2(\mathbb{Z})$-ισοδύναμα, άρα η $\mathrm{SL}_2(\mathbb{Z})$ έχει ένα cusp. Τα ελλειπτικά σημεία της $\mathrm{SL}_2(\mathbb{Z})$ είναι (μέχρις $\mathrm{SL}_2(\mathbb{Z})$- ισοδυναμίας) τα i και $\rho = (1+\sqrt{3}\mathrm{i})/2$. Τα cusps της τυχαίας Γ υποομάδας της πεπερασμένου δείκτη είναι τα ίδια, όπου τώρα οι κλάσεις της Γ-ισοδυναμίας είναι περισσότερες.

Η μελέτη τη δράσης $\mathrm{SL}_2(\mathbb{Z})$ μελετάται εν γένει μέσω της δράσης των Fuchsian ομάδων. Για παραδειγμα, ϑέλουμε να δούμε με τι μοιάζει ο χώρος των τροχιών της δράσης μιας Fuchsian ομάδας στο $\mathbb{H}$. Μας ενδιαφέρει δηλαδή να βρούμε ένα υποσύνολο του άνω μιγαδικού επιπέδου που να περιέχει έναν ακριβώς αντιπρόσωπο από κάθε τροχιά.

Ορισμός 3.4.10. *Μια ϑεμελιώδης περιοχή για την Γ είναι ένα ανοικτό συνεκτικό χωρίο D του $\mathbb{H}$ τέτοιο ώστε να μην υπάρχουν Γ-ισοδύναμα στοιχεία του (δηλαδή στην ίδια τροχιά), και να ισχύει*

$$\mathbb{H} = \bigcup \gamma \bar{D}$$

όπου η ένωση διατρέχει τα στοιχεία της Γ.

Δεν είναι προφανές πως κάθε Fuchsian ομάδα έχει μια θεμελιώδη περιοχή. Για την modular ομάδα όμως μπορούμε να γράψουμε μία:

Πρόταση 3.4.11. *Έστω η modular ομάδα* $\mathrm{SL}_2(\mathbb{Z})$. *Μια θεμελιώδης περιοχή της είναι το χωρίο*

$$D = \{z \in \mathbb{H} : |z| > 1, |\Re(z)| < \frac{1}{2}\}$$

Η γνώση μιας θεμελιώδης περιοχής για μια διακριτή υποομάδα της $\mathrm{SL}_2(\mathbb{R})$ μας επιτρέπει να κατασκευάσουμε, σύμφωνα με την επόμενη πρόταση, μια θεμελιώδη περιοχή για μια πεπερασμένου δείκτη υποομάδα της.

Πρόταση 3.4.12. *Έστω* Γ *μια διακριτή υποομάδα της* $\mathrm{SL}_2(\mathbb{R})$ *με θεμελιώδη περιοχή* D, *και* Γ_1 *μια υποομάδα της πεπερασμένου δείκτη. Συμβολίζουμε με* $\bar{\Gamma}$ *και* $\bar{\Gamma}_1$ *τις εικόνες τους στην* $\mathrm{Aut}(D)$. *Τότε, αν διαλέξουμε* $\gamma_i \in \Gamma$, $i = 1, 2, 3, ...m$, *τέτοια ώστε*

$$\bar{\Gamma} = \bigcup_{i=1}^{m} \bar{\Gamma}_1 \bar{\gamma}_i$$

φτιάχνουμε μια θεμελιώδη περιοχή D_1 *της* $\bar{\Gamma}_1$ *ως εξής:*

$$D_1 = \bigcup_{i=1}^{m} \gamma_i D$$

Απόδειξη. Έστω ένα $z \in \mathbb{H}$. Τότε, υπάρχουν $\gamma \in \Gamma$ και $z' \in \bar{D}$ τέτοια ώστε $z = \gamma z'$ και $\gamma = \pm\gamma'\gamma_i$ για κάποιο $\gamma' \in \Gamma_1$ και για κάποιο i. Άρα $z = \gamma'\gamma_i z' \in \Gamma_1\gamma_i\bar{D}$. Αν ίσχυε $\gamma D_1 = D_1 \neq \emptyset$, τότε θα περιείχε μια μεταφορά του D. Αλλά τότε θα παίρναμε $\gamma\gamma_i D = \gamma_j D$ για κάποια i, j διαφορετικά, και άρα $\gamma\gamma_i = \pm\gamma_j$, το οποίο είναι άτοπο. □

Διαισθητικά μιλώντας, τα cusps είναι τα σημεία που οι θεμελιώδεις περιοχές ακουμπάνε στο τοπολογικό σύνορο του $\mathbb{H}$. Άρα, το $\mathbb{P}^1(\mathbb{Q})$ αποτελεί το σύνολο που οι θεμελι΄χδεις περιοχές της ακουμπούν στο $\mathbb{R}$. Ένα cusp τώρα για την Γ είναι μια τροχιά της στο $\mathbb{P}^1(\mathbb{Q})$.

Οι θεμελιώδεις περιοχές λοιπόν είναι μοντέλα για τους χώρους πηλίκα που προκύπτουν από τις δράσεις των Fuchsian ομάδων στο $\mathbb{H}$, και με βάση τις δύο παραπάνω προτάσεις μπορεί κανείς να έχει μια εικόνα για τις θεμελιώδεις περιοχές των πεπερασμένου δείκτη υποομάδων της $\mathrm{SL}_2(\mathbb{Z})$. Οι χώροι αυτοί είναι πηλίκα του άνω μιγαδικού επιπέδου, άρα αναμένει κανείς να μελετήσει την μιγαδική δομή τους. Αυτό θα κάνουμε συνοπτικά στην επόμενη παράγραφο.

3.5 Modular Καμπύλες

Ας συνοψίσουμε λίγο τι έχουμε την κατασκευή που έχουμε κάνει μέχρις εδώ. Στον τοπολογικό χώρο $\mathbb{H}$ δρα η τοπικά συμπαγής ομάδα $\mathrm{SL}_2(\mathbb{R})$. Αν λοιπόν η Γ είναι μια Fuchsian ομάδα, ο χώρος $\Gamma\backslash\mathbb{H}$ είναι Hausdorff. Αφού κάθε Fuchsian ομάδα έχει θεμελιώδη περιοχή, μπορούμε να υποθέτουμε πάντα πως ο χώρος $\Gamma\backslash\mathbb{H}$ είναι πάντα συνεκτικός και Hausdorff. Αφού αυτός ο χώρος πηλίκο είναι πηλίκο του άνω μιγαδικού επιπέδου, είναι λογικό να περιμένουμε πως θα έχει και μιγαδική δομή, άρα οι $\Gamma\backslash\mathbb{H}$ να είναι επιφάνειες Riemann.

Συμβολίζουμε με $\mathbb{H}^*$ το επεκτεταμένο μιγαδικό επίπεδο $\mathbb{H}\cup\mathbb{P}^1(\mathbb{Q})$ ή το $\mathbb{H}\cup\{\mathrm{i}\infty\}$ (δηλαδή το επ΄ άπειρον σημείο στην κατεύθυνση του κάθετου άξονα). Για την modular group οι δύο συμβολισμοί αυτοί δεν έχουν ουσιαστικά διαφορά. Παρατηρείστε επίσης ότι $\mathrm{SL}_2(\mathbb{Z}) = \Gamma(1)$.

3.5α΄ Η μιγαδική δομή στον $\Gamma(1)\backslash\mathbb{H}$

Θεωρούμε την προβολή $P : \mathbb{H} \longrightarrow \Gamma(1)\backslash\mathbb{H}$, P ένα σημείο του $\Gamma(1)\backslash\mathbb{H}$ και Q ένα σημείο στην $\mathbb{H}$ με $p(Q) = P$.

Αν το Q δεν είναι ελλειπτικό σημείο, διαλέχουμε περιοχή U του Q τέτοια ώστε ο p να είναι ομοιομορφισμός $U \to p(U)$. Τότε το $(p(U), p^{-1})$ είναι τοπικός χάρτης για το P.

Αν βρούμε έναν χάρτη για το ελλειπτικό i, τότε με $\Gamma(1)$-μεταφορές βρίσκουμε χάρτες και για κάθε άλλο εελειπτικό σημείο. Η απεικόνιση

$$z \longrightarrow \frac{z-\mathrm{i}}{z+\mathrm{i}}$$

ορίζει ισομορφισμό ανάμεσα σε κάποια S-σταθερή ανοιχτή περιοχή U του i και έναν ανοικτό δίσκο D του 0, και η δράση του S στην U μεταφέρεται στον D-αυτομορφισμό $\sigma : z \to -z$. Οι $\langle S\rangle\backslash U$ και $\langle\sigma\rangle\backslash D$ είναι ομοιομορφικοί και τροφοδοτούμε τον $\langle S\rangle\backslash U$ με την μιγαδική δομή ώστε η παραπάνω απεικόνιση να είναι αμφιολόμορφος ισομορφισμός. Άρα η απεικόνιση

$$z \longrightarrow \left(\frac{z-\mathrm{i}}{z+\mathrm{i}}\right)^2$$

είναι ολόμορφη ορισμένη σε μια περιοχή του i που είναι S-αναλλοίωτη, κι άρα ορίζει ολόμορφη συνάρτηση σε μια περιοχή του $p(\mathrm{i})$. Μπορούμε να πάρουμε αυτήν σαν τοπικό χάρτη στο $p(\mathrm{i})$. Τα άλλα ελλειπτικά σημεία αντιμετωπίζονται ομοίως.

3.5β΄ Η μιγαδική δομή στον $\Gamma(1)\backslash\mathbb{H}^*$

Η επιφάνεια Riemann $\Gamma(1)\backslash\mathbb{H}$ που ορίσαμε δεν είναι συμπαγής. Για να την συμπαγοποιήσουμε υπάρχου δύο τρόποι

1ος τρόπος: Προσθέτουμε το επ΄ άπειρον σημείο στο $\mathbb{H}$ παίρνοντας έτσι το επεκτεταμένο άνω μιγαδικό ημιεπίπεδο $\mathbb{H}^*$ και θεωρούμε τον χώρο των τροχιών $\Gamma(1)\backslash\mathbb{H}^*$.

2ος τρόπος: Για τον χώρο πηλίκο $\Gamma(1)\backslash\mathbb{H}$ θεωρούμε το θεμελιώδες χωρίο του D και του επισυνάπτουμε το επ΄ άπειρον σημείο που αντιστοιχεί στον κάθετο άξονα.

Σε κάθε μία από τις παραπάνω περιπτώσεις λαμβάνουμε την ίδια συμπαγή επιφάνεια Riemann , με περιοχές του επ΄ άπειρον σημείου να είναι οι

$$U_{\alpha,\infty} = \{z \in \mathbb{H} : \Re(z) > \alpha\}$$

Την μη συμπαγή επιφάνεια Riemann $\Gamma(1)\backslash\mathbb{H}$ που ορίσαμε την συμβολίζουμε με $Y(1) \equiv Y(\Gamma(1))$. Την συμπαγοποίηση $\Gamma(1)\backslash\mathbb{H}^*$ της $Y(1)$ που ορίσαμε την συμβολίζουμε με $X(1) \equiv X(\Gamma(1))$.

Πρόταση 3.5.1. *Η συμπαγής επιφάνεια Riemann $X(1)$ έχει γένος 0, άρα είναι ισόμορφη με την σφαίρα του Riemann.*

Απόδειξη. Από τον τρόπο που κατασκευάστηκε είναι προφανές ότι η $X(1)$ είναι απλά συνεκτική, άρα από το θεώρημα σύμμορφης απεικόνισης του Riemann έχουμε ότι η $X(1)$ είναι σύμμορφα ισοδύναμη με κάποια εκ των $\mathbb{H}$, $\mathbb{C}$ και $\bar{\mathbb{C}} = P^1(\mathbb{C})$. Όμως, η μόνη συμπαγής εξ' αυτών είναι η $\bar{\mathbb{C}}$. □

3.5γ' Η μιγαδική δομή στον $\Gamma\backslash\mathbb{H}^*$

Θεωρούμε τώρα μια οποιαδήποτε υποομάδα Γ της $\Gamma(1)$ πεπερασμένου δείκτη σε αυτήν. Με παρόμοιο τρόπο ορίζεται μιγαδική δομή και στις επιφάνειες $\Gamma\backslash\mathbb{H}$ και $\Gamma\backslash\mathbb{H}^*$. Το συμπλήρωμα της $\Gamma\backslash\mathbb{H}$ στην $\Gamma\backslash\mathbb{H}^*$ είναι το σύνολο των ξένων κλάσεων ισοδυναμίας των cusps της Γ, και συμβολίζονται με $Y(\Gamma)$ και $X(\Gamma)$ αντίστοιχα. Υιοθετούμε τον συμβολισμό $X(N)$ για την $X(\Gamma(N))$, $X_0(N)$ για την $X(\Gamma_0(N))$ κ.ο.κ. Το θεώρημα 3.2.16 μας λέει ότι ο επόμενος ορισμός έχει νόημα.

Ορισμός 3.5.2. *Κάθε συμπαγής επιφάνεια Riemann της μορφής $X(\Gamma)$ ονομάζεται Modular Καμπύλη.*

Ονομάζουμε επίσης modular καμπύλη και κάθε χώρο $Y(\Gamma)$.

Έχουμε με αυτόν τον τρόπο κατασκευάσει μια άπειρη οικογένεια από συμπαγείς (και μη) επιφάνειες Riemann. Το παρακάτω θεώρημα μας δίνει έναν τρόπο να μετράμε το γένος τους.

Θεώρημα 3.5.3. *Έστω Γ μια υποομάδα της modular ομάδας $\Gamma(1)$ δείκτη μ, ν_2 το πλήθος των μη Γ-ισοδύναμων ελλειπτικών σημείων της τάξης 2, ν_3 το πλήθος των μη Γ-ισοδύναμων ελλειπτικών σημείων της τάξης 3 και ν_∞ το πλήθος των μη Γ-ισοδύναμων cusps της Γ. Τότε το γένος της $X(\Gamma)$ είναι ίσο με*

$$g(X(\Gamma)) = g = 1 + \frac{\mu}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2}$$

Απόδειξη. Αν $p : \mathbb{H}^* \to \Gamma(1)\backslash\mathbb{H}^*$ η φυσική προβολή και $\phi : \Gamma\backslash\mathbb{H}^* \to \Gamma(1)\backslash\mathbb{H}^*$ η προβολή επικάλυψης. Η ιδέα της απόδειξης έγκειται στο να δούμε την $X(\Gamma)$ σαν κάλυμμα της $X(\Gamma(1))$. Έστω λοιπόν ένα Q στο $\mathbb{H}^*$ και P', P οι εικόνες του στις $\Gamma\backslash\mathbb{H}^*$ και $\Gamma(1)\backslash\mathbb{H}^*$. Από τις ιδιότητες του δείκτη διακλάδωσης παίρνουμε

$$e(Q/P) = e(Q/P')e(P'/P)$$

Αν το Q είναι cusp τότε η p είναι τοπικά ∞ προς 1 και ο τύπος αυτός είναι άχρηστος. Αν το Q δεν είναι ελλειπτικό, τότε το P' δεν διακλαδίζεται.

Αν $P = p(\mathrm{i})$ τότε το Q είναι $\Gamma(1)$-ισοδύναμο με το i. Τότε είτε $e(Q/P') = 2$ είτε $e(P'/P) = 2$. Στην πρώτη περίπτωση το Q είναι ελλειπτικό για την Γ και το P' είναι αδιακλάδιστο πάνω από το P. Στην δεύτερη περίπτωση το Q δεν είναι ελλειτπικό για την Γ. Υπάρχουν ν_2 P' του πρώτου τύπου και $(\mu - \nu_3)/2$ σημεία του δεύτερου τύπου. Άρα

$$\sum(e(P') - 1) = \frac{\mu - \nu_2}{2}$$

Αν $P = p(\rho)$, τότε το Q είναι $\Gamma(1)$-ισοδύναμο με το ρ. Τότε είτε $e(Q/P') = 3$ είτε $e(P'/P) = 3$. Ομοίως με πριν βλέπουμε ότι

$$\sum(e(P') - 1) = \frac{2(\mu - \nu_3)}{3}$$

Αν $P = p(\infty)$, τότε το Q είναι cusp της Γ. Υπάρχουν ν_∞ P' και $\sum e_i = \mu$, άρα

$$\sum(e_i - 1) = \mu - \nu_\infty$$

Συνοψίζοντας, και εφαρμόζωντας τον τύπο του Hurwitz παίρνουμε

$$g(X(\Gamma)) = 1 - \mu + \sum \frac{e(P) - 1}{2}$$

$$= 1 - \mu + \sum_{P' over \phi(\mathrm{i})} \frac{e(P') - 1}{2} + \sum_{P' over \phi(\rho)} \frac{e(P') - 1}{2} + \sum_{P' over \phi(\infty)} \frac{e(P') - 1}{2}$$

$$= 1 + \frac{\mu}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2}$$

□

Τώρα, η πρόταση 3.4.6 μας δίνει ότι

$$[\Gamma(1) : \Gamma(N)] = N^3 \prod_{p|N} \left(1 - \frac{1}{p^2}\right)$$

και αν συμβολίσουμε με $\bar{\Gamma}$ την εικόνα της Γ μέσα στην $P\mathrm{SL}_2(\mathbb{Z})$, βλέπουμε ότι για κάθε $N \geq 3$ ισχύει

$$[\bar{\Gamma}(1) : \bar{\Gamma}(N)] = \frac{[\Gamma(1) : \Gamma(N)]}{2}$$

Εφαρμόζωντας αυτές τις παρατηρήσεις και το θεώρημα 3.5.3, παίρνουμε το παρακάτω

Πόρισμα 3.5.4. *Για $N \geq 3$ το γένος της $X(N)$ δίνεται από τον τύπο*

$$g(X(N)) = g(N) = 1 + \left(\frac{N - 6}{24}\right) N^2 \prod_{p|N} \left(1 - \frac{1}{p^2}\right)$$

Απόδειξη. Για $N \geq 3$ η $\Gamma(N)$ δεν έχει ελλειπτικά σημεία, και ο αριθμός των μη ισοδύναμων cusps της είναι ίσος με

$$\frac{[\bar{\Gamma}(1) : \bar{\Gamma}(N)]}{N} = \frac{[\Gamma(1) : \Gamma(N)]}{2N}$$

το οποίο, απ΄ το θεώρημα 3.5.3 μας δίνει

$$g(N) = 1 + \frac{[\bar{\Gamma}(1) : \bar{\Gamma}(N)]}{12} - \frac{[\bar{\Gamma}(1) : \bar{\Gamma}(N)]}{2N}$$

$$= 1 + \frac{[\Gamma(1) : \Gamma(N)]}{24} - \frac{[\Gamma(1) : \Gamma(N)]}{4N}$$

το οποίο δίνει το ζητούμενο. □

Για $N = 2$ εύκολα βλέπει κανείς ότι $g = 0$.

Οι modular καμπύλες αποδεικνύονται πολύ σημαντικές για την μελέτη των ελλειπτικών καμπυλών. Θα επανέλθουμε στην μελέτη των modular καμπυλών στο 4ο κεφάλαιο, όταν θα έχουμε εξετάσει τις συναρτήσεις και τα διαφορικά που ορίζονται πάνω σε αυτές.

Κεφάλαιο 4

Modular Forms

Μελετώντας τις modular καμπύλες, δείξαμε ότι αυτές είναι επιφάνειες Riemann. Μάλιστα, το uniformization θεώρημα για συμπαγείς επιφάνειες Riemann μας λέει ότι μπορούμε να δούμε κάθε συμπαγή επιφάνεια Riemann σαν modular καμπύλη (μέχρις conformal αμφιδιαφόρισης). Όμως, δοθείσης μιας συμπαγούς επιφάνειας Riemann, είναι φυσιολογικό να μελετήσει κανείς τις μερόμορφες συναρτήσεις καθώς και τα διαφορικά που ορίζονται πάνω σε αυτήν. Οδηγείται λοιπόν κανείς να μελετήσει τις μερόμορφες συναρτήσεις και τα διαφορικά που ορίζονται πάνω στις modular καμπύλες. Το κεντρικό αντικείμενο μελέτης αυτής της παραγράφου είναι αυτά ακριβώς τα αντικείμενα.

4.1 Βασικές έννοιες

Ορισμός 4.1.1. *Έστω Γ μια υποομάδα της $\mathrm{SL}_2(\mathbb{Z})$, η οποία είναι πεπερασμένου δείκτη στην $\mathrm{SL}_2(\mathbb{Z})$. Μια συνάρτηση $f : \mathbb{H} \to \mathbb{C}$ που ικανοποιεί τις ιδιότητες:*

(i) $f(\gamma(z)) = f(z)$ *για κάθε* $\gamma \in \Gamma$

(ii) *η f είναι μερόμορφη στο $\mathbb{H}$*

(iii) *η f είναι μερόμορφη στα cusps της Γ*

λέγεται modular function (modular συνάρτηση) για την ομάδα Γ. Δηλαδή, μια modular συνάρτηση για την Γ είναι μια μερόμορφη συνάρτηση στην modular καμπύλη $\Gamma\backslash\mathbb{H}^* \equiv X(\Gamma)$.

Όπως δείξαμε στο θεώρημα 3.4.2, η modular ομάδα παράγεται από τα στοιχεία

$$T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}.$$

Άρα, για την συνθήκη (i) αρκεί, για να ελέγξουμε αν η f είναι modular συνάρτηση για την $\mathrm{SL}_2(\mathbb{Z})$, να ελέγξουμε ότι η f ικανοποιεί τις σχέσεις:

$$f(z+1) = f(z)$$

$$f(-1/z) = f(z)$$

Όσον αφορά το cusp στο ∞ η τελευταία συνθήκη μπορεί να ερμηνευθεί ως εξής: μέσα στην $\mathrm{SL}_2(\mathbb{Z})$, το ∞ σταθεροποιείται από την ομάδα $\langle T \rangle$. Έστω

$$\gamma = \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \in \Gamma$$

με $h > 0$ το ελάχιστο δυνατό. Το h λέγεται πλάτος του cusp. Αφού $\gamma \in \Gamma$ έπεται ότι $f(z+h) = f(\gamma(z)) = f(z)$, δηλαδή η f είναι h-περιοδική. Έπεται ότι η f μπορεί να εκφραστεί συναρτήσει της $f^*(q)$, όπου $q = e^{2\pi i z/h}$ σε κάποιον ανοιχτό δίσκο $D(0,\varepsilon)$ με την f^* μερόμορφη στο 0. Άρα, η f^* έχει στον $D(0,\varepsilon)$ ανάπτυγμα

$$f^*(q) = \sum_{n=n_0}^{\infty} a_n q^n$$

με $n_0 \in \mathbb{Z}$. Αν τώρα z_0 είναι ένα άλλο cusp της Γ, η μεριμορφία στο z_0 σημαίνει το εξής: έστω $\sigma \in \Gamma$ με $\sigma(\infty) = z_0$, τότε η $f \circ \sigma$ είναι $\sigma\Gamma\sigma^{-1}$-αναλλοίωτη και η $f \circ \sigma$ είναι μερόμορφη στο ∞.

Επίσης, μια γενική παρατήρηση είναι πως, όπως η συναρτησιακή σχέση αρκεί να επαληθευτεί για τους πεπερασμένους γεννήτορες της Γ, έτσι και η μεριμορφία αρκεί να επαληθευτεί για τους πεπερασμένους αντιπρόσωπους των cusps.

Τονίσαμε το γεγονός πως οι modular functions είναι οι φυσιολογικές μερόμορφες συναρτήσεις που ορίζονται πάνω στις modular καμπύλες $X(\Gamma)$, καθώς και το γεγονός ότι είναι εξίσου φυσιολογικό βήμα να μελετήσει κανείς και τα διαφορικά που ορίζονται πάνω σε αυτές. Για να το πετύχουμε αυτό, θα πρέπει πρώτα να δώσουμε κάποιους ορισμούς:

Ορισμός 4.1.2. *Έστω Γ μια υποομάδα της $\mathrm{SL}_2(\mathbb{Z})$, πεπερασμένου δείκτη στην $\mathrm{SL}_2(\mathbb{Z})$, και ένας $k \in \mathbb{Z}$. Μια συνάρτηση $f : \mathbb{H} \to \mathbb{C}$ που ικανοποιεί τις ιδιότητες:*

(i) $f(\gamma(z)) = (cz+d)^k f(z)$ *για κάθε* $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$

(ii) *η f είναι ολόμορφη στο $\mathbb{H}$*

(iii) *η f είναι ολόμορφη στα cusps της Γ*

λέγεται modular form (modular μορφή) βάρους k για την ομάδα Γ.

Σχόλια 4.1.3. (i) Αν η f ικανοποιεί μόνο την πρώτη συνθήκη, τότε λέγεται weakly modular form. Αν αντί για ολόμορφη η f είναι μερόμορφη, τότε λέγεται μερόμορφη ή αυτόμορφη (automorphic) μορφή.

(ii) Μια modular form βάρους 0 είναι σταθερή.

(iii) Αν η f είναι modular μορφή περιττού βάρους για την Γ και $-I \in \Gamma$, τότε είναι αναγκαστικά η μηδενική. Πράγματι, για $\gamma = -I$, παρατηρούμε ότι

$$f = (-1)^k f \Rightarrow f \equiv 0$$

(iv) Σε αντιστοιχία με τις modular functions, η συναρτησιακή σχέση αρκεί πάντα να επαληθεύται για τους πεπερασμένους γεννήτορες της Γ και η ολομορφία για τους πεπερασμένους αντιπρόσωπους των cusps.

(v) Αν η f είναι modular form για την $\Gamma(N)$, τότε λέμε ότι είναι form ύψους N.

Συμβολισμός 4.1.4. Ο χώρος των modular forms βάρους k της Γ είναι $\mathbb{C}$-διανυσματικός χώρος και συμβολίζεται με $M_k(\Gamma)$.

Το σχόλιο (iii) μας λέει πως αν $-I \in \Gamma$, τότε:

$$\dim M_{2k-1}(\Gamma) = 0$$

για κάθε k. Επίσης, αν $k \leq -1$ τότε

$$\dim M_k(\Gamma) = 0.$$

Αν $-I \notin \Gamma$, τότε ο M_{2k-1} δεν έχει πάντα διάσταση 0. Από εδώ και πέρα όμως, εμείς θα ασχοληθούμε κυρίως με τα άρτια βάρη. Ένας λόγος για αυτό είναι ότι συχνά οι ομάδες Γ που θα μας ενδιαφέρουν θα περιέχουν το $-I$. Ένας άλλος λόγος δίνεται παρακάτω, και αφορά την ταύτιση των modular μορφών με τα διαφορικά της $X(\Gamma)$.

Μια ακόμα βασική παρατήρηση είναι πως το γινόμενο μιας modular form βάρους n και μιας modular form βάρους m δίνει μια modular form βάρους $n+m$. Έπεται ότι ο χώρος

$$M(\Gamma) = \bigoplus_{k=0}^{\infty} M_k(\Gamma),$$

είναι ένας *graded ring* (βαθμωτός δακτύλιος). Συχνά, θα χρειαστεί να θεωρούμε το παραπάνω άθροισμα πάνω από τους άρτιους k.

Όπως θα δούμε αργότερα, το βάρος 2 έχει μεγάλη σημασία, καθώς αυτό είναι το βάρος των modular μορφών στις οποίες αναφέρεται το Modularity Θεώρημα.

Μεγάλο αριθμοθεωρητικό ενδιαφέρον παρουσιάζουν οι συναρτήσεις που μηδενίζονται στα cusps.

Ορισμός 4.1.5. *Μια modular form που έχει ρίζα σε κάθε cusp της* Γ *ονομάζεται cusp form.*

Ο χώρος των cusp forms της Γ βάρους k συμβολίζεται με $S_k(\Gamma)$. Προφανώς, ο $S_k(\Gamma)$ είναι υπόχωρος του $M_k(\Gamma)$. Όμοίως με πριν ορίζεται ο

$$S(\Gamma) = \bigoplus_{k=0}^{\infty} S_k(\Gamma),$$

ο οποίος είναι ιδεώδες του $M(\Gamma)$.

Παρατήρηση 4.1.6. Έστω f μια modular μορφή για την Γ. Με την αλλαγή μεταβλητής $q{=}e^{2\pi iz}$, η f παίρνει την μορφή

$$f^*(q) = \sum_{n=0}^{\infty} a_n q^n,$$

όπου τώρα η f^* είναι ορισμένη: $\mathbb{D} \to \mathbb{C}$. Για μια cusp form, η ιδιότητα του μηδενισμού στα cusps επιβάλλει επιπλέον συνθήκες για τους συντελεστές της a_n. Για την $\mathrm{SL}_2(\mathbb{Z})$, μια f ειναι cusp form αν και μόνο αν $a_0{=}0$. Συχνα θα γράφουμε $f(q)$ αντί για $f^*(q)$.

Ο τρόπος που ορίστηκαν οι modular μορφές μπορεί να φαντάζει παράξενος. Επίσης, δεν είναι προφανές με ποιόν τρόπο αυτές αντιστοιχίζονται με τα διαφορικά των $X(\Gamma)$. Εξηγούμε τώρα αυτήν την σύνδεση.

Θεωρούμε μια διαφορική μορφή $\omega = f(z)dz$ στο $\mathbb{H}$, όπου η f είναι μερόμορφη στο $\mathbb{H}$, και Γ μια υποομάδα πεπερασμένου δείκτη της $\Gamma(1)$. Θέλουμε να βρούμε ποιες πρέπει να είναι οι συνθήκες πάνω στην f ώστε το ω να είναι Γ-αναλλοίωτο. Έστω ένα $\gamma \in \Gamma$, με $\gamma^*(\omega) = \omega$. Αν

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

τότε

$$\gamma^*(\omega) = \omega \Longrightarrow f(\gamma z)d\left(\frac{az+b}{cz+d}\right) = f(z)dz$$

$$\Longrightarrow f(\gamma z)\frac{a(cz+d)-c(az+b)}{(cz+d)^2}dz = f(z)dz$$

$$\Longrightarrow f(\gamma z)\frac{1}{(cz+d)^2} = f(z),$$

δηλαδή το ω είναι Γ-αναλλοίωτο (ορίζεται δηλαδή πάνω στην $\Gamma\backslash\mathbb{H}^*$) αν και μόνο αν η $f(z)$ είναι weakly modular form βάρους 2. Μάλιστα, η αντιστοιχία αυτή

$$\omega = f(z)dz \longleftrightarrow f(z)$$

ανάμεσα στις μερόμορφες διαφορικές μορφές της $\Gamma\backslash\mathbb{H}^*$ και τις μερόμορφες modular μορφές βάρους 2 της Γ είναι 1-1.

Ομοίως, μια k-fold διαφορική μορφή σε μια επιφάνεια Riemann είναι μια διαφορική μορφή η οποία τοπικά μπορεί να δοθεί ως μια έκφραση $\omega = f(z)(dz)^k$. Τότε, η ω είναι Γ-αναλλοίωτη αν και μόνο αν η $f(z)$ είναι μερόμορφη modular μορφή βάρους $2k$. Οι αντιστοιχίες αυτές δεν μεταφέρονται αυτούσιες στην περίπτωση που έχουμε ολομορφία. Μπορεί κανείς να ρωτήσει πόσο αποκλίνει μια τέτοια υπόθεση από την αλήθεια. Την απάντηση την δίνει το λήμμα 4.2.2 παρακάτω.

Σχόλια 4.1.7. Στο σημείο αυτό, είναι ίσως εύλογο να ρωτήσει κανείς από που πηγάζει το αριθμοθεωρητικό ενδιαφέρον των modular forms. Μια πρώτη απάντηση που μπορούμε να δώσουμε είναι πως μπορεί η ακολουθία των a_n να έχει ενδιαφέρον για την θεωρία αριθμών: όπως θα δούμε παρακάτω, μια τέτοια περίπτωση ήταν οι εικασίες του Ramanujan. Επίσης, θα δούμε πως μια αριθμητική ακολουθία πολυωνυμικής τάξης μεγέθους ορίζει, υπό κάποιες συνθήκες μια modular form. Μια βαθύτερη απάντηση δίνει το Modularity Theorem.

Δεν είναι βέβαια προφανές ότι υπάρχουν modular μορφές. Θα δούμε συγκεκριμμένα παραδείγματα modular μορφών για την $\Gamma(1)$, και στην συνέχεια θα χρησιμοποιήσουμε τις σειρές Poincare για να κατασκευάσουμε modular μορφές για τις ομάδες $\Gamma(N)$. Πρίν από αυτό όμως, θα μελετήσουμε τους χώρους M_k, S_k. Αφού αυτοί οι χώροι είναι διανυσματικοί χώροι διαφορικών πάνω σε συμπαγείς επιφάνειες Riemann, η διάσταση του θα μετράται από το Riemann-Roch.

4.2 Οι χώροι $M_k(\Gamma)$ και $S_k(\Gamma)$

Το πιο σημαντικό μη τετριμμένο γεγονός σχετικά με τους διανυσματικούς χώρους $M_k(\Gamma)$ και $S_k(\Gamma)$ είναι πως έχουν πεπερασμένη διάσταση. Η κεντρική ιδέα της απόδειξης είναι η εφαρμογή του Θεωρήματος Riemann-Roch για τις επιφάνειες Riemann $X(\Gamma) = \Gamma\backslash\mathbb{H}^*$.

Θεώρημα 4.2.1. *Αν Γ είναι μια πεπερασμένου δείκτη υποομάδα της $\Gamma(1)$, η διάσταση του $M_{2k}(\Gamma)$ ισούται με*

$$dim M_{2k}(\Gamma) = \begin{cases} 1 & , k = 0 \\ (2k-1)(g-1) + 2\nu_\infty k + \sum_P \left[2k\left(1 - \frac{1}{e_P}\right)\right] & , k \geq 1 \end{cases}$$

όπου g είναι το γένος της $X(\Gamma)$, ν_∞ το πλήθος των μη ισοδύναμων cusps για την Γ, το άθροισμα είναι πάνω από ένα σύνολων αντιπροσώπων των ελλειπτικών σημείων P της Γ, e_P είναι η τάξη του σταθεροποιητή του P στην εικόνα της Γ στην $\Gamma(1)/\pm I$, και με $[x]$ συμβολίζεται το ακέραιο μέρο του x.

Πριν αποδείξουμε το θεώρημα αυτό, ας δούμε το εξής παράδειγμα: έστω $g : \mathbb{D} \to \mathbb{D}$, με $g(z) = z^n$. Αν το $Q \neq 0$, τότε η g είναι τοπικός ισομορφισμός και δεν έχουμε πρόβλημα. Έστω ότι $Q = g(Q) = 0$, f μια άλλη συνάρτηση απ' τον δίσκο στον εαυτό του με ρίζα στο 0, και έστω $f^* = f \circ g$. Αν η f έχει ρίζα τάξης m, τότε η f^* έχει τάξη ρίζας mn. Άρα

$$\mathrm{ord}_Q(f^*) = n\mathrm{ord}_{g(Q)}(f)$$

Αν τώρα $\omega = f(z)(dz)^k$ για κάποια μερόμορφη f και $\omega^* = g^*(\omega)$, παίρνουμε

$$\omega^* = f(z^n)(dz^n)^k = f(z^n)(nz^{n-1}dz)^k = n^k f(z^n) z^{k(n-1)} (dz)^k$$

οπότε

$$\mathrm{ord}_Q(\omega^*) = n\mathrm{ord}_{g(Q)}(\omega) + k(n-1)$$

Το παράδειγμα αυτό μας οδηγεί φυσιολογικά στο επόμενο λήμμα:

Λήμμα 4.2.2. *Έστω f μια modular form βάρους $2k$ για την Γ και ω η αντίστοιχη k-fold διαφορική μορφή της στην $X(\Gamma)$. Έστω ότι το σημείο $Q \in \mathbb{H}^*$ απεικονίζεται μέσω της προβολής p στο $P \in \Gamma\backslash\mathbb{H}^*$. Τότε:*

(i) *Αν το Q είναι ελλειπτικό με πολλαπλότητα n, ισχύει:*

$$\mathrm{ord}_Q(f) = n\mathrm{ord}_P(\omega) + k(n-1)$$

(ii) *Αν το Q είναι cusp, τότε:*

$$\mathrm{ord}_Q(f) = \mathrm{ord}_P(\omega) + k$$

(iii) *Αν το Q δεν είναι ελλειπτικό ή cusp, τότε:*

$$\mathrm{ord}_Q(f) = \mathrm{ord}_P(\omega)$$

Απόδειξη. (i) Η περίπτωση αυτή είναι ισόμορφη με το παράδειγμα που μελετήσαμε.

(ii) Θεωρούμε την απεικόνιση $q : \mathbb{H} \to \mathbb{D}$, με $q(z) \to q = e^{2\pi \mathrm{i} z/h}$, και την $\omega^* = g(q)(dq)^k$ που είναι μια k-fold διαφορική μορφή στον $\mathbb{D}$. Τότε $dq = (2\pi h \mathrm{i}) q dz$, άρα η αντίστροφη εικόνα ω του ω^* στο $\mathbb{H}$ είναι

$$\omega = c_0 g(q(z)) q(z)^k (dz)^k$$

όπου c_0 σταθερά, άρα η ω^* αντιστοιχεί στην modular μορφή

$$f(z) = c_0 g(q(z)) q(z)^k.$$

Άρα $f^*(q) = g(q)q^k$, το οποίο δίνει το ζητούμενο.

(iii) Σε αυτήν την περίπτωση η προβολή p είναι τοπικός ισομορφισμός.

□

Μπορούμε τώρα να αποδείξουμε το θεώρημα 4.2.1:

Απόδειξη. Σημειώσαμε και πιο πάνω πως μια modular form βάρους 0 είναι αναγκαστικά σταθερή. Άρα, για $k = 0$ το θεώρημα είναι προφανές. Έστω $f \in M_{2k}(\Gamma)$ και ω το αντίστοιχο της ολόμορφο διαφορικό στην $X(\Gamma)$. Η ολομορφία της f μας δίνει

$$n\mathrm{ord}_P(\omega) + k(n-1) = \mathrm{ord}_Q(f) \geq 0$$

στις εικόνες των ελλειπτικών σημείων,

$$\mathrm{ord}_P(\omega) + k = \mathrm{ord}_Q(f) \geq 0$$

στις εικόνες των cusps, και

$$n\mathrm{ord}_P(\omega) + k(n-1) = \mathrm{ord}_Q(f) \geq 0$$

στις εικόνες των άλλων σημείων. Αν σταθεροποιήσουμε ένα άλλο διαφορικό ω_0 και γράψουμε $\omega = h\omega_0$, τότε παίρνουμε

$$\mathrm{ord}_P(h) + \mathrm{ord}_P(\omega_0) + k\left(1 - \frac{1}{n}\right) \geq 0$$

στις εικόνες των ελλειπτικών σημείων,

$$\mathrm{ord}_P(h) + \mathrm{ord}_P(\omega_0) + k \geq 0$$

στις εικόνες των cusps, και

$$\mathrm{ord}_P(h) + \mathrm{ord}_P(\omega_0) \geq 0$$

στις εικόνες των άλλων σημείων. Προσθέτωντας κατά μέλη και θέτωντας

$$D = div(\omega_0) + \sum kP_i + \sum \left[k\left(1 - \frac{1}{e_i}\right)\right] P_i,$$

όπου το πρώτο άθροισμα να είναι πάνω απ' όλα τα cusps και το δεύτερο πάνω απ' όλα τα ελλειπτικά σημεία, συμπεραίνουμε ότι

$$div(h) + D \geq 0.$$

Από το πορίσματα του Riemann-Roch (για επιφάνειες Riemann τώρα), ξέρουμε ότι ο βαθμός του divisor μιας 1-fold διαφορικής μορφής ισούται με $2g-2$, άρα ο βαθμός μια k-fold διαφορικής μορφής ισούται $k(2g-2)$. Απ' αυτά συμπεραίνουμε πως ο βαθμός του D είναι ίσος με

$$\deg D = k(2g-2) + \nu_\infty k + \sum_P \left[k\left(1 - \frac{1}{e_p}\right)\right],$$

όπου το άθροισμα είναι πάνω από τα ελλειπτικά P. Τα h βρίσκονται εξ' ορισμού σε 1-1 αντιστοιχία με τις modular μορφές ύψους $2k$. Το Riemann-Roch μας λέει, επειδή $\deg D > 2g-2$, ότι ο χώρος των h έχει διάσταση ίση με

$$\deg D - g + 1 = (2k-1)(g-1) + 2\nu_\infty k + \sum_P \left[2k\left(1 - \frac{1}{e_P}\right)\right],$$

κι αυτό αποδεικνύει το θεώρημα. □

Μια εκτενέστερη ανάλυση των διαστάσεων των $M_k(\Gamma)$ και $S_k(\Gamma)$, η οποία συμπεριλαμβάνει και την περίπτωση όπου $-I \notin \Gamma$ (οπότε οι χώροι περιττού βάρους έχουν μη τετριμμένη διάσταση), περιέχεται στο [Diamond-Shurman, [8] κεφ.3].

Πόρισμα 4.2.3. *Έστω μια f weakly modular μορφή για την Γ βάρους $2k$. Τότε:*

$$\sum \left(\frac{\mathrm{ord}_Q(f)}{e_Q} - k\left(1 - \frac{1}{e_Q}\right)\right) = k(2g-2) + k\nu_\infty$$

όπου το άθροισμα είναι πάνω από ένα σύνολο αντιπροσώπων της $\Gamma\backslash\mathbb{H}^*$, και το e_Q είναι ο δείκτης διακλάδωσης αν $Q \in \mathbb{H}$ και 1 αν το Q είναι cusp.

Απόδειξη. Έστω ω η k-fold διαφορική μορφή στην $\Gamma\backslash\mathbb{H}^*$ που αντιστοιχεί στην f. Δείξαμε πως

$$\frac{\mathrm{ord}_Q(f)}{e_Q} = \mathrm{ord}_P(\omega) + k\left(1 - \frac{1}{e_Q}\right)$$

για τα ελλειπτικά Q της Γ,

$$\mathrm{ord}_Q(f) = \mathrm{ord}_P(\omega) + k$$

για τα cusps Q, και

$$\mathrm{ord}_Q(f) = \mathrm{ord}_P(\omega)$$

για τα υπόλοιπα. Για να συνάγουμε τον τύπο που θέλουμε αθροίζουμε κατά μέλη και χρησιμοποιούμε την παρατήρηση που κάναμε παραπάνω πως $\deg(\mathrm{div}(\omega)) = k(2g-2)$. □

Εφαρμόζωντας τώρα το θεώρημα 4.2.1 για την modular ομάδα $\Gamma(1)$ παίρνουμε το επόμενο πόρισμα:

Πόρισμα 4.2.4. *Για την $\mathrm{SL}_2(\mathbb{Z}) = \Gamma(1)$ ισχύει*

$$\dim M_{2k}(\mathrm{SL}_2(\mathbb{Z})) = 1 - k + \left[\frac{k}{2}\right] + \left[\frac{2k}{3}\right]$$

για κάθε $k \geq 1$.

Από το πόρισμα 4.2.4 υπολογίζουμε πως οι χώροι $M_4(\Gamma(1))$, $M_6(\Gamma(1))$, $M_8(\Gamma(1))$ και $M_{10}(\Gamma(1))$ έχουν διάσταση 1, ενώ ο $M_2(\Gamma(1))$ έχει διάσταση 0. Θα μελετήσουμε τώρα μερικά παραδείγματα που θα μας επιτρέψουν να γράψουμε γεννήτορες για τους χώρους $M_{2k}(\Gamma(1))$.

4.3 Παραδείγματα modular μορφών και αναπτύγματα Fourier

Μελετάμε κάποια συγκεκριμμένα παραδείγματα modular μορφών, καθώς επίσης και την modular συνάρτηση j, όπως επίσης και την συνάρτηση η του Dedekind. Στην πραγματικότητα, δεν είναι δύσκολο να δει κάποιος πως έχουμε ήδη συναντήσει τα περισσότερα παραδείγματα που ακολουθούν.

4.3α′ Σειρες Eisenstein

Το πρώτο παράδειγμα, που το συναντήσαμε στην μελέτη των διπλά περιοδικών συναρτήσεων και της δομής της $E(\mathbb{C})$, είναι το δισδιάστατο ανάλογο της συνάρτησης $\zeta(s)$ του Riemann.

Έστω L ο χώρος των lattices στο $\mathbb{C}$. Με $\Lambda(\omega_1, \omega_2) \equiv \Lambda$ συμβολίζουμε, όπως και προηγουμένως, το lattice με βάση τα ω_1, ω_2, όπου $\omega_1/\omega_2 \in \mathbb{H}$.

Λήμμα 4.3.1. *Έστω $F : L \to \mathbb{C}$ συνάρτηση τέτοια ώστε $F(\lambda\Lambda) = \lambda^{-2k}F(\Lambda)$ για κάθε λ στο $\mathbb{C}^*$ ($\mathbb{C}\backslash(0)$). Τότε η $f(z) = F(\Lambda(z, 1))$ είναι weakly modular form βάρους $2k$ για τη $\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})$. Επιπλέον, η αντιστοιχία $F \to f$ είναι 1-1 και επί.*

Απόδειξη. Έστω $F(\omega_1, \omega_2) = F(\Lambda(\omega_1, \omega_2))$. Αφού η F είναι βάρους $2k$, έχουμε

$$F(\lambda\omega_1, \lambda\omega_2) = \lambda^{-2k}F(\omega_1, \omega_2)$$

για κάθε $\lambda \in \mathbb{C}$, και, εξ′ ορισμού, έπεται ότι

$$F(a\omega_1 + b\omega_2, c\omega_1 + d\omega_2) = F(\omega_1, \omega_2)$$

για κάθε

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

Απο την πρώτη σχέση, έπεται ότι η ποσότητα

$$\omega_2^{2k}F(\omega_1, \omega_2)$$

είναι αναλλοίωτη υπό την απεικόνιση $(\omega_1, \omega_2) \to (\lambda\omega_1, \lambda\omega_2)$, άρα εξαρτάται μόνο από την ποσότητα ω_1/ω_2. Έστω μια $f(z)$ τέτοια ώστε

$$F(\omega_1, \omega_2) = \omega_2^{-2k}f(\omega_1/\omega_2).$$

Η πρώτη σχέση τώρα γράφεται

$$(c\omega_1 + d\omega_2)^{-2k}f(a\omega_1 + b\omega_2/c\omega_1 + d\omega_2) = \omega_2^{-2k}f(\omega_1/\omega_2),$$

ή αλλιώς

$$(cz + d)^{-2k}f(\frac{az + b}{cz + d}) = f(z)$$

το οποίο δείχνει ότι η f είναι modular form. Αντιστρόφως, δοθείσης f, ορίζουμε την F από την τρίτη σχέση. □

Πόρισμα 4.3.2. *Για κάθε $k > 1$, οι σειρές Eisenstein*

$$G_{2k}(z) = \sum_{(m,n):m,n\in\mathbb{Z}\setminus(0,0)} \frac{1}{(mz+n)^{2k}}$$

είναι modular forms βάρους $2k$ για την $\mathrm{SL}_2(\mathbb{Z})$.

Απόδειξη. Υπενθυμίζουμε ότι

$$G_{2k}(\Lambda) = \sum_{\omega\in\Lambda,\omega\neq 0} \frac{1}{\omega^{2k}}.$$

Αυτό μας δίνει ότι $G_{2k}(\lambda\Lambda) = \lambda^{-2k}G_{2k}(\Lambda)$. Άρα, από το προηγούμενο λήμμα, η

$$G_{2k}(z) = G_{2k}(\Lambda(z,1))$$

είναι weakly modular. Από την πρόταση 2.10.10, οι $G_{2k}(z)$, για $k > 1$, είναι ολόμορφες στο $\mathbb{H}$. Τέλος, από την ομοιόμορφη σύγκλιση, για την τιμή στο cusp $\mathrm{i}\infty$ έχουμε ότι

$$\lim_{z\to \mathrm{i}\infty} G_{2k}(z) = \sum_{n\in\mathbb{Z},n\neq 0} \frac{1}{n^{2k}} = 2\sum_{n=1}^{\infty} \frac{1}{n^{2k}} = 2\zeta(2k).$$

Άρα οι G_{2k}, για $k > 1$, είναι ολόμορφες παντού, το οποίο μας δίνει ότι οι G_{2k} είναι modular forms για την $\Gamma(1)$. □

Παρατηρήσαμε πως οι χώροι $M_4(\Gamma(1))$, $M_6(\Gamma(1))$, $M_8(\Gamma(1))$ και $M_{10}(\Gamma(1))$ έχουν διάσταση 1. Συνδυάζοντας το γεγονός αυτό με το προηγούμενο πόρισμα βλέπουμε πως για $k = 2, 3, 4, 5$

$$M_{2k}(\Gamma(1)) = \langle G_{2k}\rangle$$

και αφού οι G_{2k} δεν μηδενίζονται στο άπειρο, έπεται πως

$$\dim S_{2k}(\Gamma(1)) = 0$$

για $k = 2, 3, 4, 5$.

Ένας άλλος στόχος μας είναι να υπολογίσουμε, αν γίνεται, τους συντελεστές Fourier των modular μορφών που ορίζουμε. Για τις G_{2k} οι συντελεστές Fourier δίνονται από τον παρακάτω τύπο:

Θεώρημα 4.3.3. *Για κάθε $k \geq 2$ ισχύει*

$$G_{2k}(z) = G^*_{2k}(q) = 2\zeta(2k) + 2\frac{(2\pi\mathrm{i})^{2k}}{(2k-1)!}\sum_{n=1}^{\infty}\sigma_{2k-1}(n)q^n,$$

όπου η συνάρτηση $\sigma_k(n)$ ορίζεται από τον τύπο

$$\sigma_k(n) = \sum_{d|n} d^k.$$

Για να το αποδείξουμε, θα χρειαστούμε το επόμενο λήμμα.

Λήμμα 4.3.4. *Για κάθε $k \geq 1$,*

$$\zeta(2k) = \frac{2^{2k-1}}{(2k)!} B_k \pi^{2k}$$

όπου οι αριθμοί Bernoulli ορίζονται από τον τύπο

$$\frac{x}{e^x - 1} = 1 - \frac{x}{2} + \sum_{k=1}^{\infty} (-1)^{k+1} B_k \frac{x^{2k}}{(2k)!}$$

Απόδειξη. Συνδυάζοντας τους τύπους

$$cos(z) = \frac{e^{\mathrm{i}z} + e^{-\mathrm{i}z}}{2}, sin(z) = \frac{e^{\mathrm{i}z} - e^{-\mathrm{i}z}}{2\mathrm{i}}$$

παίρνουμε

$$cot(z) = \mathrm{i} + \frac{2\mathrm{i}}{e^{2\mathrm{i}z} - 1}.$$

Αν στον τύπο που ορίζει τους αριθμούς Bernoulli αντικαταστήσουμε το x με $2\mathrm{i}z$, βρίσκουμε

$$zcot(z) = 1 - \sum_{k=1}^{\infty} B_k \frac{2^{2k} z^{2k}}{(2k)!}.$$

Από την άλλη μεριά, λογαριθμώντας και παραγωγίζοντας κατά μέλη στον τύπο του απειρογινομένου για το $sin(z)$:

$$sin(z) = z \prod_{n=1}^{\infty} \left(1 - \frac{z^2}{n^2 \pi^2}\right)$$

λαμβάνουμε τον τύπο

$$\begin{aligned} zcot(z) &= 1 - \sum_{n=1}^{\infty} \frac{2z^2/n^2\pi^2}{1 - z^2/n^2\pi^2} = 1 + 2\sum_{n=1}^{\infty} \frac{z^2}{z^2 - n^2\pi^2} \\ &= 1 - 2\sum_{n=1}^{\infty} \sum_{k=1}^{\infty} \frac{z^{2k}}{n^{2k}\pi^{2k}} \\ &= 1 - 2\sum_{n=1}^{\infty} \left(\sum_{k=1}^{\infty} \frac{1}{n^{2k}}\right) \frac{z^{2k}}{\pi^{2k}} \\ &= 1 - 2\sum_{n=1}^{\infty} \zeta(2k) \frac{z^{2k}}{\pi^{2k}} \end{aligned}$$

οπότε, οι δύο τύποι για το $zcot(z)$ μας δίνουν

$$1 - \sum_{k=1}^{\infty} B_k \frac{2^{2k} z^{2k}}{(2k)!} = 1 - 2\sum_{n=1}^{\infty} \zeta(2k) \frac{z^{2k}}{\pi^{2k}}$$

και εξισώνοντας τους συντελεστές παίρνουμε το ζητούμενο. □

Αποδεικνύουμε τώρα το θεώρημα 4.3.3.

Απόδειξη. Δείξαμε πριν ότι

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

Αντικαθιστώντας όπου z το πz και διαιρώντας με z παίρνουμε

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

Δείξαμε επίσης ότι

$$cot(z) = \mathrm{i} + \frac{2\mathrm{i}}{e^{2\mathrm{i}z} - 1}.$$

Αντικαθιστώντας τώρα όπου z το πz και πολλαπλασιάζοντας με π παίρνουμε

$$\pi cot(\pi z) = \pi\mathrm{i} - \frac{2\pi\mathrm{i}}{1-q} = \pi\mathrm{i} - 2\pi\mathrm{i}\sum_{n=1}^{\infty} q^n.$$

Εξισώνοντας παίρνουμε

$$\frac{1}{z} + \sum_{n=1}^{\infty} \left(\frac{1}{z+n} + \frac{1}{z-n} \right) = \pi\mathrm{i} - 2\pi\mathrm{i}\sum_{n=1}^{\infty} q^n.$$

Παραγωγίζοντας κατά μέλη, η $(k-1)$-οστή παράγωγος δίνει την εξίσωση

$$\sum_{n\in\mathbb{Z}} \frac{1}{(n+z)^k} = \frac{1}{(k-1)!}(-2\pi\mathrm{i})^k \sum_{n=1}^{\infty} n^{k-1} q^n.$$

Άρα, για τις σειρές Eisenstein παίρνουμε

$$\begin{aligned} G_{2k}(z) &= \sum_{(m,n)\neq(0,0)} \frac{1}{(nz+m)^{2k}} \\ &= 2\zeta(2k) + 2\sum_{n=1}^{\infty}\sum_{m\in\mathbb{Z}} \frac{1}{(nz+m)^{2k}} \\ &= 2\zeta(2k) + \frac{2(-2\pi\mathrm{i})^{2k}}{(2k-1)!}\sum_{n=1}^{\infty}\sum_{a=1}^{\infty} n^{2k-1} q^{an} \\ &= 2\zeta(2k) + \frac{2(2\pi\mathrm{i})^{2k}}{(2k-1)!}\sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n \end{aligned}$$

□

Άμεσο πόρισμα των παραπάνω είναι το ακόλουθο:

Πόρισμα 4.3.5. *$G_{2k} = 2\zeta(2k)E_{2k}(z)$, όπου*

$$E_{2k}(z) = 1 + \gamma_k \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n$$

και

$$\gamma_k = (-1)^k \frac{4k}{B_k}.$$

Οι $E_{2k}(z)$ λέγονται κανονικοποιημένες σειρές Eisenstein.

Ένα πλήθος χρήσιμων ταυτοτήτων μπορούν αν αποδειχθούν με χρήση των αναπτυγμάτων Fourier των σειρών Eisenstein. Για παράδειγμα, η σχέση $E_4^2 = E_8$ δίνει την ταυτότητα

$$\sigma_7(n) = \sigma_3(n) + 120 \sum_{i=1}^{n-1} \sigma_3(i)\sigma_3(n-i)$$

για $n \geq 1$.

Παρατηρήσαμε και πριν, όταν είδαμε ότι ο $M(\Gamma)$ είναι graded ring, ότι ένας γραμμικός συνδυασμός δυνάμεων modular μορφών είναι modular μορφή. Ωστόσο, το επόμενο παράδειγμα, η συνάρτηση Δ της διακρίνουσας, έχει ξεχωριστή σημασία, μιας και, εξ΄ ορισμού, η τιμή της στο $z \in \mathbb{H}$ ταυτίζεται με την διακρίνουσα του lattice $\Lambda(z, 1)$.

4.3β΄ Η συνάρτηση $\Delta(z)$

Έστω $g_2(z) = 60G_4(z)$ και $g_3(z) = 140G_6(z)$. Η συνάρτηση (διακρίνουσας) $\Delta(z)$ ορίζεται από τον τύπο

$$\Delta(z) = {g_2}^3(z) - 27{g_3}^2(z)$$

Πρόταση 4.3.6. *Η $\Delta(z)$ είναι cusp form βάρους 12 για την $\Gamma(1)$.*

Απόδειξη. Το ότι η Δ είναι modular μορφή βάρους 12 για την $\Gamma(1)$ είναι άμεσο από το πόρισμα 4.3.2. Για το γεγονός ότι μηδενίζεται στο άπειρο, αρκεί να κάνει κανείς τον υπολογισμό

$$\Delta(\infty) = 60^3 G_4^3(\infty) - 27 \cdot 140^2 G_6^2(\infty) = 60^3 \cdot 8 \cdot \frac{\pi^{12}}{90^3} - 27 \cdot 140^2 \cdot 4 \cdot \frac{\pi^{12}}{945^2} = 0$$

όπου οι τελευταίοι υπολογισμοί έπονται από το λήμμα 4.3.4. Άρα, η Δ μηδενίζεται στο cusp ∞. □

Η Δ έχει ξεχωριστό ενδιαφέρον. Από τον ορισμό της έπεται ότι η τιμή της Δ στο z ισούται, όπως τονίσαμε και προηγουμένως, με την διακρίνουσα της ελλειπτικής καμπύλης που αντιστοιχεί στο lattice με βάση $\{1, z\}$. Εφαρμόζωντας το πόρισμα 4.2.3 για την $\Gamma(1)$ και για $k = 6$, βλέπουμε ότι η Δ έχει ρίζα τάξης 1 στο ∞, και καμία άλλη ρίζα.

Πρόταση 4.3.7. *Ο πολλαπλασιασμός με Δ ορίζει έναν ισομορφισμό διανυσματικών χώρων*

$$M_{2k-12}(\Gamma(1)) \cong S_{2k}(\Gamma(1)).$$

Απόδειξη. Η απεικόνιση

$$M_{2k-12}(\Gamma(1)) \longrightarrow S_{2k}(\Gamma(1))$$

με

$$f \longrightarrow f\Delta$$

είναι, προφανώς, ομομορφισμός. Έστω τώρα μια $f \in S_{2k}(\Gamma(1))$. Τότε: f/Δ ανήκει στον $M_{2k-12}(\Gamma(1))$ επειδή η Δ έχει έναν απλό πόλο στο ∞ και η f έχει πόλο εκεί. Οι απεικονίσεις $f \to f/\Delta$ και $f/\Delta \to f$ είναι η μία αντίστροφη της άλλης, άρα ο πολλαπλασιασμός με Δ είναι ισομορφισμός. □

Θεώρημα 4.3.8. *Για τον graded ring $M(\Gamma(1))$ ισχύει*

$$M(\Gamma(1)) = \bigoplus_{k=0}^{\infty} M_{2k}(\Gamma(1)) = \mathbb{C}[G_4, G_6]$$

Απόδειξη. Πρώτα θα δείξουμε ότι το σύνολο

$$A_{2k} = (G_4^m \cdot G_6^n : 4m + 6n = 2k)$$

είναι βάση του $M_{2k}(\Gamma(1))$. Η απόδειξη θα γίνει με επαγωγή στο k. Για $k \leq 3$ είναι προφανές. Έστω ένας $k \geq 4$. Διαλέγουμε $m \geq 0$ και $n \geq 0$ τέτοιους ώστε $4m + 6n = 2k$ (παρατηρείστε ότι τέτοιοι m και n υπάρχουν) και θέτουμε $g = G_4^m \cdot G_6^n$. Η g δεν μηδενίζεται στο ∞. Αν f είναι μια συνάρτηση $\in M_{2k}$, τότε η

$$f - \frac{f(\infty)}{g(\infty)} g$$

μηδενίζεται στο ∞, άρα είναι cusp form βάρους $2k$. Από την πρόταση 4.3.6, και αφού οι cusp forms βάρους 12 έχουν διάσταση 1, υπάρχει $h \in M_{2k-12}$ με

$$f - \frac{f(\infty)}{g(\infty)} g = \Delta \cdot h \Longrightarrow f = \frac{f(\infty)}{g(\infty)} g + \Delta \cdot h,$$

οπότε, η επαγωγική υπόθεση μας δίνει ότι $f \in$ στον χώρο που παράγει το A_{2k}. Η απεικόνιση

$$\mathbb{C}[G_4 \cdot G_6] \longrightarrow \bigoplus_{k=0}^{\infty} M_{2k}(\Gamma(1))$$

είναι επί. Θα δείξουμε ότι είναι και 1-1. Αν δεν ήταν, η G_4^3/G_6^2 θα ικανοποιούσε μια αλγεβρική εξίσωση πάνω απ' το $\mathbb{C}$, οπότε θα ήταν σταθερή. Αυτό είναι άτοπο γιατί $G_4(\rho) = 0 \neq G_6(\rho)$, ενώ $G_4(\mathrm{i}) \neq 0 = G_6(\mathrm{i})$. □

Το επόμενο θεώρημα εκφράζει την συνάρτηση της διακρίνουσας ως απειρογινόμενο, και θα μας οδηγήσει στην μελέτη των συντελεστών Fourier της Δ.

Θεώρημα 4.3.9 (Jacobi)**.** *Αν $q = e^{2\pi i z}$, τότε*

$$\Delta(z) = \Delta(q)^* = (2\pi)^{12} q \prod_{n=1}^{\infty} (1 - q^n)^{24}.$$

Απόδειξη. Θεωρούμε την συνάρτηση

$$F(z) = f(q) = q \prod_{n=1}^{\infty} (1 - q^n)^{24}.$$

Θα δείξουμε ότι η Δ είναι πολλαπλάσιο της f. Για να το κάνουμε αυτό, αρκεί να δείξουμε ότι η f είναι μια cusp μορφή βάρους 12. Αν το δείξουμε, τότε, από το γεγονός ότι ο χώρος $S_{12}(\Gamma(1))$ έχει διάσταση 1 θα έχουμε το ζητούμενο. Για την δικαιολόγηση του συντελεστή $(2\pi)^{12}$, δείτε [Silverman, [31], κεφ. 1].

Ότι η f είναι cusp, είναι άμεσο, μιας και το ανάπτυγμα της μηδενίζεται στο 0. Η ολομορφία της στον δίσκο είναι επίσης προφανής. Για την F είναι επίσης προφανές ότι $F(z+1)=F(z)$. Η απόδειξη θα έχει ολοκληρωθεί αν δείξουμε ότι

$$F(-1/z)=z^{12}F(z).$$

Ορίζουμε τις σειρές

$$G_1(z)=\sum_n{\sum_m}' \frac{1}{(m+nz)^2},$$

$$G(z)=\sum_m{\sum_n}' \frac{1}{(m+nz)^2},$$

$$H_1(z)=\sum_n{\sum_m}' \frac{1}{(m+nz)(m-1+nz)},$$

$$H(z)=\sum_m{\sum_n}' \frac{1}{(m+nz)(m-1+nz)},$$

όπου ο τόνος σημαίνει, για τις μεν G και G_1 ότι το άθροισμα εκτείνεταιι πάνω από όλους τους $m\in\mathbb{Z}$, $n\in\mathbb{Z}$ με $(m,n)\neq(0,0)$, για τις δε H και H_1 ότι το άθροισμα εκτείνεται πάνω από όλους τους $m\in\mathbb{Z}$, $n\in\mathbb{Z}$ με $(m,n)\neq(0,0),(1,0)$. Τηλεσκοπικά, για της H και H_1 υπολογίζουμε

$$H_1=2, H=2-2\frac{\pi\mathrm{i}}{z}.$$

Επειδή η σειρά με γενικό όρο

$$\frac{1}{(m+nz)(m-1+nz)}-\frac{1}{(m+nz)^2}=\frac{1}{(m+nz)^2(m-1+nz)}$$

συγκλίνει απολύτως, έπεται ότι $G_1-H_1=G-H$. Άρα, οι σειρές G και G_1 συγκλίνουν, και μάλιστα

$$G_1(z)-G(z)=H_1(z)-H(z)=\frac{2\pi\mathrm{i}}{z}.$$

Από την σχέση $G_1(-1/z)=z^2G(z)$, έπεται ότι

$$G_1(-1/z)=z^2G_1(z)-2\pi\mathrm{i}z.$$

Χρησιμοποιώντας την ίδια τεχνική που εφαρμόσαμε στην απόδειξη του θεωρήματος 4.3.3, παίρνουμε το ανάπτυγμα

$$G_1(z)=\frac{\pi^2}{3}-8\pi^2\sum_{n=1}^{\infty}\sigma_1(n)q^n.$$

Η λογαριθμική παράγωγος της f δίνει την εξίσωση:

$$\frac{dF}{F}\equiv\frac{df}{f}=\frac{dq}{q}\left(1-24\sum_{n=1}^{\infty}\sigma_1(n)q^n\right),$$

οπότε, συγκρίνοντας τις δύο τελευταίες εξισωσεις, παίρνουμε την σχέση

$$\frac{dF}{F} = \frac{6\mathrm{i}}{\pi} G_1(z)dz.$$

Η τελευταία εξίσωση, σε συνδυασμό με την συναρτησιακή σχεση $G_1(-1/z) = z^2 G_1(z) - 2\pi \mathrm{i} z$ δίνουν ότι

$$\frac{dF(-1/z)}{F(-1/z)} = \frac{dF(z)}{F(z)} + 12\frac{dz}{z}.$$

Δηλαδή, οι $F(-1/z)$ και $z^{12}F(z)$ έχουν την ίδια λογαριθμική παράγωγο. Έπεται πως υπάρχει μια σταθερά C τέτοια ώστε

$$F(-1/z) = Cz^{12}F(z)$$

για κάθε $z \in \mathbb{H}$. Θέτοντας $z = \mathrm{i}$ παίρνουμε $C = 1$, που είναι ακριβώς η ζητούμενη σχέση. □

Ορισμός 4.3.10. *Θεωρούμε το ανάπτυγμα Fourier της* Δ

$$\Delta(z) = \Delta(q)^* = (2\pi)^{12} q \prod_{n=1}^{\infty} (1-q^n)^{24} = \sum_{n=1}^{\infty} \tau(n) q^n.$$

Η ακολουθία των συντελεστών Fourier $\tau(n)$ *της* Δ *ονομάζεται συνάρτηση* τ *του Ramanujan.*

Σχόλια 4.3.11. Το 1916 ο Ramanujan έκανε την εικασία, χωρίς να μπορέσει να την αποδείξει, πως η τ έχει τις ακόλουθες ιδιότητες:

(i) $\tau(mn) = \tau(m)\,\tau(n)$ όταν μκδ$(m,n) = 1$ (δηλαδή η $\tau(n)$ είναι πολλαπλασιαστικκή συνάρτηση),

(ii) $\tau(p^{r+1}) = \tau(p)\tau(p^r) - p^{11}\tau(p^{r-1})$ για κάθε πρώτο p και $r > 0$,

(iii) $|\tau(p)| \leqslant 2p^{11/2}$ για κάθε πρώτο p.

Οι δύο πρώτες ιδιότητες αποδείχθηκαν από τον Mordell το 1917 ([Mordell, [24]]), και η τρίτη, που ονομάστηκε Εικασία τ του Ramanujan, αποδείχθηκε από τον Deligne το 1974 ως συνέπεια της απόδειξης της Εικασίων του Weil για τις Z-συναρτήσεις των αλγεβρικών varieties. Πιο συγκεκριμμένα, ο Deligne έδειξε την γενική εικασία Ramanujan-Petersson

Θεώρημα 4.3.12 (Deligne)**.** *Αν η* $f = \sum a_n q^n$ *είναι cusp form βάρους* $2k$ *για την* $\Gamma(1)$ *και είναι κανονικοποιημένη ομοιόμορφη ιδιομορφή για τους τελεστές Hecke (παράγραφος 4.5), τότε για κάθε* $n \geq 1$ *ισχύει*

$$|a_n| \leq \sigma_0(n) n^{k-\frac{1}{2}}.$$

Ένα πλήθος αποτελεσμάτων είναι γνωστά για την ακολουθία $\tau(n)$, όπως κάποιες διάσημες εικασίες του Ramanujan για τις ιδιότητες διαιρετότητας της $\tau(n)$. Απ΄ την άλλη μέρια, υπάρχουν πλήθος ανοικτών εικασίων, όπως η ακόλουθη:

Εικασία 4.3.13 (Lehmer). *Για κάθε $n \geq 1$ ισχύει*

$$\tau(n) \neq 0.$$

Θα δείξουμε παρακάτω ένα ασθενέστερο από την εικασία του Ramanujan αποτέλεσμα για την τάξη μεγέθους των συντελεστών Fourier μιας cusp form, που οφείλεται στον Hecke.

Ωστόσο, οι δύο πρώτες ιδιότητες της τ θα αποδειχθούν πιο ουσιαστικός παράγοντας για την εξέλιξη της θεωρίας. Η προσπάθεια για την απόδειξη τους θα μας οδηγήσει στον ορισμό των τελεστών Hecke, ενώ θα δούμε κι ότι είναι αυτές ακριβώς οι ιδιότητες που επιτρέπουν στην L-σειρά της Δ να έχει γινόμενο Euler.

4.3γ΄ Η j-συνάρτηση $j(z)$

Η επόμενη συνάρτηση που κατασκευάζουμε, η οποία καλείται j-συνάρτηση, είναι παράδειγμα μιας modular συνάρτησης. Μια σημαντική ιδιότητα της περιγράφεται στην επόμενη πρόταση.

Πρόταση 4.3.14. *Υπάρχει μοναδική modular function J της $\mathrm{SL}_2(\mathbb{Z})$, ολόμορφη στο $\mathbb{H}$ και με απλό πόλο στο ∞, τέτοια ώστε $J(i) = 1$ και $J(\rho) = 0$*

Απόδειξη. Έχουμε ήδη δει πως οι επιφάνεις Riemann $\Gamma(1)\backslash\mathbb{H}^*$ και $\mathbb{P}^1(\mathbb{C})$ είναι ισόμορφες. Θεωρούμε έναν ισομορφισμό

$$f : \Gamma(1)\backslash\mathbb{H}^* \longrightarrow \mathbb{P}^1(\mathbb{C})$$

Έστω $f(\rho) = a$, $f(\mathrm{i}) = b$ και $f(\infty) = c$. Τότε, υπάρχει μοναδικός μετασχηματισμός Mobius από την $\mathbb{P}^1(\mathbb{C})$ στον εαυτό της που να στέλνει τα a, b και c στα 0, 1 και ∞ αντίστοιχα. Συνθέτοντας με την f παίρνουμε την J που επιθυμούμε.

Για την μοναδικότητα, αρκεί να παρατηρήσουμε πως αν η g είναι μια δεύτερη συνάρτηση όπως στην εκφώνηση, τότε η $g \circ f^{-1}$ είναι ένας αυτομορφισμός της $\mathbb{P}^1(\mathbb{C})$ που σταθεροποιεί τα 0, 1 και ∞, άρα είναι σταθερή. □

Θεωρούμε την συνάρτηση

$$j(z) = 1728\frac{g_2^3(z)}{\Delta(z)}.$$

Τότε η j είναι $\Gamma(1)$-αναλλοίωτη, αφού οι $g_2^3(z)$ και $\Delta(z)$ είναι και οι δύο modular forms βάρους 12. Αφού οι $g_2^3(z)$ και $\Delta(z)$ είναι ολόμορφες στο $\mathbb{H}$ και η Δ δεν μηδενίζεται στο $\mathbb{H}$, έπεται πως η j είναι ολόμορφη στο $\mathbb{H}$. Επίσης, η g_2 δεν μηδενίζεται στο ∞, ενώ η Δ έχει ρίζα τάζης 1 εκεί. Άρα, η j έχει στο ∞ απλό πόλο. Άρα η

$$j : \Gamma(1)\backslash\mathbb{H}^* \longrightarrow \mathbb{P}^1(\mathbb{C})$$

είναι ισομορφισμός επιφανειών Riemann. Πιο συγκεκριμμένα, ισχύει ότι $j(z) = 1728J(z)$. Περαιτέρω, το θεώρημα ύπαρξης για τους χώρους των μερόμορφων συναρτήσεων των συμπαγών επιφανειών Riemann (θεώρημα 3.2.13) μας δίνει ως πόρισμα ότι κάθε $f \in M(\mathbb{P}^1(\mathbb{C}))$ είναι ρητή συνάρτηση της j.

Παρατηρείστε πως εξ΄ ορισμού, η τιμή της j στο σημείο z είναι j-αναλλοίωτη της ελλειπτικής καμπύλης που αντιστοιχεί στο lattice με βάση τα $\{1, z\}$.

Πόρισμα 4.3.15. *Άν f είναι μια μερόμορφη συνάρτηση στο $\mathbb{H}$, τότε τα ακόλουθα είναι ισοδύναμα*

(i) *Η f είναι modular συνάρτηση για την $\Gamma(1)$.*

(ii) *Η f είναι πηλίκο δύο modular μορφών ιδίου βάρους.*

(iii) *Η f είναι ρητή συνάρτηση της j.*

Απόδειξη. Προφανής από την παραπάνω συζήτηση. □

Θεώρημα 4.3.16. *Για το ανάπτυγμα j^* της j ισχύει*

$$j^*(q) = \frac{1}{q} + 744 + 196884q + ... = \frac{1}{q} + \sum_{n=1}^{\infty} c(n)q^n$$

όπου $c(n) \in \mathbb{Z}$ για κάθε $n \geq 1$.

Οι συντελεστές της j συνάρτησης έχουν πολύ σημαντική ιστορία. Για παράδειγμα, συνδέονται με την διάσημη Moonshine conjesture.

Μια πολύ σημαντική εφαρμογή της συνάρτησης j είναι μια εναλλακτική απόδειξη του ακόλουθου σημαντικού θεωρήματος της κλασσικής μιγαδικής ανάλυσης, του μικρού θεωρήματος του Picard:

Θεώρημα 4.3.17 (Μικρό θεώρημα του Picard)**.** *Μια μη σταθερή ακέραια συνάρτηση πιάνει κάθε μιγαδικό αριθμό με το πολύ μία εξαίρεση.*

Απόδειξη. Υποθέτουμε ότι η f είναι μια ακέραια συνάρτηση που δεν λαμβάνει τις τιμές a και b, όπου $a \neq b$. Θα δείξουμε ότι η f είναι σταθερή. Έστω

$$g(z) = \frac{f(z) - a}{b - a}.$$

Τότε, η g είναι ακέραια και δεν λαμβάνει τις τιμές 0 και 1.

Η J απεικονίζει το άνω μιγαδικό ημιεπίπεδο σε μια επιφάνεια Riemann με σημεία διακλάδωσης τις εικόνες των ρ, i και ∞. Η αντίστροφη J^{-1} της J απεικονίζει αυτήν την επιφάνεια στην κλειστότητα ενός θεμελιώδους χωρίου της $\Gamma(1)$. Αφού $J'(z) = 0$ αν και μόνο αν $z = \rho$ ή $z = \mathrm{i}$, κάθε μονότιμος κλάδος της J^{-1} είναι τοπικά αναλυτικός παντού, εκτός από τα σημεία $J(\rho) = 0$, $J(\mathrm{i}) = 1$ και $J(\infty) = \infty$. Για κάθε μονότιμο λοιπόν κλάδο της J^{-1}, η σύνθεση

$$h(z) = J^{-1}(g(z))$$

είναι μονότιμη και τοπικά αναλυτική σε κάθε πεπερασμένο z με $g(z) \neq 0$ ή 1. Άρα, η h επεκτείνεται συνεχώς στο μιγαδικό επίπεδο. Από το monodromy theorem, η επέκταση της h είναι μονοτιμη αναλυτική, δηλαδή ακέραια. Έπεται πως και η

$$\phi(z) = e^{\mathrm{i}h(z)}$$

είναι ακέραια. Όμως

$$h(z) \in \mathbb{H} \Longrightarrow \Im(h(z)) > 0 \Longrightarrow |\phi(z)| = e^{-\Im(h(z))} < 1.$$

Από το θεώρημα του Liouville, η ϕ είναι σταθερή, άρα και οι h και g είναι σταθερές. Τέλος, συμπεραίνουμε πως η $f(z) = (b - a)g(z) + a$ είναι σταθερή. □

Μια ακόμα πολύ σημαντική εφαρμογή της j συνάρτησης είναι η απόδειξη του Uniformization θεωρήματος για ελλειπτικές καμπύλες (θεώρημα 2.10.20):

Απόδειξη. Έστω E μια ελλειπτική καμπύλη πάνω από το $\mathbb{C}$, με

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

και j_0 η j-αναλλοίωτη της. Αφού η συνάρτηση $j(z)$ είναι αναλυτικός ισομορφισμός $\Gamma(1)\backslash\mathbb{H} \to \mathbb{C}$, υπάρχει ένα z_0 στο $\mathbb{H}$ με $j(z_0) = j_0$. Τότε, η ελλειπτική καμπύλη E_{z_0} με εξίσωση

$$y^2 = 4x^3 - g_2(z_0)x - g_3(z_0)$$

έχει j-αναλλοίωτη ίση με j_0, και επειδή το $\mathbb{C}$ είναι αλγεβρικά κλειστό έπεται ότι οι E και E_{Z_0} είναι ισόμορφες. Όμως

$$\mathbb{C}/(\mathbb{Z} + z_0\mathbb{Z}) \cong E_{z_0} \cong E,$$

και αυτός ο ισομορφισμός μας δίνει το lattice που θέλαμε. □

4.3δ′ Η συνάρτηση $\eta(z)$

Ορίζουμε τώρα την συνάρτηση $\eta(z)$ του Dedekind:

Ορισμός 4.3.18. *Ορίζουμε την συνάρτηση*

$$\eta(z) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n),$$

όπου $q = e^{2\pi \mathrm{i} z}$, δηλαδή η η ορίζεται έτσι ώστε $\Delta(z) = (2\pi)^{12}\eta(z)^{24}$.

Η $\eta(z)$ έχει σημαντικές αριθμοθεωρητικές ιδιότητες. Για παράδειγμα, ικανοποιεί τους μετασχηματισμούς:

Πρόταση 4.3.19. *Αν $z \in \mathbb{H}$, τότε*

(i)
$$\eta\left(-\frac{1}{z}\right) = (\mathrm{i}z)^{1/2}\eta(z).$$

(ii)
$$\eta(z+1) = e^{\pi \mathrm{i}/12}\eta(z)$$

(iii) *Για κάθε $\gamma \in \Gamma(1)$ υπάρχει $\epsilon = \epsilon(\gamma)$, τέτοιο ώστε $\epsilon^{24} = 1$ και*

$$\eta(\gamma z) = \epsilon\{-\mathrm{i}(cz + d)\}^{1/2}\eta(z)$$

όπου

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Η ακριβής έκφραση του ϵ εκφράζεται συναρτήσει των αθροισμάτων Dedekind, και ικανοποιεί έναν νόμο αντιστροφής. Για λεπτομέρειες σχετικά με τις ιδιότητες της συνάρτησης η παραπέμπουμε στον [Apostol, [2], κεφ. 3].

Τα παραπάνω παραδείγματα δίνουν μια εικόνα με τι μοιάζουν οι modular συναρτήσεις και οι modular μορφές. Έχουμε δείξει πως η μελέτη τους μπορεί να μεταφερθεί σε μερόμορφες και ολόμορφες συναρτήσεις στον μοναδιαίο δίσκο $\mathbb{D}$, και οι αλγεβρικές συνθήκες μεταφράζονται σε κάποιες ιδιότητες που πρέπει να ικανοποιούν οι συντελεστές τους. Οι επόμενες προτάσεις είναι ένα τέτοιο παράδειγμα των ιδιοτήτων που επιβάλλουν οι αλγεβρικές συνθήκες στους συντελεστές.

Πρόταση 4.3.20. *Αν $f = G_{2k}$, η τάξη των συντελεστών a_n είναι n^{2k-1}.*

Απόδειξη. Από το θεώρημα 4.3.3, έπεται πως υπάρχει σταθερά $A > 0$ τέτοια ώστε

$$a_n = (-1)^k A\sigma_{2k-1}(n),$$

άρα

$$|a_n| = A\sigma_{2k-1}(n) \geq An^{2k-1}.$$

Περαιτέρω,

$$\frac{|a_n|}{n^{2k-1}} = A\sum_{d|n} \frac{1}{d^{2k-1}} \leq A\sum_{d=1}^{\infty} \frac{1}{d^{2k-1}} = A\zeta(2k-1) < +\infty.$$

□

Πρόταση 4.3.21 (Hecke)**.** *Έστω*

$$f(z) = f^*(q) = \sum_{n=0}^{\infty} a_n q^n$$

μια cusp form της $\mathrm{PSL}_2(\mathbb{Z})$ βάρους $2k$. Τότε $a_n = O(n^k)$.

Απόδειξη. Η f είναι cusp, δηλαδή $a_0 = 0$, άρα μπορούμε να εξάγουμε κοινό παράγοντα το q έξω από το ανάπτυγμα της $f^*(q)$. Τότε, αν $y = \Im(z)$, παίρνουμε:

$$|f(z)| = O(q) = O(e^{-2\pi y})$$

καθώς $q \to 0$. Θέτουμε $\phi(z) = |f(z)|y^k$. Η ϕ είναι αναλλοίωτη υπό την δράση τη $\Gamma(1)$, συνεχής στο θεμελιώδες χωρίο της $\Gamma(1)$, και, από τον προηγούμενο τύπο, η ϕ τείνει στο 0 όταν $y \to \infty$. Άρα η ϕ είναι φραγμένη, δηλαδή υπάρχει M τέτοιο ώστε:

$$|f(z)| \leq My^{-k}.$$

για κάθε $z \in \mathbb{H}$. Σταθεροποιούμε το y, και αφήνουμε το x να κυμανθεί από 0 έως 1. Το σημείο $q = e^{2\pi\mathrm{i}(x+\mathrm{i}y)}$ κινείται σε κύκλο C_y με κέντρο το 0. Από τον τύπο των ολοκληρωτικών υπολοίπων:

$$a_n = \frac{1}{2\pi\mathrm{i}} \int_{C_y} f(z)q^{-n-1}dq = \int_0^1 f(x+\mathrm{i}y)q^{-n}dx.$$

Τον τύπο αυτόν μπορεί κάποιος να τον συνάγει και από τον τύπο που δίνει τους συντελεστές Fourier, μιας περιοδικής συνάρτησης. Από το φράγμα της $|f(z)|$, συνάγουμε το φράγμα

$$|a_n| \leq My^{-k}e^{2\pi ny}.$$

Αυτή η ανισότητα ισχύει για κάθε $y > 0$. Επιλέγοντας $y = 1/n$, έχουμε

$$|a_n| \leq e^{2\pi}Mn^k,$$

και το ζητούμενο έπεται. □

Πρόταση 4.3.22. *Αν η f είναι μια modular μορφή βάρους $2k$ για την $\Gamma(1)$ ύψους $2k$ που δεν είναι cusp form, τότε η τάξη των a_n είναι ακριβώς n^{2k-1}.*

Απόδειξη. Παρατηρούμε ότι ισχύει η σχέση $M_{2k} = S_{2k} \bigoplus \mathbb{C}G_{2k}$. Γράφουμε την $f \in M_{2k}$ στην μορφή $f = g + \lambda G_{2k}$ με $\lambda \neq 0$ και g cusp μορφή. Η τάξη της g είναι n^k και της G_{2k} είναι n^{2k-1}. Αυτό σημαίνει ότι η f έχει την ζητούμενη τάξη. □

Πριν την απόδειξη του Delinge που προαναφέραμε, ο Selberg είχε επίσης καταφέρει να αποδείξει την ακόλουθη

Πρόταση 4.3.23 (Selberg)**.** *Αν η f είναι cusp, τότε*

$$a_n = O(n^{k-\frac{1}{4}+\epsilon})$$

για κάθε ϵ θετικό.

Ο επόμενος στόχος είναι να ορίσουμε modular μορφές για τις πρωταρχικές ομάδες ισοτιμίας. Ο στόχος αυτός μας οδηγεί να ορίσουμε ένα εσωτερικό γινόμενο στον χώρο των cusp μορφών.

4.4 Σειρές Poincare και το εσωτερικό γινόμενο του Petersson

Επιθυμούμε λοιπόν να κατασκευάσουμε modular μορφές για υποομάδες της $\Gamma(1)$. Ένας άλλος είναι να γράψουμε ένα σύνολο γεννητόρων για τις cusp μορφές μιας υποομάδας Γ της modular ομάδας πεπερασμένου δείκτη. Για να το πετύχουμε αυτό, θα χρησιμοποιήσουμε τις σειρές Poincare. Για να τις ορίσουμε, χρειαζόμαστε την έννοια του αυτομορφικού παράγοντα. Ο αυτομορφικός παράγοντας είναι ένα παράδειγμα ενός συν-κύκλου.

Αν η X είναι μια τοπολογική πολλαπλότητα, μια γραμμική δέσμη (line bundle) είναι μια απεικόνιση τοπολογικών χώρων $\pi : L \to X$ τέτοια ώστε για κάποιο ανοιχτό κάλυμμα του $X = \bigcup U_i$ να ισχύει $\pi^{-1}(U_i) \cong U_i \times \mathbb{R}$. Ομοίως, μια γραμμική δέσμη σε μια επιφάνεια Riemann είναι μια απεικόνιση μιγαδικών πολλαπλοτήτων $\pi : L \to X$ έτσι ώστε η L να είναι τοπικά ισομορφη με $U \times \mathbb{C}$, ενώ μια γραμμική δέσμη σε μια αλγεβρική variety είναι μια απεικόνιση μεταξύ αλγεβρικών varieties $\pi : L \to X$ έτσι ώστε, τοπικά για την Zariski τοπολογία στον X, να ισχύει $L \cong U \times \mathbb{A}^1$.

Αν η L είναι μια γραμμική δέσμη στην επιφάνεια Riemann X, τότε, για κάθε ανοιχτό U στον X, συμβολίζουμε με $\Gamma(U, L)$ την ομάδα των ολόμορφων απεικονίσεων f πάνω απ' το U με $\pi \circ f = id$ (ομάδα των sections του L πάνω απ' το U).

Αν τώρα η Γ είναι μια ομάδα που δρα ελεύθερα και γνήσια ασυνεχώς σε μια επιφάνεια Riemann H, και $X = \Gamma\backslash H$, γράφουμε $\pi : H \to X$ για την συνάρτηση προβολής. Αν η $\pi : L \to X$ είναι μια διανυσματική δέσμη, ορίζουμε

$$\pi^*(L) = \{(h, \ell) \in H \times L : p(h) = \pi(\ell)\}$$

η οποία είναι διανυσματική δέσμη στην H, και η Γ δρα στο $\pi^*(L)$. Αν μας δοθεί ένας ισομορφισμός $i : H \times \mathbb{C} \to \pi^*(L)$, μεταφέρουμε την δράση της Γ στο $\pi^*(L)$ σε μια δράση της Γ στο $H \times \mathbb{C}$. Για κάθε $\gamma \in \Gamma$ και $(\tau, z) \in H \times \mathbb{C}$ γράφουμε

$$\gamma(\tau, z) = (\gamma\tau, j_\gamma(\tau)z)$$

όπου $j_\gamma(\tau) \in \mathbb{C}^*$. Τότε,

$$\gamma\gamma'(\tau, z) = (\gamma\gamma'\tau, j_\gamma(\gamma'\tau) \cdot j_{\gamma'}(\tau) \cdot z).$$

Άρα, θα πρέπει να ισχύει η σχέση

$$j_{\gamma\gamma'}(\tau) = j_\gamma(\gamma'\tau) \cdot j_{\gamma'}(\tau).$$

Ορισμός 4.4.1. *Έστω Γ μια Fuchsian ομάδα. Μια συνάρτηση $j : \Gamma \times \mathbb{H} \longrightarrow \mathbb{C} - \{0\}$ με $j : (\gamma, \tau) \longrightarrow j(\gamma, \tau) = j_\gamma(\tau)$ τέτοια ώστε:*

(i) *για κάθε $\gamma \in \Gamma$, η $\tau \longrightarrow j_\gamma(\tau)$ είναι ολόμορφη στο $\mathbb{H}$*

(ii) *$j_{\gamma\gamma'}(\tau) = j_\gamma(\gamma'\tau) \cdot j_{\gamma'}(\tau)$ για κάθε γ, $\gamma' \in \Gamma$*

λέγεται αυτομορφικός παράγοντας για την Γ. Η δεύτερη ιδιότητα σημαίνει ότι η j είναι ένας 1-συνκύκλος.

Παρατηρείστε ότι αν η j είναι ένας αυτομορφικός παράγοντας και k ένας ακέραιος, τότε η j^k είναι επίσης αυτομορφικός παράγοντας.

Αν έχουμε δυο απεικονίσεις $a : M \to N$ και $b : N \to P$ στις μιγαδικές πολλαπλότητες M, N και P, τότε, στους εφαπτόμενους χώρους έχουμε $(d(b \circ a))_m = (db)_{a(n)} \circ (da)_m$. Άρα, ο κανόνας της αλυσίδας συνεπάγεται ότι η απεικόνιση $j_\gamma(\tau) = (d\gamma)_\tau$ είναι αυτομορφικός παράγοντας.

Για παράδειγμα, θεωρούμε την δράση της modular ομάδας στο $\mathbb{H}$. Αν το $\gamma \in \Gamma(1)$ είναι ο μετασχηματισμός

$$\gamma(z) = \frac{az + b}{cz + d},$$

τότε

$$d\gamma = \frac{1}{(cz + d)^2} dz,$$

δηλαδή $j_\gamma(\tau) = (cz + d)^{-2}$ και $j_\gamma(\tau)^k = (cz + d)^{-2k}$. Αυτή η κατασκευή μας επιτρέπει να αντιλαμβανόμαστε τις modular μορφές ως sections των διανυσματικών δεσμών πάνω στις modular καμπύλες. Η αντιστοιχία αυτή είναι 1-1 (για λεπτομέρειες πάνω σε αυτήν την αντιστοιχία, παραπέμπουμε στον [Milne, [22], κεφάλαιο 4]).

Προχωράμε τώρα στην κατασκευή modular μορφών για τις ομάδες πεπερασμένου δείκτη στην modular ομάδα. Υιοθετούμε τον συμβολισμό Γ' για την εικόνα μιας υποομάδας της $\Gamma \leqslant \mathrm{SL}_2(\mathbb{Z})$ στην $\mathrm{PSL}_2(\mathbb{Z})$.

Ο στάνταρ τρόπος για να ορίσει κανείς Γ-αναλλοίωτες συναρτήσεις είναι ο εξής: δοσμένης μια συνάρτησης h στο $\mathbb{H}$, να θεωρήσει το άθροισμα

$$f(z) = \sum_{\gamma \in \Gamma'} h(\gamma z)$$

η οποία είναι Γ-αναλλοίωτη, εφ' όσον η σειρά συνγκλίνει απολύτως. Μια παραλλαγή αυτού του επιχειρήματος από τον Poincare επιτρέπει να κατασκευάσουμε modular μορφές.

Έστω ένας αυτομορφίκός παράγοντας

$$\Gamma \times \mathbb{H} \to \mathbb{C}, (\gamma, z) \to j_\gamma(z)$$

για την Γ. Εφ' όσον εμείς ενδιαφερόμαστε για την περίπτωση που $j_\gamma(z) = (cz + d)^{2k}$, επιδιώκουμε να ορίσουμε μια συνάρτηση έτσι ώστε

$$f(\gamma z) = j_\gamma(z) f(z).$$

Θεωρούμε την σειρά

$$f(z) = \sum_{\gamma \in \Gamma'} \frac{h(\gamma z)}{j_\gamma(z)}.$$

Αν η σειρά συγκλίνει απολύτως και ομοιόμορφα στα συμπαγή, τότε, χρησιμοποιώντας το γεγονός ότι ο $j_\gamma(z)$ είναι αυτομορφικός παράγοντας, παίρνουμε

$$f(\gamma' z) = \sum_{\gamma \in \Gamma'} \frac{h(\gamma\gamma' z)}{j_\gamma(\gamma' z)} = \sum_{\gamma \in \Gamma'} \frac{h(\gamma\gamma' z)}{j_{\gamma\gamma'}(z)} j_{\gamma'}(z) = j_{\gamma'}(z) f(z)$$

δηλαδή η f ικανοποιεί την ζητούμενη ιδιότητα. Ωστόσο, ένα σημαντικό εμπόδιο είναι πως η σειρά αυτή σπανίως συγκλίνει απολύτως. Αυτό συμβαίνει επειδή μπορεί να υπάρχουν πολλά γ ώστε να ισχύει ταυτοτικά $j_\gamma(z) = 1$. Έστω

$$\Gamma_0 = \{\gamma \in \Gamma' : j_\gamma(z) \equiv 1\}.$$

Αν $j_\gamma(z) = (cz + d)^{-2k}$, τότε

$$\begin{aligned} \Gamma_0 &= \left\{ \pm \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma : c = 0, d = 1 \right\} \\ &= \left\{ \pm \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in \Gamma \right\} \\ &= \left\langle \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \right\rangle, \end{aligned}$$

όπου h είναι το πλάτος του cusp $i\infty$ για την Γ, και γενικά, η Γ_0 του αυτομορφικού παράγοντα $j_\gamma(z)$ είναι υποομάδα της Γ'.

Αν η h είναι μια ολόμορφη Γ_0-αναλλοίωτη συνάρτηση στο $\mathbb{H}$, τότε

$$\frac{h(\gamma_0\gamma z)}{j_{\gamma_0\gamma}(z)} = \frac{h(\gamma z)}{j_{\gamma_0}(\gamma z) j_\gamma(z)} = \frac{h(\gamma z)}{j_\gamma(z)},$$

δηλαδή η $\frac{h(\gamma z)}{j_\gamma(z)}$ είναι $\Gamma_0\gamma$-σταθερή. Θεωρούμε λοιπόν την σειρά

$$f(z) = \sum_{\Gamma_0\backslash\Gamma'} \frac{h(\gamma z)}{j_\gamma(z)}.$$

Αν η σειρά αυτή συγκλίνει απολύτως και ομοιόμορφα στα συμπαγή, τότε η συζήτηση που προηγήθηκε δείχνει ότι λαμβάνουμε έτσι μια ολόμορφη συνάρτηση f με $f(\gamma z) = j_\gamma(z)f(z)$. Για $j_\gamma(z) = (cz+d)^{2k}$ και Γ μια ομάδα πεπερασμένου δείκτη στην $\mathrm{SL}_2(\mathbb{Z})$, η Γ_0 παράγεται από τις μεταφορές $z \to z+h$ για κάποιο h, και μια τυπική αναλλοίωτη υπό αυτές τις μεταφορές συνάρτηση είναι η $\exp(2\pi i n z/h)$.

Ορισμός 4.4.2. *Η σειρά Poincare ύψους $2k$ και χαρακτήρα n για την Γ είναι η σειρά*

$$\phi_n(z) = \sum_{\Gamma_0\backslash\Gamma'} \frac{\exp\left(\frac{2\pi i n\gamma(z)}{h}\right)}{(cz+d)^{2k}}.$$

Λήμμα 4.4.3. *Οι σειρές Poincare $\phi_n(z)$ για $k \geq 1$, $n \geq 0$, είναι modular μορφές βάρους $2k$ για την Γ. Επίσης, για $n \geq 1$, οι $\phi_n(z)$ είναι cusp μορφές.*

Η ιδέα της απόδειξης, όσον αφορά την σύγκλιση, είναι να συγκρίνουμε τις σειρές Poincare με τις

$$\sum_{(m,z)\in\mathbb{Z},(m,n)\neq(0,0)} \frac{1}{|mz+n|^{2k}}.$$

Η πλήρης απόδειξη δεν είναι ιδιαίτερα δύσκολη, και παραλείπεται.

Στόχος μας είναι να δείξουμε το ακόλουθο θεώρημα:

Θεώρημα 4.4.4. *Οι σειρές Poincare $\phi_n(z)$ βάρους $2k$ παράγουν τον χώρο $S_{2k}(\Gamma)$.*

Για να μπορέσουμε να το αποδείξουμε, θα χρειαστεί να ορίσουμε ένα εσωτερικό γινόμενο στον $S_{2k}(\Gamma)$. Για να γίνει αυτό, πρέπει να θεωρήσουμε το άνω μιγαδικό ημιεπίπεδο με την υπερβολική μετρική. Ως γνωστόν, στην υπερβολική μετρική του $\mathbb{H}$ οι γεωδαισιακές είναι οι κάθετες ευθείες καθώς και τα ημικύκλια που είναι κάθετα στην πραγματική ευθεία.

Η ομάδα $\mathrm{PSL}_2(\mathbb{R})$ δρα στο $\mathbb{H}$, και μάλιστα αποτελεί την ομάδα των μετασχηματισμών που διατηρούν την απόσταση και τον προσανατολισμό.

Το μέτρο

$$\mu(U) = \iint_U \frac{dxdy}{y^2}$$

είναι το ανάλογο του $\iint_U dxdy$ στο $\mathbb{R}^2$ - είναι αναλλοίωτο υπό την δράση της $\mathrm{PSL}_2(\mathbb{R})$.

Μπορούμε λοιπόν να θεωρούμε το

$$\mu(D) = \iint_D \frac{dxdy}{y^2}$$

για κάθε θεμελιώδες χωρίο D μιας Γ - το γεγονός ότι η διαφορική μορφή $y^{-2}dxdy$ είναι Γ-αναλλοίωτη συνεπάγεται ότι το $\mu(D)$ είναι καλά ορισμένο.

Υπάρχουν πολλά στοιχεία της σχέσης μεταξύ των Fuchsian ομάδων και της υπερβολικής δομής στο $\mathbb{H}$ τα οποία δεν μπορούμε, λόγω χώρου, να μελετήσουμε εκτενέστερα.

Για παράδειγμα, μπορεί κανείς να δείξει (και η απόδειξη δεν είναι ιδιαίτερα δύσκολη) ότι το θεμελιώδες χωρίο D της Γ μπορεί πάντοτε να επιλεγεί ούτως ώστε να είναι ένα υπερβολικό τρίγωνο. Επίσης, μια μορφή του Gauss-Bonnet σε αυτήν την περίπτωση είναι ο εξής τύπος:

$$\iint_D \frac{dxdy}{y^2} = 2\pi\left(2g - 2 + \nu_\infty + \sum\left(1 - \frac{1}{e_P}\right)\right).$$

Εκτενέστερες αναλύσεις της σχέσης της υπερβολικής γεωμετρίας του $\mathbb{H}$ με τις Fuchsian ομάδες υπάρχουν στους [Miyake, [21], κεφ.1], [Bump, [5], κεφ.1] και [Shimura, [29], κεφ.1].

Έστω λοιπόν δύο modular μορφές f, g βάρους $2k$ για μια υποομάδα $\Gamma \leqslant_f \Gamma(1)$.

Λήμμα 4.4.5. *Η διαφορική μορφή $f(z)\overline{g(z)}y^{2k-2}dxdy$ είναι $\mathrm{SL}_2(\mathbb{R})$-αναλλοίωτη (όπου, ως συνήθως, $z = x + \mathrm{i}y$).*

Απόδειξη. Έστω ένα $\gamma = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$. Τότε, από τον ορισμό της modular form, έχουμε ότι

$$f(\gamma z) = (cz + d)^{2k} f(z),$$
$$\overline{g(\gamma z)} = \overline{(cz + d)}^{2k}\overline{g(z)}.$$

και από το κεφάλαιο 3:

$$\Im(\gamma z) = \frac{\Im(z)}{|cz + d|^2}.$$

Το γ δρα στην μορφή $dxdy$ ως

$$\gamma^*(dxdy) = \frac{dxdy}{|cz + d|^4},$$

όπου η τελευταία εξίσωση έπεται από το γεγονός ότι μια ολόμορφη συνάρτηση w του z πολλαπλασιάζει τα εμβαδά με $|w'(z)|^2$ και τον τύπο $d\gamma/dz = 1/(cz + d)^2$. Για να πάρουμε το ζητούμενο, υψώνουμε την τρίτη εξίσωση στην $(2k - 2)$-οστή δύναμη, και πολλαπλασιάζουμε κατά μέλη. □

Λήμμα 4.4.6. *Αν D είναι ένα θεμελιώδες χωρίο για την Γ, και η f ή η g είναι cusp, τότε το ολοκλήρωμα*

$$\iint_D f(z)\overline{g(z)}y^{2k-2}dxdy$$

συγκλίνει.

Απόδειξη. Προφανώς το ολοκλήρωμα συγκλίνει αν εξαιρέσουμε μια περιοχή χύρω από κάθε cusp. Κοντά στο cusp $\mathrm{i}\infty$, $f(z)\overline{g(z)} = O(e^{-cy})$ για κάποια σταθερά $c > 0$, κι άρα το ολοκλήρωμα φράσσεται από ένα ολοκλήρωμα της μορφής

$$\int_{y_1}^{\infty} e^{-cy}y^{2k-2}dy < \infty.$$

Για τα υπόλοιπα cusps, εργαζόμαστε αναλόγως. □

Ορισμός 4.4.7. *Έστω f και g δύο modular forms βάρους $2k$ για την $\Gamma \leqslant_f \Gamma(1)$, εκ των οποίων η μία τουλάχιστον είναι cusp form. Τότε, το Petersson εσωτερικό γινόμενο τους ορίζεται ως η ποσότητα*

$$\langle f, g\rangle = \iint_D f(z)\overline{g(z)}y^{2k-2}dxdy.$$

Το λήμμα 4.4.5 λέει ότι το $\langle f, g\rangle$ είναι ανεξάρτητο του D. Επίσης, το $\langle f, g\rangle$ έχει τις εξής ιδιότητες:

(i) Είναι γραμμικό στην πρώτη μεταβλητή και ημιγραμμικό στην δεύτερη,

(ii) $\langle f, g\rangle = \overline{\langle g, f\rangle}$,

(iii) $\langle f, f\rangle > 0$ για κάθε $f \neq 0$.

Δηλαδή, το $\langle \cdot, \cdot\rangle$ είναι μια θετικά ορισμένη Ερμιτιανή μορφή στον $S_{2k}(\Gamma)$, κι άρα ο χώρος

$$(S_{2k}(\Gamma), \langle \cdot, \cdot\rangle)$$

είναι ένας χώρος Hilbert πεπερασμένης διάστασης.

Θεώρημα 4.4.8. *Έστω f μια cusp form βάρους $2k \geq 2$ για την Γ, και ϕ_n οι σειρές Poincare βάρους $2k$ και χαρακτήρα $n \geq 1$ για την Γ. Έστω επίσης h το πλάτος του $i\infty$ στην Γ, και*

$$f = \sum a_n e^{\frac{2\pi i n z}{h}}$$

το Fourier ανάπτυγμα της f. Τότε:

$$\langle f, \phi_n\rangle = \frac{h^{2k}(2k-2)!}{(4\pi n)^{2k-1}}a_n.$$

Απόδειξη. (Σκιαγράφηση) Γράφουμε την ϕ_n ως άθροισμα (ορισμός της ϕ_n) και εναλλάσουμε την σειρά ολοκληρώματος και αθροίσματος. Γράφοντας το σαν ολοκλήρωμα πάνω από ένα θεμελιώδες χωρίο της Γ_0 στο $\mathbb{H}$ έχουμε

$$\langle f, \phi_n\rangle = \int_{x=0}^{h}\int_{y=0}^{\infty} f(z)\exp\left(-\frac{2\pi i n z}{h}\right)y^{2(2k-1)}dxdy.$$

Γράφουμε την f σαν αθροισμα, και αλλάζοντας πάλι την σειρά ολοκληρώματος και αθροίσματος έχουμε το ζητούμενο. □

Απόδειξη. (του θεωρήματος 4.4.4) Αν η f είναι ορθογώνια στον χώρο που παράγουν οι σειρές Poincare, τότε, από το προηγούμενο πόρισμα, έπεται ότι όλοι οι συντελεστές της f είναι ίσοι με 0. □

Έχουμε λοιπόν κατασκευάσει μια βάση για τον χώρο $S_{2k}(\Gamma)$ για την τυχαία Γ πεπερασμένου δείκτη στην $\Gamma(1)$. Στο υπόλοιπο της παραγράφου αυτής, κατασκευάζουμε σειρές Einsenstein για την $\Gamma(N)$.

Κατ' αρχάς, η σειρά Poincare βάρους $2k$ και χαρακτήρα 0 για την $\Gamma(N)$ είναι η

$$\phi_0(z) = \sum \frac{1}{(cz+d)^{2k}}$$

όπου το άθροισμα εκτείνεται πάνω απ' όλα τα ζευγάρια (c,d) με c,d σχετικά πρώτους και $(c,d) \equiv (0,1) \mod N$. Η $\phi_0(z)$ δεν είναι cusp, γιατί αν και μηδενίζεται σε όλα τα πεπερασμένα cusps, στο $i\infty$ παίρνει την τιμή 1.

Έστω S το σύνολο των cusps της $\Gamma(N)$. Για κάθε συνάρτηση $\nu : S \to \mathbb{C}$, θέλουμε να κατασκευάσουμε μια modular μορφή f βάρους $2k$ για την $\Gamma(N)$, τέτοια ώστε η f περιορισμένη στο S να ταυτίζεται με την ν. Επίσης, θέλουμε η f να είναι κάθετη στον $S_{2k}(\Gamma(N))$ ως προς το εσωτερικό γινόμενο του Petersson. Θα κατασκευάσουμε μια συνάρτηση η οποία παίρνει την τιμή 1 σε ένα cusp, 0 στα υπόλοιπα, και είναι ορθογώνια στον $S_{2k}(\Gamma(N))$.

Θεωρούμε τον συνήθη αυτομορφικό παράγοντα

$$j_\gamma(z) = \frac{1}{(cz+d)^{2k}}.$$

Έστω P ένα cusp για την $\Gamma(N)$, διάφορο του $i\infty$, και έστω ένα σ στην $\Gamma(N)$ τέτοιο ώστε $\sigma(P) = i\infty$. Ορίζουμε την

$$\phi(z) = j_\sigma(z)^k \phi_0(\sigma z).$$

Λήμμα 4.4.9. *Η $\phi(z)$ είναι modular form βάρους $2k$ για την $\Gamma(N)$, παίρνει την τιμή 1 στο P και μηδενίζεται στα άλλα cusps.*

Απόδειξη. Έστω ένα γ στην $\Gamma(N)$. Κατ' αρχάς, πρέπει να δείξουμε ότι $\phi(\gamma z) = j_\gamma(z)^{-k}\phi(z)$. Από τον ορισμό της ϕ, ισχύει

$$\phi(\gamma z) = j_\sigma(\gamma z)^k \phi_0(\sigma\gamma z).$$

Όμως η $\Gamma(N)$ είναι κανονική στην $\Gamma(1)$, άρα $\sigma\gamma\sigma^{-1} \in \Gamma(N)$, κι άρα

$$\phi_0(\sigma\gamma z) = \phi_0(\sigma\gamma\sigma^{-1}\sigma z) = j_{\sigma\gamma\sigma^{-1}}(\sigma z)^{-k}\phi_0(\sigma z).$$

Συγκρίνοντας αυτόν τον τύπο με τον τύπο

$$\phi(\gamma z) = j_\gamma(z)^{-k}\phi(z) = j_\gamma(z)^{-k} j_\sigma(z)^k \phi_0(\sigma z),$$

βλέπουμε ότι για αρκεί να αποδείξουμε

$$j_\sigma(\gamma z) j_{\sigma\gamma\sigma^{-1}}(\sigma z)^{-1} = j_\gamma(z)^{-1} j_\sigma(z),$$

ή ισοδύναμα,

$$j_\sigma(\gamma z) j_\gamma(z) = j_{\sigma\gamma\sigma^{-1}}(\sigma z) j_\sigma(z).$$

Εξ' αιτίας όμως της βασικής ιδιότητας του αυτομορφικού παράγοντα, αυτό είναι ισοδύναμο με την προφανή σχέση

$$j_{\sigma\gamma}(z) = j_{\sigma\gamma\sigma^{-1}\sigma}(z).$$

Οι υπόλοιποι ισχυρισμοί είναι άμεσες συνέπειες του ορισμού της $\phi(z)$ και της $\phi_0(z)$. □

Έστω T ένα σύνολο αντιπροσώπων της Γ_0 στην $\Gamma(N)$. Τότε, εξ' ορισμού, για την $\phi(z)$ παίρνουμε

$$\phi(z) = j_\sigma(z)^k \phi_0(\sigma z)$$

$$= j_\sigma(z)^k \cdot \sum_{\tau \in T} j_\tau(\sigma z)^k$$
$$= \sum_{\tau \in T} j_{\tau\sigma}(z)^k$$
$$= \sum_{\gamma \in T\sigma} j_\gamma(z)^k.$$

Αν τώρα

$$\sigma = \begin{pmatrix} a_0 & b_0 \\ c_0 & d_0 \end{pmatrix},$$

τότε το σύμπλοκο $T\sigma$ περιέχει ακριβώς ένα στοιχείο της $\Gamma(N)'$ για κάθε ζεύγος (c,d) με $\mu\kappa\delta(c,d) = 1$ και $(c,d) \equiv (c_0, d_0) \mod N$.

Ορισμός 4.4.10. (i) *Μια περιορισμένη σειρά Eisenstein βάρους $2k > 2$ για την $\Gamma(N)$ είναι μια σειρά*

$$G(z; c_0, d_0; N) = \sum \frac{1}{(cz+d)^{2k}}$$

όπου το άθροισμα εκτείνεται πάνω απ΄ όλα τα ζεύγη (c,d) με $\mu\kappa\delta(c,d) = 1$ και $(c,d) \equiv (c_0, d_0) \mod N$ (όπου το (c_0, d_0) είναι ένα ζεύγος τέτοιο ώστε $\mu\kappa\delta(c_0, d_0, N) = 1$).

(ii) *Μια γενικευμένη σειρά Eisenstein βάρους $2k > 2$ για την $\Gamma(N)$ είναι μια σειρά*

$$G(z; c_0, d_0; N) = \sum \frac{1}{(cz+d)^{2k}}$$

όπου το άθροισμα εκτείνεται πάνω απ΄ όλα τα ζεύγη (c,d) με $(c,d) \equiv (c_0, d_0) \mod N$ και $c,d) \neq (0,0)$ (εδώ δεν απαιτείται να ισχύει $\mu\kappa\delta(c_0, d_0, N) = 1$).

Αν $G(z; c_0, d_0; N)$ και $G(z; c_1, d_1; N)$ είναι δύο περιορισμένες σειρές Eisenstein, τότε

$$G(z; c_0, d_0; N) = G(z; c_1, d_1; N)$$

αν και μόνο αν $(c_0, d_0) \equiv \pm(c_1, d_1) \mod N$. Από την άλλη, για κάθε cusp έχουμε μια περιορισμένη σειρά Eisenstein, και αυτές οι σειρές είναι γραμμικά ανεξάρτητες. Μετρώντας, βλέπουμε ότι υπάρχει ακριβώς μία περιορισμένη σειρά Eisenstein για κάθε cusp, κι άρα οι διακεκριμμένες περιορισμένες σειρές Eisenstein είναι γραμμικά ανεξάρτητες.

Πρόταση 4.4.11. *Οι γενικευμένες σειρές Eisenstein είναι ακριβώς οι γραμμικοί συνδυασμοί των περιορισμένων σειρών Eisenstein.*

Μερικές φορές, οι γενικευμένες σειρές Eisenstein ορίζονται ακριβώς ως οι γραμμικοί συνδυασμοί των περιορισμένων.

Παρατήρηση 4.4.12. Το Petersson εσωτερικό γινόμενο $\langle f, g \rangle$ ορίζεται αν μια εκ των f, g είναι cusp form. Αν η f είναι cusp και η g περιορισμένη σειρά Eisenstein, τότε

$$\langle f, g \rangle = 0,$$

και από την πρόταση 4.4.11 έπεται ότι οι σειρές Eisenstein είναι το ορθογώνιο συμπλήρωμα του $S_{2k}(\Gamma(N))$ στον $M_{2k}(\Gamma(N))$.

4.5 Τελεστές Hecke

Σκοπός μας σε αυτήν την παράγραφο είναι να ορίσουμε και να μελετήσουμε μια πολύ σημαντική οικογένεια τελεστών που δρουν πάνω στις modular forms, τους τελεστές Hecke.

Οι τελεστές Hecke πρωτοεμφανίζονται στην εργασία του Mordell όπου έλυσε την εικασία του Ramanujan για την πολλαπλασιαστικότητα της $\tau(n)$ (σχόλια 4.3.11, πόρισμα 4.5.13 παρακάτω). Αυστηρός ορισμός δόθηκε στην δεκαετία του '30 από τον Hecke, ο οποίος ανέπτυξε και το βασικό κομμάτι της θεωρίας τους. Αποτελούν οικογένειες φυσιολογικών τελεστών T_n για τις υποομάδες της modular ομάδας υπό την ακόλουθη έννοια: για κάθε Γ υποομάδα πεπερασμένου δείκτη της $\mathrm{PSL}_2(\mathbb{Z})$ και για κάθε $n \in \mathbb{N}$ ορίζεται μια ακολουθία τελεστών

$$T_n : M_{2k}(\Gamma) \to M_{2k}(\Gamma)$$

που διατηρούν τους cusp υπόχωρους, δηλαδή

$$T_n(S_{2k}(\Gamma)) \leqslant S_{2k}(\Gamma).$$

Η ιδιότητα τους αυτή θα δούμε ότι έχει σημαντικό αριθμοθεωρητικό ενδιαφέρον. Περαιτέρω, θα δούμε κι άλλες σημαντικές ιδιότητες τους, όπως για παράδειγμα ότι κάθε T_n της $\Gamma(1)$ είναι Ερμιτιανός στον $S_{2k}(\Gamma(1))$ ως προς το εσωτερικό γινόμενο του Petersson. Θα μελετήσουμε τους τελεστές Hecke κυρίως για την $\Gamma(1)$. Το πιο σημαντικό αριθμοθεωρητικό πρόβλημα που συνδέεται με αυτούς είναι το πρόβλημα των ιδιοσυναρτήσεων και των ιδιοτιμών τους.

Η διαδικασία ορισμού τους είναι η εξής: πρώτα ορίζεται οικογένεια τελεστών T_n στα lattices , και μέσω του λήμματος 4.3.1 στις modular forms. Για αρχή θα χρειαστούμε ένα κλασσικό λήμμα για γραμμικές απεικονίσεις σε πεπερασμένης διάστασης διανυσματικούς χώρους:

Λήμμα 4.5.1. *Έστω V ένας πεπερασμένης διάσταση διανυσματικός χώρος υπεράνω του $\mathbb{C}$, και μια θετικά ορισμένη Ερμιτιανή μορφή $\langle \cdot, \cdot \rangle$ ορισμένη στον V. Τότε:*

(i) *Αν η $f : V \to V$ είναι Ερμιτιανή γραμμική απεικόνιση, τότε η f είναι διαγωνίσιμη.*

(ii) *Αν $f_1, f_2, \ldots$ είναι ακολουθία Ερμιτιανών γραμμικών απεικονίσεων $: V \to V$ που αντιμετατίθονται, τότε ο V έχει βάση από διανύσματα a_i που είναι ιδιοδιανύσματα για κάθε f_i, $i = 1, 2, \ldots$.*

Απόδειξη. Αυτό είναι το φασματικό θεώρημα για χώρους πεπερασμένης διάστασης. □

Ορίζουμε τώρα τους τελεστές Hecke που δρουν πάνω στα lattices.

Έστω L, όπως και πριν, ο χώρος των lattices στο $\mathbb{C}$, και έστω D η ελεύθερη αβελιανή ομάδα που παράγεται από τα στοιχεία του L. Δηλαδή, τα στοιχεία της D είναι της μορφής:

$$\sum n_i[\Lambda_i],$$

όπου $n_i \in \mathbb{Z}$ και $\Lambda_i \in L$. Για κάθε $n \in \mathbb{N}$ ορίζουμε έναν $\mathbb{Z}$-γραμμικό τελεστή $T_n : D \to D$ με

$$T_n[\Lambda] = \sum_{[\Lambda:\Lambda']=n} [\Lambda'],$$

δηλαδή το άθροισμα εκτείνεται πάνω από όλα τα sublattices του Λ δείκτη n, καθώς και τον τελεστή $R_n \equiv \langle n \rangle : L \to L$, με τύπο

$$R_n[\Lambda] = [n\Lambda].$$

Πρόταση 4.5.2. *Έστω ένα lattice Λ, μια βάση του ω_1, ω_2 και Λ' ένα sublattice του. Τότε $[\Lambda : \Lambda'] = n$ αν και μόνο αν υπάρχει πίνακας*

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

με $\det \gamma = n$, τέτοιος ώστε να ισχύει $\Lambda' = \gamma\Lambda = \Lambda(a\omega_1 + \omega_2, c\omega_1 + d\omega_2)$. Κάθε τέτοιο sublattice του Λ περιέχει το $n\Lambda$, και αφού $[\Lambda : n\Lambda] < \infty$, έπεται ότι το άθροισμα που στον ορισμό του T_n είναι πεπερασμένο. Άρα ο τελεστής T_n ορίζεται καλά.

Οι βασικές ιδιότητες του τελεστή T_n, οι οποίες συνοψίζονται στην επόμενη πρόταση, δείχνουν ότι ο τελεστής αυτός έχει πολλαπλασιαστικές ιδιότητες σαν αυτές που διατυπώνονται στις εικασίες του Ramanujan.

Πρόταση 4.5.3. (i) *Αν μκδ(m, n)=1, τότε*

$$T_m \circ T_n = T_{mn}$$

(ii) *Αν ο p είναι ένας πρώτος αριθμός, και $n \geq 1$, τότε:*

$$T_{p^{n+1}} = T_p \circ T_{p^n} - pR_p \circ T_{p^{n-1}}$$

Απόδειξη. (i) Κατ' αρχάς,

$$T_{mn}[\Lambda] = \sum_{[\Lambda:\Lambda'']=mn} [\Lambda''].$$

Επίσης,

$$T_m \circ T_n = \sum [\Lambda''],$$

όπου το άθροισμα εκτείνεται πάνω από όλα τα ζεύγη (Λ', Λ'') τέτοια ώστε $[\Lambda : \Lambda'] = n$ και $[\Lambda' : \Lambda''] = m$. Όμως, αν το Λ'' είναι ένα sublattice του Λ δείκτη mn, τότε υπάρχει μοναδική αλυσίδα

$$\Lambda'' \subset \Lambda' \subset \Lambda,$$

με $[\Lambda : \Lambda'] = n$, επειδή η ομάδα $\Lambda/mn\Lambda$ είναι το ευθύ άθροισμα μιας ομάδας τάξης m και μιας ομάδας τάξης n.

(ii) Έστω Λ ένα lattice. Τότε

$$T_p \circ T_{p^n}[\Lambda] = \sum [\Lambda''],$$

όπου το άθροισμα εκτείνεται πάνω από τα ζεύγη (Λ', Λ'') τέτοια ώστε $[\Lambda : \Lambda'] = p$ και $[\Lambda' : \Lambda''] = p^n$,

$$T_{p^{n+1}}[\Lambda] = \sum [\Lambda''],$$

όπου το άθροισμα εκτείνεται πάνω από όλα τα Λ'' με $[\Lambda : \Lambda''] = p^{n+1}$, και τέλος

$$pR_p \circ T_{p^{n-1}}[\Lambda] = p \sum R_p[\Lambda'],$$

με το άθροισμα να είναι πάνω από τα $\Lambda' \subset \Lambda$ με $[\Lambda : \Lambda'] = p^{n-1}$. Άρα

$$pR_p \circ T_{p^{n-1}}[\Lambda] = p \sum [\Lambda''],$$

πάνω από τα $\Lambda'' \subset p\Lambda$ με $[p\Lambda : \Lambda''] = p^{n-1}$. Όμως, το καθένα από αυτά τα αθροίσματα είναι ένα άθροισμα από sublattices Λ'' δείκτη p^{n+1} του Λ. Σταθεροποιούμε ένα τέτοιο lattice και έστω a το πλήθος των φορών που εμφανίζεται στο πρώτο άθροισμα και b το πλήθος των φορών που εμφανίζεται στο τελευταίο άθροισμα. Στο δεύτερο άθροισμα εμφανίζεται ακριβώς μια φορά, οπότε, για να δείξουμε το ζητούμενο, θα πρέπει να αποδείξουμε ότι $a - pb = 1$. Διακρίνουμε δύο περιπτώσεις:

Περίπτωση 1η: Το Λ'' δεν περιέχεται στο $p\Lambda$. Τότε προφανώς $b = 0$, και a είναι το πλήθος των Λ' που περιέχουν το Λ'' και είναι δείκτη p στο Λ. Ένα τέτοιο lattice περιέχει το $p\Lambda$, και η εικόνα της στο $\Lambda/p\Lambda$ είναι τάξης p και περιέχει το περιέχει την εικόνα του Λ'', η οποία είναι επίσης τάξης p. Αφού οι υποομάδες της Λ δείκτη p είναι είναι σε 1-1 αντιστοιχία με τις υποομάδες της $\Lambda/p\Lambda$ δείκτη p, έπεται πως υπάρχει ακριβώς ένα lattice Λ', το $\Lambda + p\Lambda''$, άρα $a = 1$.

Περίπτωση 2η: Το Λ'' περιέχεται στο $p\Lambda$. Τότε $b = 1$. Κάθε lattice Λ' δείκτη p περιέχει το $p\Lambda$. Πρέπει να μετρήσουμε το πλήθος των υποομάδων της $\Lambda/p\Lambda$ δείκτη p, και αυτό είναι ίδιο με το πλήθος των γραμμών που διέρχονται από την αρχή των αξόνων στο $\mathbb{F}$-επίπεδο, το οποίο είναι ίσο με $(p^2 - 1)/(p - 1) = p + 1$.

□

Πόρισμα 4.5.4. *Για κάθε m και n φυσικούς αριθμούς ισχύει:*

$$T_m \circ T_n = \sum_{d|gcd(m,n), d>0} d \cdot R_d \circ T_{mn/d^2}$$

Απόδειξη. Μπορούμε να υποθέσουμε ότι $s \leq r$. Πρώτα, με χρήση επαγωγής, αποδεικνύεται εύκολα ότι

$$T_{p^s} \circ T_{p^r} = \sum_{i \leq min(r,s)} p^i \cdot R_{p^i} \circ T_{p^{r+s-2i}}$$

(για $s = 1$ είναι το δεύτερο σκέλος της προηγούμενης πρότασης) και μετά εφαρμόζουμε το (i) της προηγούμενης πρότασης. □

Πόρισμα 4.5.5. *Η $\mathbb{Z}-$υποάλγεβρα του $\mathrm{End}(D)$ που παράγεται από τους T_p και R_p είναι μεταθετική και περιέχει τους T_n για κάθε n.*

Απόδειξη. Και τα δύο συμπεράσματα είναι άμεσα από το πόρισμα 4.5.4. □

Η άλγεβρα του πορίσματος 4.5.5 καλείται μερικές φορές και Hecke άλγεβρα. Αντίστοιχα, για τους τελεστές Hecke που θα ορίσουμε παρακάτω να δρουν στις modular forms, ορίζεται και εκεί μια άλγεβρα Hecke με όμοιο τρόπο.

Επεκτείνουμε τώρα λοιπόν τους τελεστές Hecke με γραμμικό τρόπο στις συναρτήσεις που ορίζονται στα lattices ως εξής:

Έστω μια $F : D \to \mathbb{C}$. Επεκτείνουμε γραμμικά την F σε μια συνάρτηση $F : L \to \mathbb{C}$:

$$F\left(\sum n_i[\Lambda_i]\right) = \sum n_i F(\Lambda_i).$$

Για κάθε τελεστή T στην D, ορίζουμε την $T \cdot F$ να είναι συνάρτηση : $L \to \mathbb{C}$ τέτοια ώστε

$$(T \cdot F)([\Lambda]) = F(T[\Lambda]).$$

Πιο συγκεκριμμένα, για τον τελεστή T_n έχουμε

$$(T_n \cdot F)([\Lambda]) = \sum F([\Lambda'])$$

με το άθροισμα, όπως παραπάνω, να εκτείνεται πάνω από όλα τα sublattices δείκτη n. Αν η F έχει βάρος $2k$, δηλαδή $F(\lambda\Lambda) = \lambda^{-2k}F(\Lambda)$, τότε

$$R_n \cdot F = n^{-2k} \cdot F.$$

Από τον τρόπο που ορίσαμε να δρουν οι τελεστές στις F, την πρόταση 4.5.3 και το πόρισμα 4.5.4, έπεται η επόμενη πρόταση:

Πρόταση 4.5.6. *Έστω $F : L \to \mathbb{C}$ μια ομογενής συνάρτηση βάρους $2k$. Τότε, η $T_n \cdot F$ είναι επίσης βάρους $2k$, και, για κάθε m και n, ισχύει*

$$T_m \cdot T_n \cdot F = \sum_{d|(m,n),d>0} d^{1-2k} \cdot T_{mn/d^2} \cdot F.$$

Ιδιαιτέρως, αν οι m και n είναι σχετικά πρώτοι, τότε

$$T_m \cdot T_n \cdot F = T_{mn} \cdot F,$$

και, αν ο p είναι πρώτος και $n \geq 1$, τότε

$$T_p \cdot T_{p^n} \cdot F = T_{p^{n+1}} \cdot F + p^{1-2k} \cdot T_{p^{n-1}} \cdot F.$$

Για να μπορέσουμε να ορίσουμε τους τελεστές Hecke στην $\Gamma(1)$, θα χρειαστούμε ένα λήμμα για 2×2 πίνακες. Συμβολίζουμε με $M_2(\mathbb{Z})$ τον δακτύλιο των 2×2 πινάκων με στοιχεία από το $\mathbb{Z}$, και με $M(n)$ τα στοιχεία του $M_2(\mathbb{Z})$ με ορίζουσα n.

Λήμμα 4.5.7. *Έστω $A \in M(n)$. Τότε, υπάρχει αντιστρέψιμος πίνακας $U \in M_2(\mathbb{Z})$ τέτοιος ώστε*

$$U \cdot A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix},$$

όπου $ad = n$, $a \geq 1$ και $0 \leq b < d$. Επιπλέον, οι a, b, d είναι μοναδικοί.

Απόδειξη. (Σκιαγράφηση:) Εφαρμόζουμε γραμμικούς μετασχηματισμούς στο A οι οποίοι είναι αντιστρέψιμοι στον $M_2(\mathbb{Z})$, για να φέρουμε τον A σε άνω τριγωνική μορφή. Για την μοναδικότητα, παρατηρούμε ότι ο a είναι ο μέγιστος κοινός διαιρέτης των στοιχείων της πρώτης στήλης του A, το d είναι ο n/a και το b προσδιορίζεται προφανώς μοναδικά modulo d. □

Η $\mathrm{SL}_2(\mathbb{Z})$ δρα στο $M(n)$ με πολλαπλασιασμό από αριστερά, και το λήμμα μας παρέχει ένα σύνολο αντιπροσώπων των τροχιών:

$$M(n) = \bigcup \mathrm{SL}_2(\mathbb{Z}) \cdot \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}.$$

Έστω Λ ένα lattice στο $\mathbb{C}$. Επιλέγουμε μια βάση ω_1, ω_2 για το Λ, δηλαδή $\Lambda = \Lambda(\omega_1, \omega_2)$. Για κάθε $\alpha \in M(n)$, ορίζουμε ως συνήθως $\alpha\Lambda = \Lambda(a\omega_1 + b\omega_2, c\omega_1 + d\omega_2)$, και, όπως σημειώσαμε και παραπάνω, το $\alpha\Lambda$ είναι δείκτη n στο Λ και κάθε sublattice του Λ είναι αυτής της μορφής. Αφού $\alpha\Lambda = \beta\Lambda$ αν και μόνο αν $\alpha = u\beta$ για κάποιο $u \in \mathrm{SL}_2(\mathbb{Z})$, το λήμμα μας λέει ότι τα sublattices του Λ δείκτη n είναι ακριβώς τα

$$\Lambda(a\omega_1 + b\omega_2, 0\omega_1 + d\omega_2),$$

όπου $a, b, d \in \mathbb{Z}$, $ad = n$, $a \geq 1$, $0 \leq b \leq d-1$. Έστω $n = p$. Τότε, τα sublattices του Λ δείκτη p είναι σε 1-1 αντιστοιχία με τις γραμμές που διέρχονται απ' το $(0,0)$ του 2-δισδιάστατου F_p-διανυσματικού χώρου $\Lambda/p\Lambda$. Γράφουμε

$$\Lambda/p\Lambda = F_p e_1 \otimes F_p e_2$$

με $e_i \equiv \omega_i \mod p$. Οι ευθείες απ' το $(0,0)$ καθορίζονται με την τομή τους, αν υπάρχει, με το $(1,0)$. Άρα, υπάρχουν $p+1$ ευθείες από το $(0,0)$, οι

$$F_p \cdot e_1, F_p \cdot (e_1 + e_2), ..., F_p \cdot (e_1 + (p-1)e_2), F_p \cdot e_2.$$

Άρα, υπάρχουν ακριβώς $p+1$ sublattices του $\Lambda(\omega_1, \omega_2)$ δείκτη p, τα

$$\Lambda(\omega_1, p\omega_2), \Lambda(\omega_1 + \omega_2, p\omega_2), ..., \Lambda(p\omega_1, \omega_2),$$

το οποίο συμφωνεί με την γενική θεωρία.

Αν $\alpha \in M(n)$ και $\Lambda' = \alpha\Lambda$, διαλέγουμε βάσεις ω_1, ω_2 για το Λ και ω_1', ω_2' για το Λ' τέτοια ώστε

$$\omega_1' = a\omega_1, \omega_2' = d\omega_2, a, d \in \mathbb{Z}, ad = n, a|d, a \geq 1,$$

και τα a, d προσδιορίζονται μοναδικά. Στην γλώσσα των πινάκων, αυτό σημαίνει ότι

$$M(n) = \bigcup \mathrm{SL}_2(\mathbb{Z}) \cdot \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \cdot \mathrm{SL}_2(\mathbb{Z})$$

όπου η ξένη ένωση είναι πάνω από τα $a, d \in \mathbb{Z}$, $ad = n$, $a \geq 1$.

Στο λήμμα 4.3.1, δείξαμε ότι υπάρχει μια 1-1 αντιστοιχία ανάμεσα στις συναρτήσεις F βάρους $2k$ που ορίζονται πάνω στο L και τις weakly modular f βάρους $2k$ που ορίζονται στο $\mathbb{H}$, ως

$$F(\Lambda(\omega_1, \omega_2)) = \omega_2^{-2k} \cdot f(\omega_1/\omega_2),$$

$$F(\Lambda(z, 1)) = f(z).$$

Έστω λοιπόν $f(z)$ μια modular μορφή βάρους $2k$, και F η αντίστοιχη συνάρτηση βάρους $2k$ στο L. Ορίζουμε την δράση του T_n στην f, έτσι ώστε η $T_n \cdot f(z) \equiv T_n(f)$ να είναι η συνάρτηση στο $\mathbb{Z}$ που αντιστοιχεί στην $n^{2k-1} \cdot T_n \cdot F$ (ο παράγοντας n^{2k-1} εμφανίζεται έτσι ώστε να εμφανίζονται ακέραιοι συντελεστές στις επόμενους τύπους). Δηλαδή:

$$T_n \cdot f(z) \equiv T_n(f(z)) = n^{2k-1} \cdot (T_n \cdot F)(\Lambda(z, 1)).$$

Αναπτύσσωντας, παίρνουμε τον τύπο

$$T_n \cdot f(z) = n^{2k-1} \cdot \sum d^{-2k} f\left(\frac{az+b}{d}\right)$$

όπου το άθροισμα λαμβάνεται πάνω από τα a, b, d τέτοια ώστε $ad = n$, $a \geq 1$, $0 \leq b < d$. Το επόμενο θεώρημα δείχνει ότι οι πολλαπλασιαστικές ιδιότητες των τελεστων T_n που δρουν στα lattices μεταφέρονται στους τελεστές T_n που ορίζονται στις modular μορφές.

Θεώρημα 4.5.8. (i) *Έστω f μία weakly modular form βάρους $2k$ για την $\mathrm{PSL}_2(\mathbb{Z})$, και ένας $n \in \mathbb{N}$. Τότε, η $T_n(f)$ είναι επίσης weakly modular form βάρους $2k$ για την $\mathrm{PSL}_2(\mathbb{Z})$. Επειδή ο T_n διατηρεί την ολομορφία, έπεται πως αν η f είναι modular form, τότε και η $T_n \cdot f$ είναι modular form. Άρα, ο T_n διατηρεί τον $M_k(\Gamma)$.*

(ii) *Αν $\mu\kappa\delta(m,n) = 1$,*

$$T_{mn} \cdot f = T_m \cdot T_n \cdot f.$$

(iii) *Αν ο p είναι ένας πρώτος και $n \geqslant 1$,*

$$T_{p^{n+1}} \cdot f = T_p \cdot T_{p^n} \cdot f - p^{2k-1} \cdot T_{p^{n-1}} \cdot f,$$

(iv) *Αν η f είναι μια modular form βάρους $2k$ για την $\Gamma(1)$, με Fourier ανάπτυγμα*

$$f(q) = \sum_{n=0}^{\infty} a_n q^n$$

τότε

$$T_n \cdot f(z) = \sum_{m=0}^{\infty} c_m q^m,$$

όπου:

$$c_m = \sum_{b \mid gcd(m,n), b \geqslant 1} b^{2k-1} a_{\frac{mn}{b^2}}$$

(v) *ο T_n διατηρεί τον $S_{2k}(\Gamma)$ (αν η f είναι μια cusp form βάρους $2k$, τότε και η $T_n(f)$ είναι cusp form βάρους $2k$).*

Απόδειξη. (i), (ii), (iii) Προφανώς, αν η f είναι μερόμορφη (ολόμορφη) σε ένα σημείο, τότε και η $T_n(f)$ είναι, αφού είναι πεπερασμένο άθροισμα μερόμορφων (αντίστοιχα ολομόρφων).

Το ότι η $T_n \cdot f(z)$ είναι weakly modular έπεται από την συζήτηση που προηγήθηκε του θεωρήματος.

(iv) Ξέρουμε ότι

$$T_n \cdot f(z) = n^{2k-1} \sum_{ad=n, a \geq 1, 0 \leq b < d} d^{-2k} f\left(\frac{az+b}{d}\right).$$

Αντικαθιστώντας το Fourier ανάπτυγμα της f στον τύπο της $T_n \cdot f(z)$, έχουμε

$$T_n \cdot f(z) = n^{2k-1} \sum_{a,b,d, ad=n, a \geq 1, 0 \leq b < d} d^{-2k} \sum_{m=0}^{\infty} a_m q^{2\pi \mathrm{i} \frac{az+b}{d} m}.$$

Όμως,

$$\sum_{0\le b<d} e^{2\pi i \frac{b}{d}m} = d,$$

όταν $d|m$, και 0 αλλιώς. Θέτωντας $m/d = m'$, παίρνουμε

$$T_n \cdot f(z) = n^{2k-1} \sum_{a,d,m',ad=n,a\ge 1} d^{1-2k} a_{m'd} q^{am'}.$$

Ο συντελεστής του q^t σε αυτό το ανάπτυγμα ισούται με

$$\sum_{b|gcd(n,t),b\ge 1} b^{2k-1} a_{\frac{tn}{b^2}}.$$

Αντικαθιστώντας όπου t το m, έχουμε το ζητούμενο.

(v) Αν $a_0 = 0$ τότε $c_0 = a_0 = 0$, άρα η $T_n(f)$ είναι μια cusp form. □

Πόρισμα 4.5.9. (i) $c_0 = \sigma_{2k-1}(n) \cdot a_0$ *και* $c_1 = a_n$.

(ii) *Αν* $n = p$, *όπου* p *πρώτος, τότε, αν* o p *δεν διαιρεί τον* m *έχουμε*

$$c_m = a_{mp}$$

και, αν $p|m$, *τότε*

$$c_m = a_{mp} + p^{2k-1} a_{m/p}.$$

Άρα, οι T_n δρουν στους χώρους $M_{2k}(\Gamma(1))$ και $S_{2k}(\Gamma(1))$, και ικανοποιούν τις πολλαπλασιαστικές σχέσεις

$$T_{mn} = T_m \circ T_n$$

για σχετικά πρώτους m και n και

$$T_{p^{n+1}} = T_p \circ T_{p^n} - p^{2k-1} \cdot T_{p^{n-1}}.$$

για p πρώτο, $r \ge 1$. Ένα ερώτημα που προς το παρόν δεν έχουμε μελετήσει, όσον αφορά τους τελεστές Hecke, είναι η εύρεση των ιδιοτιμών τους και των ιδιοσυναρτήσεων τους (ή ιδιομορφών). Όπως θα δούμε, οι ιδιοσυναρτήσεις αυτές παίζουν σημαντικό ρόλο στην μελέτη των modular forms. Η επόμενη πρόταση μας δίνει κάποιες απλές πληροφορίες για τις ιδιοσυναρτήσεις αυτές.

Πρόταση 4.5.10. *Έστω* f *μια μη μηδενική modular form βάρους* $2k$ *για την* $\Gamma(1)$, *με*

$$f(q) = \sum_{n=0}^{\infty} a_n q^n.$$

Έστω ακόμη ότι η f *είναι ιδιομορφή (δηλαδή ιδιοσυνάρτηση) για κάθε* T_n. *Τότε,* $a_1 \neq 0$. *Αν υποθέσουμε ότι η* f *είναι κανονικοποιημένη (δηλαδή* $a_1 = 1$*), τότε ο* a_n *είναι η ιδιοτιμή του τελεστή* T_n *που αντιστοιχεί στην ιδιομορφή* f.

Απόδειξη. Υποθέτουμε ότι

$$T_n(f) = \lambda(n) \cdot f.$$

Τότε, ο συντελεστής του q στην $T_n(f)$ είναι ο a_n. Όμως, από το δεύτερο μέλος της εξίσωσης, ο συντελεστής του q ισούται και με $\lambda(n)a_1$. Έπεται πως για κάθε $n \ge 1$ ισχύει $a_n = \lambda(n)a_1$. Αν ίσχυε $a_1 = 0$, τότε θα είχαμε $f \equiv 0$, το οποίο είναι αδύνατον. Ο δεύτερος ισχυρισμός τώρα είναι προφανής. □

Καλούμε τις f που είναι ιδιομορφές για κάθε T_n ομοιόμορφες ιδιομορφές.

Πόρισμα 4.5.11. *Δύο κανονικοποιημένες ομοιόμορφες ιδιομορφές του ιδίου βάρους και με τις ίδιες ιδιοτιμές ταυτίζονται.*

Πόρισμα 4.5.12. *Αν η*

$$f = \sum_{n=0}^{\infty} a_n q^n$$

είναι κανονικοποιημένη ομοιόμορφη ιδιομορφή για τους T_n, τότε, αν m, n, p και r είναι όπως στα παραπάνω, ισχύουν

$$a_m a_n = a_{mn}$$

και

$$a_{p^{n+1}} = a_p a_{p^n} - p^{2k-1} a_{p^{n-1}}.$$

Απόδειξη. Αφού οι σχέσεις αυτές ισχύουν για τους T_n, ισχύουν και για τις ιδιομορφές τους. □

Είμαστε σε θέση τώρα να αποδείξουμε τις εικασίες του Ramanujan (ιδιότητες (i) και (ii) στα σχόλια 4.3.12).

Πόρισμα 4.5.13 (Mordell). (i) *Αν $\mu\kappa\delta(m, n) = 1$, τότε*

$$\tau(mn) = \tau(m)\tau(n),$$

δηλαδή η $\tau(n)$ είναι πολλαπλασιαστική συνάρτηση.

(ii) *Για κάθε πρώτο p και $r > 0$*

$$\tau(p^{r+1}) = \tau(p)\tau(p^r) - p^{11}\tau(p^{r-1}).$$

Απόδειξη. Ο τελεστής Hecke T_n διατηρεί τον υπόχωρο $S_{2k}(\Gamma(1))$ του $M_{2k}(\Gamma(1))$. Αφού

$$\dim S_{12}(\Gamma(1)) = 1$$

και $\Delta \in S_{12}(\Gamma(1))$, έπεται πως ο $S_{12}(\Gamma(1))$ παράγεται από την Δ. Άρα, η Δ είναι μια ιδιομορφή για κάθε T_n. Όμως ο συντελεστής του q στο ανάπτυγμα Fourier της Δ είναι 1, άρα η ιδιοτιμή του T_n στην Δ είναι ο n-οστός συντελεστής a_n της Δ, δηλαδή ο $\tau(n)$. Το ζητούμενο τώρα έπεται από το πόρισμα 4.5.12. □

Σκοπός μας τώρα είναι να δείξουμε ότι οι τελεστές Hecke της $\Gamma(1)$ είναι Ερμιτιανοί στον $S_{2k}(\Gamma(1))$ ως προς το εσωτερικό γινόμενο του Petersson. Για να το κάνουμε αυτό, θα χρειαστεί να υιοθετήσουμε πρώτα έναν νέο συμβολισμό.

Έστω α ένας πίνακας στην $\mathrm{GL}_2(\mathbb{R})^+$, και f μια συνάρτηση ορισμένη στο $\mathbb{H}$. Ορίζουμε το

$$f|_k\alpha = (\det \alpha)^k (cz + d)^{-2k} f\left(\frac{az + b}{cz + d}\right).$$

Το κέντρο της $\mathrm{GL}_2(\mathbb{R}^+$ δρα τετριμμένα, δηλαδή για κάθε διαγώνιο α έχουμε $f|_k\alpha = f$. Μια f είναι weakly modular βάρους $2k$ για την $\Gamma < \Gamma(1)$ αν και

μόνο αν $f|_k\alpha = f$ για κάθε $\alpha \in \Gamma$. Ο τύπος που δίνει τον τελεστή Hecke T_n παίρνει τώρα την μορφή

$$T_n \cdot f = \sum n^{k-1} \cdot f|_k\alpha,$$

όπου οι α είναι από το κατάλληλο σύνολο αντιπροσώπων των τροχιών $\Gamma(1)\backslash M(n)$. Είναι προφανές ότι ο τύπος αυτός είναι ανεξάρτητος της επιλογής των αντιπροσώπων.

Λήμμα 4.5.14. *Για κάθε* $\alpha \in \mathrm{GL}_2(\mathbb{R})^+$,

$$\langle f|_k\alpha, g|_k\alpha\rangle = \langle f, g\rangle$$

Απόδειξη. Γράφουμε

$$\omega(f,g) = f(z)\overline{g(z)}y^{2k-2}dxdy.$$

Αν δείξουμε ότι

$$\omega(f|_k\alpha, g|_k\alpha) = \alpha^*\omega(f,g),$$

τότε θα έχουμε το ζητούμενο ως εξής:

$$\begin{aligned}\langle f|_k\alpha, g|_k\alpha\rangle &= \iint_D \omega(f|_k\alpha, g|_k\alpha)\\ &= \iint_D \alpha^*\omega(f,g)\\ &= \iint_{\alpha D} \omega(f,g) = \langle f, g\rangle.\end{aligned}$$

Επειδή ο πολλαπλασιασμός με βαθμωτό δεν αλλάζει τα $\omega(f|_k\alpha, g|_k\alpha)$ και $\alpha^*\omega(f,g)$, μπορούμε να υποθέσουμε ότι $det\alpha = 1$. Τότε

$$f|_k\alpha = (cz+d)^{-2k} f\left(\frac{az+b}{cz+d}\right)$$

και

$$\overline{g}|_k\alpha = (c\overline{z}+d)^{-2k}\overline{g\left(\frac{az+b}{cz+d}\right)},$$

κι άρα

$$\omega(f|_k\alpha, g|_k\alpha) = |cz+d|^{-4k} f(\alpha z)\overline{g(\alpha z)}dxdy.$$

Ξέρουμε όμως ότι

$$\Im(\alpha z) = \frac{\Im(z)}{|cz+d|^2},$$

$$\alpha^*(dxdy) = \frac{dxdy}{|cz+d|^4},$$

κι άρα

$$\begin{aligned}\alpha^*(\omega(f,g)) &= f(\alpha z)\cdot\overline{g(\alpha z)}\cdot|cz+d|^{4-4k}\cdot y^{2k-2}\cdot|cz+d|^{-4}\cdot dxdy\\ &= \omega(f|_k\alpha, g|_k\alpha),\end{aligned}$$

και έχουμε το ζητούμενο. □

Το λήμμα τώρα μας δίνει

$$\langle f|_k\alpha, g\rangle = \langle f, g|_k\alpha^{-1}\rangle$$

για κάθε $\alpha \in \mathrm{GL}_2(\mathbb{R})$.

Θεώρημα 4.5.15. *Αν f και $g \in S_{2k}(\Gamma(1))$, τότε*

$$\langle T_n \cdot f, g\rangle = \langle f, T_n \cdot g\rangle$$

για κάθε n.

Είναι απλό να δει κανείς ότι εξ' αιτίας του πορίσματος 4.5.4, αρκεί να δείξουμε το θεώρημα για τους T_p. Πρώτα θα χρειαστούμε το εξής λήμμα:

Λήμμα 4.5.16. *Υπάρχει κοινό σύνολο αντιπροσώπων για τις αριστερές τροχιές $\Gamma(1)\backslash M(p)$ και τις δεξιές τροχιές $M(p)/\Gamma(1)$.*

Απόδειξη. Έστω α και $\beta \in M(p)$. Τότε:

$$\Gamma(1)\cdot\alpha\cdot\Gamma(1) = \Gamma(1)\cdot\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}\cdot\Gamma(1) = \Gamma(1)\cdot\beta\cdot\Gamma(1).$$

Δηλαδή, υπάρχουν u, u', v, v' στην $\Gamma(1)$ τέτοια ώστε

$$u\alpha v = u'\beta v'.$$

Άρα $u'^{-1}u\alpha = \beta v' v^{-1} = \gamma$, οπότε $\Gamma(1)\cdot\alpha = \Gamma(1)\cdot\gamma$ και $\beta\cdot\Gamma(1) = \gamma\cdot\Gamma(1)$. □

Απόδειξη. (του θεωρήματος 4.5.15) Για ένα

$$\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M(p),$$

θέτουμε

$$\alpha' = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} = p\cdot\alpha^{-1} \in M(p).$$

Έστω α_i ένα κοινό σύνολο αντιπροσώπων για τους $\Gamma(1)\backslash M(p)$ και $M(p)/\Gamma(1)$, ούτως ώστε οι

$$M(p) = \bigcup_i \Gamma(1)\cdot\alpha_i = \bigcup_i \alpha_i\cdot\Gamma(1)$$

να είναι ξένες ενώσεις. Τότε

$$M(p) = p\cdot M(p)^{-1} = \bigcup_i p\cdot\Gamma(1)\cdot\alpha_i^{-1} = \bigcup_i \Gamma(1)\cdot\alpha_i'.$$

Άρα, παίρνουμε

$$\langle T_p\cdot f, g\rangle = p^{k-1}\sum_i \langle f|_k\alpha_i, g\rangle = p^{k-1}\sum_i \langle f, g|_k\alpha_i^{-1}\rangle = p^{k-1}\sum_i \langle f, g|_k\alpha_i'\rangle = \langle f, T_n\cdot g\rangle.$$

□

Χρησιμοιώντας το πόρισμα 4.2.4 και την πρόταση 4.3.7, για τις modular και τις cusp μορφές στην $\Gamma(1)$ συνάγουμε τους τύπους

$$\dim S_{2k} = \dim M_{2k} - 1$$

και

$$\dim M_{2k-12} = \dim M_{2k} - 1.$$

Αυτό μας δίνει την διάσπαση του M_{2k}:

$$M_{2k} = S_{2k} \oplus \langle G_{2k} \rangle = S_{2k} \oplus \langle E_{2k} \rangle$$

που σημειώσαμε και νωρίτερα στην απόδειξη της πρότασης 4.3.22, και το πόρισμα:

Πόρισμα 4.5.17. *Οι σειρές Eisenstein G_{2k}, $k \geq 2$ είναι ομοιόμορφες ιδιομορφές για τους T_n, με ιδιοτιμές $\sigma_{2k-1}(n)$. Η αντίστοιχη κανονικοποιημένη ιδιομορφή της G_{2k} είναι η $\gamma_k^{-1} E_{2k}$.*

Απόδειξη. Η G_{2k} είναι ορθογώνια στον S_{2k}, ο T_n Ερμιτιανός και διατηρεί τον S_{2k}. Έπεται πως και η $T_n \cdot G_{2k}$ είναι ορθογώνια στον S_{2k}, κι άρα πολλαπλάσιο του G_{2k}.

Από τον ορισμό της G_{2k} παίρνουμε

$$T_p \cdot G_{2k}(\Lambda) = \sum_{\Lambda'} \sum_{\lambda \in \Lambda', \lambda \neq 0} \frac{1}{\lambda^{2k}},$$

όπου το άθροισμα είναι πάνω απ' τα sublattices Λ' του Λ δείκτη p. Αν $\lambda \in p\Lambda$, τότε $\lambda \in \Lambda'$ για κάθε Λ', κι άρα συνεισφέρει $(p+1)/\lambda^{2k}$ στο άθροισμα. Αλλιώς, συνεισφέρει $1/\lambda^{2k}$. Άρα

$$T_p \cdot G_{2k})(\Lambda) = G_{2k}(\Lambda) + p \sum_{\lambda \in p\Lambda, \lambda \neq 0} \frac{1}{\lambda^{2k}} = (1 + p^{1-2k}) G_{2k}(\Lambda).$$

Άρα, η $G_{2k}(\Lambda)$, ως συνάρτηση στο L είναι ιδιομορφή του T_p με ιδιοτιμή $1 + p^{1-2k}$. Ως συνάρτηση στο $\mathbb{H}$ είναι ιδιομορφή με ιδιοτιμή $p^{2k-1}(1 + p^{1-2k}) = p^{2k-1} + 1 = \sigma_{2k-1}(p)$. Η γενική περίπτωση τώρα για τους T_n έπεται από την έκφραση του T_n ως πολυώνυμο στους T_p. Ο ισχυρισμός για την E_{2k} έπεται από τον τύπο της E_{2k} και την πρόταση 4.5.10. □

Η $\mathbb{Z}$-δομή στον $\mathbb{C}$-διανυσματικό χώρο V είναι ένα ελεύθερο $\mathbb{Z}$-πρότυπο διάστασης ίσης με του V.

Πρόταση 4.5.18. *Η $\mathbb{Z}$-δομή στον $\mathbb{C}$-διανυσματικό χώρο $M_{2k}(\Gamma(1))$ είναι το πρότυπο*

$$M_{2k}(\mathbb{Z}) = \{f \in M_{2k}(\Gamma(1)) : f = \sum_{n=0}^{\infty} a_n q^n, a_n \in \mathbb{Z}\}.$$

Απόδειξη. Αρκεί να δείξουμε ότι

$$M(\mathbb{Z}) = \bigoplus_k M_{2k}(\mathbb{Z}) = \mathbb{Z}[E_4, E_6].$$

Οι E_4, e_6 και Δ έχουν ακέραιους συντελεστές. Έστω ότι ο $M_{2\ell}(\mathbb{Z})$ ικανοποιεί το ζητούμενο για $\ell < k$, και εφαρμόζουμε επαγωγή. Έστω μια $f \in M_{2k}(\mathbb{Z})$. Η f γράφεται στην μορφή

$$f = a_0 E_4^a \cdot E_6^b + \Delta g,$$

με $2a + 3b = k$ και $g \in M_{2k-12}$. Τότε $a_0 \in \mathbb{Z}$ και $g \in M_{2k-12}(\mathbb{Z})$. □

Πρόταση 4.5.19. *Οι ιδιοτιμές των τελεστών Hecke είναι αλγεβρικοί ακέραιοι.*

Απόδειξη. Το $M_{2k}(\mathbb{Z})$ διατηρείται υπό την δράση του T_n:

$$T_n \cdot f(z) = \sum_{m=0}^{\infty} c_m q^m,$$

όπου δείξαμε ότι οι συντεκεστές δίνονται από τον τύπο

$$c_m = \sum_{b|(m,n), b\geq 1} b^{2k-1} \cdot a_{\frac{mn}{b^2}}.$$

Άρα, ο πίνακας του T_n ως προς μια βάση του $M_{2k}(\mathbb{Z})$ έχει ακέραιους συντελεστές, και αυτό δείχνει ότι οι ιδιοτιμές του T_n είναι αλγεβρικοί ακέραιοι. □

Η γενίκευση της πρότασης 4.5.19 για τις Siegel modular forms (παράγραφο 4.7 παρακάτω) αποδείχθηκε στην δεκαετία του ’80, από τους Chai και Faltings, με χρήση αλγεβρικής γεωμετρίας.

Ένα πρόβλημα για τους τελεστές Hecke είναι ο χαρακτηρισμός των ομοιόμορφων ιδιομορφών τους. Έχουμε δει τις πολλαπλασιαστικές ιδιότητες των συντελεστών Fourier των modular μορφών. Η επόμενη πρόταση δείχνει ότι η αυξημένη πολλαπλασιαστικότητα είναι ακριβώς η ιδιότητα που κάνει μια cusp form ομοιόμορφη ιδιομορφή.

Πρόταση 4.5.20. *Έστω f μια cusp form βάρους $2k \geq 12$. Η f είναι ομοιόμορφη κανονικοποιημένη ιδιομορφή αν και μόνο αν οι συντελεστές Fourier της f ικανοποιούν την ιδιότητα*

$$a_m a_n = \sum_{b|(m,n), b\geq 1} b^{2k-1} \cdot a_{\frac{mn}{b^2}}$$

για κάθε $m, n \geq 1$.

Απόδειξη. Ξέρουμε ότι η εξίσωση $T_n \cdot f = \lambda(n) f$ είναι, συγκρίνοντας συντελεστές, ακριβώς ισοδύναμη με την σχέση $c_m = \lambda(n) a_m$. Επίσης $c_1 = a_n$, άρα αν $a_1 = 1$ τότε $\lambda(n) = a_n$ και $c_m = a_n a_m$. Ο τύπος για την c_m δείχνει ότι, αν $a_1 = 1$, ο τύπος που ζητάμε να αποδείξουμε είναι ισοδύναμος με την σχέση

$$c_m = \lambda(n) a_m$$

και έχουμε την ισοδυναμία που θέλουμε. □

Πότε μια modular μορφή που δεν είναι cusp είναι ομοιόμορφη ιδιομορφή;

Πρόταση 4.5.21. *Μια $f \in M_{2k}(\Gamma(1))$, $k \geq 2$, που δεν είναι cusp, είναι κανονικοποιημένη ομοιόμορφη ιδιομορφή αν και μόνο αν*

$$f(z) = \frac{(2k-1)!}{2(2\pi \mathrm{i})^{2k}} G_{2k}(z).$$

Απόδειξη. Έχουμε, από την προηγούμενη πρόταση, την ισοδυναμία του ζητούμενου με την σχέση

$$c_m = \lambda(n)a_m.$$

Για $m = 0$:

$$c_0 = \lambda(n)a_0.$$

Όμως, $c_0 = \sigma_{2k-1}(n)a_0$. Αφού $a_0 \neq 0$, η $T_n \cdot f = \lambda(n)f$ είναι ισοδύναμη με την $\lambda(n) = \sigma_{2k-1}(n)$. Παίρνουμε την σχέση

$$c_m = \sigma_{2k-1}(n)a_m.$$

Θέτοντας $m = 1$, παίρνουμε

$$a_n = \sigma_{2k-1}(n)a_1.$$

Άρα, η f είναι κανονικοποιημένη ομοιόμορφη ιδιομορφή στον $M_{2k}(\Gamma(1))$ αν και μόνο αν

$$a_n = \sigma_{2k-1}(n)$$

για κάθε $n \geq 1$. Από το ανάπτυγμα Fourier της G_{2k} (θεώρημα 4.3.3), έχουμε τώρα το ζητούμενο. □

Εφαρμόζωντας το λήμμα 4.5.1 στους χώρους $M_{2k}(\Gamma(1))$, $S_{2k}(\Gamma(1))$ βλέπουμε πως η γνώση των ιδιομορφών τους μας δίνει βάσεις για αυτούς. Για παράδειγμα, έχουμε άμεσα το επόμενο

Θεώρημα 4.5.22 (Petersson)**.** *Το σύνολο των cusp κανονικοποιημένων ομοιόμορφων ιδιομορφών των T_n για την $\Gamma(1)$ αποτελεί βάση για τον $S_{2k}(\Gamma(1))$.*

Φυσικά, μερικές φορές μπορούμε να βρούμε βάσεις πολύ πιο εύκολα, όπως κάναμε για την Δ στον $S_{12}(\Gamma(1))$. Αφού

$$\dim S_{2k}(\Gamma(1)) = 1$$

για $k = 6, 8, 9, 10, 11, 13$, υπολογίζουμε τις βάσεις τους Δ, ΔG_4, ΔG_6, ΔG_8, ΔG_{10} και ΔG_{14}.

Μέχρι στιγμής δεν ασχοληθήκαμε με τελεστές Hecke σε άλλες ομάδες πέρα από την $\Gamma(1)$. Στην πραγματικότητα, δεν είναι δύσκολο να γράψει κάποιος τον τύπο τους για τις $\Gamma_0(N)$, αρκεί να τονίσουμε ότι η θεωρία αναπτύσσεται όμοια με την $\Gamma(1)$, εκτός από το ότι στο λήμμα 4.5.7, όπου φτιάχνουμε ένα σύνολο αντιπροσώπων για την ομάδα που μας ενδιαφέρει, χρειάζεται, για την $\Gamma_0(N)$, να συμπεριλάβουμε την συνθήκη $\text{μκδ}(a, N) = 1$. Αυτή η συνθήκη λαμβάνεται υπ' όψην και στους τύπους που ορίζουν την δράση του T_n στις modular μορφές της $\Gamma_0(N)$.

Τα θεωρήματα 4.5.8, 4.5.15, η σχέση $a_n\lambda(n) = a_1$ και ως εκ τούτου οι πολλαπλασιαστικές ιδιότητες των συντελεστών Fourier μεταφέρονται αντίστοιχα κι εδώ.

Οι divisor ομάδες καθώς και οι τελεστές Hecke που ορίσαμε μπορούν να γενικευθούν υπό την εξής έννοια · για κάθε σύνολο X, η ομάδα $\text{Div}(X)$ των divisors του X είναι η ελεύθερη αβελιανή ομάδα που παράγεται από τα στοιχεία του X:

$$\text{Div}(X) = \bigoplus_{x \in X} \mathbb{Z} \cdot x.$$

Ένα ομομορφισμός της $\text{Div}(X)$ λέγεται correspondence στο X. Θα γενικεύσουμε αυτήν την έννοια στις επόμενες παραγράφους.

4.6 Η θεωρία Atkin-Lehner

Θα παρουσιάσουμε τώρα τα εισαγωγικά στοιχεία μιας σημαντικής θεωρίας των modular μορφών, της θεωρίας Atkin-Lehner. Πιο συγκεκριμμένα, θα δούμε την απόδειξη ενός βασικού αποτελέσματος, του Κύριου Λήμματος.

Πρώτα θα αλλάξουμε λίγο τον συμβολισμό που εισαγάγαμε μετά την πρόταση 4.5.13: αν α είναι ένας πίνακας στην $\mathrm{GL}_2(\mathbb{R})^+$, και f μια συνάρτηση ορισμένη στο $\mathbb{H}$, ορίζουμε

$$f|_k\alpha = (\det\alpha)^{k-1}(cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right).$$

Η αλλαγή αυτή του συμβολισμού είναι χρήσιμη επειδή εδώ, στην περίπτωση της $\Gamma_0(N)$, υπάρχουν εν γένει και modular forms περιττού ύψους.

Μέχρι στιγμής, έχουμε δει την δομή των modular μορφών ενός δοσμένου σταθερού ύψους. Στην παράγραφο αυτήν θα συνδέσουμε μεταξύ τους διανυσματικούς χώρους μορφών για τις $\Gamma_1(N)$ διαφορετικού ύψους. Πιο συγκεκριμμένα, θα συνδέσουμε μορφές ύψους N με μορφές ύψους M, όπου $M|N$, κυρίως όπου $N = pM$, όπου p είναι ένας πρώτος διαιρέτης του N.

Ο πιο εύκολος τρόπος είναι να παρατηρήσει κανείς πως αν $M|N$, τότε $S_k(\Gamma_1(M)) \subset S_k(\Gamma_1(N))$. Ένας άλλος τρόπος να εμβαπτίσουμε την $S_k(\Gamma_1(M))$ στην $S_k(\Gamma_1(N))$ είναι συνθέτοντας με την πολλαπλασιασμό-επί-d απεικόνιση, όπου d είναι ένας διαιρέτης του M/N ως εξής: για κάθε τέτοιο d, ορίζουμε

$$\alpha_d = \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix},$$

έτσι ώστε $f|_k\alpha_d(z) = d^{k-1}f(dz)$ για $f : \mathbb{H} \to \mathbb{C}$. Τότε, η απεικόνιση $|_k\alpha$ απεικονίζει τον $S_k(\Gamma_1(M))$ στον $S_k(\Gamma_1(N))$, ανεβάζοντας έτσι το ύψος από M σε N. Οι παρατηρήσεις αυτές δείχνουν ότι είναι φυσιολογικό να διακρίνουμε το κομμάτι του $S_k(\Gamma_1(N))$ που προέρχεται από μικρότερα ύψη.

Ορισμός 4.6.1. *Για κάθε διαιρέτη d του N, ορίζουμε την απεικόνιση i_d:*

$$i_d : (S_k(\Gamma_1(N/d)))^2 \longrightarrow S_k(\Gamma_1(N)),$$

που ορίζεται μέσω του τύπου

$$i_d(f,g) = f + g|_k\alpha_d.$$

Ο υπόχωρος των oldforms στο ύψος N είναι ο χώρος

$$S_k(\Gamma_1(N))^{old} = \sum_{p|N} i_p((S_k(\Gamma_1(N/p)))^2),$$

όπου το άθροισμα είναι πάνω από τους πρώτους (ισοδύναμα, όλους) τους διαιρέτες του N, και ο υπόχωρος των newforms ύψους N είναι το ορθογώνιο συμπλήρωμα του $S_k(\Gamma_1(N))^{old}$ ως προς το εσωτερικό γινόμενο του Petersson, δηλαδή

$$S_k(\Gamma_1(N))^{new} = (S_k(\Gamma_1(N))^{old})^{\perp}.$$

Οι τελεστές Hecke σέβονται την διάσπαση του $S_k(\Gamma_1(N))$ σε oldforms και newforms.

Πρόταση 4.6.2. *Οι χώροι $S_k(\Gamma_1(N))^{old}$ και $S_k(\Gamma_1(N))^{new}$ διατηρούνται υπό την δράση των τελεστών T_n και R_n.*

Απόδειξη. (Σκιαγράφηση) Έστω $p|N$. Η απόδειξη χωρίζεται σε δύο μέρη. Κατ' αρχάς, έστω $T = R_d$ με μκδ$(d, N) = 1$ ή $T = T_q$, όπου q πρώτος με $q \neq p$. Αν θεωρήσουμε την απεικόνιση

$$\begin{pmatrix} T & 0 \\ 0 & T \end{pmatrix} : ((S_k(\Gamma_1(N/p)))^2) \to ((S_k(\Gamma_1(N/p)))^2),$$

τότε

$$i_p \circ \begin{pmatrix} T & 0 \\ 0 & T \end{pmatrix} = T \circ i_p$$

ως απεικονίσεις

$$((S_k(\Gamma_1(N/p)))^2) \to S_k(\Gamma_1(N)),$$

όπου παρατηρούμε ότι ο T στο αριστερό μέλος συμβολίζει διαφορετικό τελεστή από τον T στο δεξί μέλος. Κατα δεύτερον, θεωρώντας την απεικόνιση

$$\begin{pmatrix} T_p & p^{k-1} \\ -R_p & 0 \end{pmatrix} : ((S_k(\Gamma_1(N/p)))^2) \to ((S_k(\Gamma_1(N/p)))^2),$$

τότε και πάλι

$$i_p \circ \begin{pmatrix} T_p & p^{k-1} \\ -R_p & 0 \end{pmatrix} = T \circ i_p.$$

Οι σχέσεις αυτές δίνουν ότι ο $S_k(\Gamma_1(N))^{old}$ είναι διατηρείται από τους T_p και R_p, και άρα και από τους T_n και R_n. Για τον $S_k(\Gamma_1(N))^{new}$, αρκεί να δείξουμε ότι ο $S_k(\Gamma_1(N))^{old}$ διατηρείται και από τους συζυγείς τελεστές T_n^* και R_n^*. Αφού $T_n^* = R_n^{-1}T_n$ και $R_n^* = R_n^{-1}$ όταν μκδ$(n, N) = 1$, και $R_n^* = 0$ όταν μκδ$(n, N) > 1$, το αποτέλεσμα σε αυτές τις περιπτώσεις έπεται απ'π τα παραπάνω. Για την περίπτωση του T_n^* όταν μκδ$(n, N) > 1$, έχουμε

$$T_n^* == wT_nw^{-1},$$

όπου η γραμμμική απεικόνιση $w : S_k(\Gamma_1(N)) \to S_k(\Gamma_1(N))$ είναι η

$$w = |_k \begin{pmatrix} 0 & 1 \\ -N & 0 \end{pmatrix}.$$

Για να ολοκληρωθεί η απόδειξη, αρκεί να δείξουμε ότι οι oldforms διατηρούνται από την 1-1 γραμμική απεικόνιση w. Αυτό όμως έπεται από το γεγονός ότι

$$i_p \circ \begin{pmatrix} 0 & p^{k-2}w \\ w & 0 \end{pmatrix} = w \circ i_p.$$

(Για τις λεπτομέρειες των βημάτων που λείπουν παραπέμπουμε στο [Diamond-Shurman, [8], κεφ.5). □

Έπεται τώρα το

Πόρισμα 4.6.3. *Οι χώροι $S_k(\Gamma_1(N))^{old}$ και $S_k(\Gamma_1(N))^{new}$ έχουν ορθογώνιες βάσεις που αποτελούνται από ιδιομορφές των τελεστων Hecke T_n, όπου μκδ$(n, N) = 1$.*

Έστω $M|N$ και $d|(N/M)$, $d > 1$. Τότε $\Gamma_1(N) \subset \Gamma_1(M)$. Προηγουμένως, σημειώσαμε ότι υπάρχουν δύο απεικονίσεις $S_k(\Gamma_1(M)) \to S_k(\Gamma_1(N))$, ο προφανής συνολοθεωρητικός εγκλεισμός και ο βάρουσ-k τελεστής $|_k\alpha_d$. Ο τελεστής $|_k\alpha_d$ είναι, μέχρι βαθμωτού πολλαπλασιασμού, σύνθεση με την πολλαπλασιασμός -επί-d απεικόνιση. Για να απαλείψουμε το βαθμωτό γινόμενο, ορίζουμε την κανονικοποιημένη παραλλαγή της i_d:

$$\iota_d : S_k(\Gamma_1(M)) \longrightarrow S_k(\Gamma_1(N)),$$

$$\iota_d(f(z)) = (\iota_d f)(z) = f(dz).$$

της οποίας η δράση στο ανάπτυγμα Fourier της f δίνεται ως εξής:

$$\iota_d : \sum_{n=1}^{\infty} a_n q^n \longrightarrow \sum_{n=1}^{\infty} a_n q^{dn}.$$

Αυτό δείχνει ότι αν $f \in S_k(\Gamma_1(N))$, τότε η f παίρνει την μορφή

$$f = \sum_{p|N} \iota_p f_p$$

όπου η κάθε μία από τις $f_p \in S_k(\Gamma_1(N/p))$, και για το Fourier ανάπτυγμα της f έχουμε ότι $a_n = 0$ για κάθε n τέτοιο ώστε μκδ $(n, N) = 1$. Το κύριο λήμμα εγγυάται ότι και το αντίστροφο είναι αληθές.

Θεώρημα 4.6.4 (Κύριο Λήμμα, 1η μορφή)**.** *Έστω μια $f \in S_k(\Gamma_1(N))$ με ανάπτυγμα Fourier*

$$f(z) = \sum_{n=1}^{\infty} a_n q^n$$

με $a_n = 0$ όταν μκδ$(n, N) = 1$. Τότε, η f παίρνει την μορφή

$$f = \sum_{p|N} \iota_p f_p$$

όπου κάθε $f_p \in S_k(\Gamma_1(N/p))$.

Το Κύριο Λήμμα αποδείχθηκε το 1970, από τους Atkin και Lehner. Θα παρουσιάσουμε μια σύντομη απόδειξη του που οφείλεται στον Carlton (1999, 2001). Για να το αποδείξουμε, θα χρειαστούμε μια πρόταση (4.6.11 παρακάτω) που αφορά την θεωρία των αναπαραστάσεων ομάδων (μια απόδειξη της βρίσκεται στο [Diamond-Shurman, [8], κεφ.5]).

Σε πρώτο βήμα, για να απλοποιήσουμε λίγο το Κύριο Λήμμα, θεωρούμε τις ομάδες $\Gamma^1(N)$ αντί για τις $\Gamma_1(N)$, ούτως ώστε να μετατρέψουμε τις ι_p σε εγκλεισμούς.

Λήμμα 4.6.5. *Για τον N ισχύει*

$$\alpha_N \Gamma_1(N) \alpha_N^{-1} = \Gamma^1(N),$$

και ομοίως ισχύει για M στην θέση του N.

Έπεται πως οι απεικονίσεις

$$N^{k-1}|_k\alpha_N^{-1} : S_k(\Gamma_1(N)) \longrightarrow S_k(\Gamma^1(N)),$$

$$M^{k-1}|_k\alpha_M^{-1} : S_k(\Gamma_1(M)) \longrightarrow S_k(\Gamma^1(M))$$

είναι ισομορφισμοί. Όσον αφορά τους συντελεστές Fourier, η δράση αυτή μεταφράζεται σε

$$\sum_{n=1}^{\infty} a_n q^n \longrightarrow \sum_{n=1}^{\infty} a_n q_N^n,$$

όπου $q_N = q^{1/N}$, και αντιστοίχως για M στην θέση του N. Αφού $\Gamma_1(N) \subset \Gamma_1(M)$, έπεται πως $S_k(\Gamma_1(M)) \subset S_k(\Gamma_1(N))$. Για $N = dM$, έχουμε πως οι απεικονίσεις

$$\sum_{n=1}^{\infty} a_n q^n \longrightarrow \sum_{n=1}^{\infty} a_n q^{dn} \longrightarrow \sum_{n=1}^{\infty} a_n q_N^{dn}$$

και

$$\sum_{n=1}^{\infty} a_n q^n \longrightarrow \sum_{n=1}^{\infty} a_n q_N^n \longrightarrow \sum_{n=1}^{\infty} a_n q_N^{dn}$$

ταυτίζονται, και βέβαια το ίδιο ισχύει για M στην θέση του N. Παίρνουμε έτσι την δεύτερη διάτυπωση για το Κύριο Λήμμα:

Θεώρημα 4.6.6 (Κύριο Λήμμα, 2η μορφή)**.** *Έστω μια $f \in S_k(\Gamma^1(N))$ με ανάπτυγμα Fourier*

$$f(z) = \sum_{n=1}^{\infty} a_n q_N^n$$

με $a_n = 0$ όταν $\mu\kappa\delta(n, N) = 1$. Τότε, η f παίρνει την μορφή

$$f = \sum_{p|N} f_p$$

όπου κάθε $f_p \in S_k(\Gamma^1(N/p))$.

Το επόμενο βήμα είναι να μεταφράσουμε το Κύριο Λήμμα στην γλώσσα της γραμμικής άλγεβρας. Για να το κάνουμε αυτό, θα ορίσουμε έναν κατάλληλο προβολικό τελεστή π.

Για κάθε $d|N$, ορίζουμε την ομάδα

$$\Gamma_d = \Gamma_1(N) \cap \Gamma^0(N/d).$$

Λήμμα 4.6.7. *Ένα σύνολο αντιπροσώπων για το πηλίκο $\Gamma(N)\backslash\Gamma_d$ είναι το*

$$\left\{ \begin{pmatrix} 1 & bN/d \\ 0 & 1 \end{pmatrix} : 0 \le b < d \right\}.$$

Ορίζουμε τον τελεστή $\pi_d : S_k(\Gamma(N)) \to S_k(\Gamma(N))$:

$$\pi_d(f) = \frac{1}{d} \sum_{b=0}^{d-1} f|_k \begin{pmatrix} 1 & bN/d \\ 0 & 1 \end{pmatrix}$$

(δηλαδή παίρνουμε τον μέσο όρο των $f|_k\alpha$). Ο τελεστής αυτός είναι προβολή στον $S_k(\Gamma_d)$ (δηλαδή $\pi_d^2 = \pi_d$). Όσον αφορά τα αναπτύγματα Fourier, ο π_d διατηρεί μόνο τους συντελεστές που που οι δείκτες τους διαιρούνται από το d:

$$\pi_d\left(\sum_{n=1}^{\infty} a_n q_N^n\right) = \sum_{n:d|n} a_n q_N^n.$$

Σαν άμεση παρατήρηση έχουμε πως $\pi_{d_1 d_2} = \pi_{d_1}\pi_{d_2} = \pi_{d_2}\pi_{d_1}$ για $d_1 d_2 | N$.

Ορισμός 4.6.8. *Ο προβολικός τελεστής* $\pi : S_k(\Gamma(N) \to S_k(\Gamma(N)$ *είναι ο*

$$\pi = \prod_{p|N}(1 - \pi_p),$$

όπου το γινόμενο τελεστών εννοεί την σύνθεση τελεστών.

Αναπτύσσοντας το γινόμενο του π και χρησιμοποιώντας την αρχή εγκλεισμού-αποκλεισμού παίρνουμε πως η π διατηρεί το ανάπτυγμα της f που είναι ξένο ως προς το N, δηλαδή

$$\pi\left(\sum_{n=1}^{\infty} a_n q_N^n\right) = \sum_{n:(n,N)=1} a_n q_N^n.$$

Άρα, η υπόθεση του Κύριου Λήμματος μεταφράζεται ως $f \in S_k(\Gamma^1(N)) \cap \ker(\pi)$. Οι π_p αντιμετατίθονται, οπότε με χρήση γραμμικής άλγεβρας συνάγουμε την σχέση

$$\ker(\pi) = \ker\left(\prod_{p|N}(1 - \pi_p)\right) = \sum_{p|N}\ker(1 - \pi_p) = \sum_{p|N}\mathrm{im}(\pi_p).$$

Όμως ο π_p είναι η προβολή του $S_k(\Gamma(N))$ στον $S_k(\Gamma_p)$, δηλαδή $\mathrm{im}(\pi_p) = S_k(\Gamma_p) = S_k(\Gamma_1(N) \cap \Gamma^0(N/p))$. Καταλήγοντας:

$$\ker(\pi) = \sum_{p|N} S_k(\Gamma_1(N) \cap \Gamma^0(N/p)).$$

Θεώρημα 4.6.9 (Κύριο Λήμμα, 3η μορφή)**.**

$$S_k(\Gamma^1(N)) \cap \sum_{p|N} S_k(\Gamma_1(N) \cap \Gamma^0(N/p)) = \sum_{p|N} S_k(\Gamma^1(N/p)).$$

Αυτή η μορφή του Κύριου Λήμματος ανάγεται στην θεωρία ομάδων, και είναι αυτή η μορφή της οποίας την απόδειξη θα δώσουμε. Η ομάδα $G = \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ δρα στον $S_k(\Gamma(N))$ από τα αριστερά με τον βάρους$-k$ τελεστή. Αν $N = p_1^{e_1} \cdot \ldots \cdot p_n^{e_n}$ είναι η ανάλυση του N σε πρώτους, τότε η G είναι προφανώς ισόμορφη με την

$$G = \prod_{i=1}^{n} G_i = \prod_{i=1}^{n} \mathrm{SL}_2(\mathbb{Z}/p_i^{e_i}\mathbb{Z}).$$

Για $i = 1, 2, \ldots, n$, ορίζουμε τις υποομάδες H_i, K_i των G_i ως εξής:

$$H_i = \Gamma^1(p_i^{e_i})/\Gamma(p_i^{e_i}),$$

$$K_i = (\Gamma_1(p_i^{e_i}) \cap \Gamma^0(p_1^{e_i-1}))/\Gamma(p_i^{e_i}).$$

Λήμμα 4.6.10. *Για κάθε πρώτο p και $e \geq 1$,*

$$\langle \Gamma^1(p^e), \Gamma_1(p^e) \cap \Gamma^0(p^{e-1} \rangle = \Gamma^1(p^{e-1}).$$

Θα δούμε την απόδειξη του λήμματος 4.6.10 παρακάτω. Προς το παρόν, ας δούμε πως με χρήση του λήμματος 4.6.10 έπεται η απόδειξη του Κύριου Λήμματος. Έστω H η ομάδα

$$H = \prod_{i=1}^{n} H_i.$$

Επιλέγοντας να συμβολίσουμε με X^G τον διανυσματικό χώρο X που σταθεροποιείται από την ομάδα G, βλέπουμε ότι το λήμμα 4.6.10 μεταφράζει την διατύπωση του θεωρήματος 4.6.9 στην εξής μορφή:

$$S_k(\Gamma(N))^H \cap \sum_{i=1}^{n} S_k(\Gamma(N))^{K_i} = \sum_{i=1}^{n} S_k(\Gamma(N))^{\langle H, K_i \rangle}.$$

Ο διανυσματικός χώρος $S_k(\Gamma(N))$ είναι ευθύ άθροισμα υποχώρων του που είναι $G-$αναλλοίωτοι. Άρα, η παραπάνω εξίσωση έπεται από την εξής πρόταση της θεωρίας αναπαραστάσεων:

Πρόταση 4.6.11. *Έστω V μια ανάγωγη αναπαράσταση της ομάδας*

$$G = \prod_{i=1}^{n} G_i,$$

και

$$H = \prod_{i=1}^{n} H_i, K = \prod_{i=1}^{n} K_i,$$

δύο υποομάδες της. Τότε

$$V^H \cap \sum_{i=1}^{n} V^{K_i} = \sum_{i=1}^{n} V^{\langle H, K_i \rangle}.$$

Μετά την παραπάνω συζήτηση, βλέπουμε τώρα πως η απόδειξη του Κύριου Λήμματος θα έχει ολοκληρωθεί αν δείξουμε το λήμμα 4.6.10.

Απόδειξη. (του λήμματος 4.6.10) Πρέπει να δείξουμε ότι

$$\langle \Gamma^1(p^e), \Gamma_1(p^e) \cap \Gamma^0(p^{e-1} \rangle = \Gamma^1(p^{e-1}).$$

Ο εγκλεισμός " $\subset$ " είναι άμεσος, οπότε αρκεί να δείξουμε τον εγκλεισμό " $\supset$ ". Έστω Γ η ομάδα $\langle \Gamma^1(p^e), \Gamma_1(p^e) \cap \Gamma^0(p^{e-1} \rangle$, και ένα

$$\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma^1(p^{e-1}).$$

Θα δείξουμε ότι υπάρχει στοιχείο $\gamma\alpha\gamma'$ της $\Gamma\alpha\Gamma$ που ανήκει στην Γ, οπότε θα έχουμε το ζητούμενο.

Έστω κατ' αρχάς πως $p|a$ ή $p|d$. Τότε $e = 1$. Αν $p|a$ τότε $p \nmid b$, κι άρα το στοιχείο

$$\alpha \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} a+b & b \\ c+d & d \end{pmatrix}$$

ικανοποιεί ότι $p \nmid a+b$. Αφού

$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in \Gamma,$$

μπορούμε να υποθέσουμε ότι $p \nmid a$. Ομοίως αντιμετωπίζεται η περίπτωση $p|d$.

Έστω $\beta = -bd^{-1} \mod p^e$. Τότε, έχουμε τις προφανείς ισοδυναμίες

$$b + d\beta \equiv 0 \mod p^e, \beta \equiv 0 \mod p^{e-1}.$$

Τότε:

$$\begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} \in \Gamma$$

και

$$\begin{pmatrix} 1 & \beta \\ 0 & 1 \end{pmatrix} \alpha = \begin{pmatrix} a + c\beta & b + d\beta \\ c & d \end{pmatrix},$$

οπότε, μπορούμε να υποθέσουμε πως $b \equiv 0 \mod p^e$. Και πάλι το επιχείρημα για την αναγωγή στην περίπτωση $c \equiv 0 \mod p^e$ είναι παρόμοιο.

Έχουμε λοιπόν αναχθεί στην περίπτωση που

$$\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

με $a \equiv d \equiv 1 \mod p^{e-1}$ και $b \equiv c \equiv 0 \mod p^e$. Αφού $\det \alpha = 1$, έχουμε $ad \equiv 1 \mod p^e$. Θεωρούμε τον πίνακα

$$\gamma = \begin{pmatrix} 1 & 1-a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1-d \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}$$

$$= \begin{pmatrix} a + a(1-ad) & 1-ad \\ ad-1 & d \end{pmatrix}.$$

Έχουμε $\gamma \in \Gamma$ και $\gamma \equiv \alpha \mod p^e$, άρα

$$\alpha\gamma^{-1} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \mod p^e,$$

ενώ επίσης $\alpha\gamma^{-1} \in \Gamma$. Άρα $\alpha \in \Gamma$, και η απόδειξη του λήμματος είναι πλήρης. □

Στο σημείο αυτό, ας συνοψίσουμε σε γενικές γραμμές την θεωρία που έχουμε δει μέχρι στιγμής. Κατ' αρχάς, ορίσαμε τις modular μορφές σε μια modular καμπύλη, και μελετήσαμε κάποια βασικά παραδείγματα εξ' αυτών. Είδαμε τους διανυσματικούς χώρους που αυτές σχηματίζουν, μετρήσαμε την διάσταση τους και για κάποιους απ' αυτούς τους χώρους μπορέσαμε να γράψουμε μια συγκεκριμμένη βάση τους. Μελετήσαμε τους σημαντικότερους (και πιο φυσιολογικούς) τελεστές που δρουν σε αυτούς τους διανυσματικούς χώρους, ενώ, στην τελευταία παράγραφο, είδαμε πως μπορούμε να μεταβούμε από στοιχεία ενός χώρου σε στοιχεία ενός άλλου. Η απόδειξη του Mordell για τις εικασίες του Ramanujan, έδειξε έναν αριθμοθεωρητικό λόγο που μελετάμε τις modular μορφές. Με φυσιολογικό τρόπο τίθονται τώρα τρία ερωτήματα:

(i) Ποια άλλα παραδείγματα εφαρμογών των modular μορφών σε κλασσικά προβλήματα της θεωρίας αριθμών υπάρχουν.

(ii) Με ποιούς τρόπους γενικεύονται οι συναρτήσεις αυτές.

(iii) Ποια είναι η βαθύτερη σχέση που συνδέει τις modular μορφές με τις ελλειπτικές καμπύλες.

Όσον αφορά το πρώτο ερώτημα, στην επόμενη παράγραφο περιγράφουμε εν συντομία δύο (από τις πολλές που υπάρχουν) εφαρμογές των modular μορφών σε κλασσικά προβλήματα της θεωρίας αριθμών.

Στην παράγραφο 4.8 γίνεται μια σύνοψη των σημαντικοτέρων γενικεύσεων που επιδέχονται οι modular μορφές.

Το αντικείμενο των παραγράφων 4.9-4.13, το οποίο είναι τα βασικά στοιχεία της θεωρίας Eichler-Shimura, και το κεφάλαιο 5, στο οποίο αναπτύσσεται η βασική θεωρία των L-συναρτήσεων και περιγράφεται το Modularity θεώρημα, αποτελούν μια μερική απάντηση στο τρίτο ερώτημα.

4.7 Εφαρμογές των modular μορφών

Θα περιγράψουμε δύο εφαρμογές των modular μορφών σε δύο κλασσικά προβλήματα της θεωρίας αριθμών. Το πρώτο είναι το πρόβλημα των τεσσάρων τετραγώνων, και το δεύτερο είναι το πρόβλημα των διαμερίσεων. Τα προβλήματα αυτά δικαιολογούν την παρατήρηση που κάναμε πριν, λέγοντας πως το ενδιαφέρον των modular μορφών για την θεωρία αριθμών πηγάζει εν μέρει από το γεγονός ότι μπορεί σαν συντελεστές Fourier τους να εμφανίζονται σημαντικές αριθμητικές συναρτήσεις.

4.7α΄ Το πρόβλημα των τεσσάρων τετραγώνων

Το 1770 ο Lagrange απέδειξε ότι κάθε φυσικός μπορεί να γραφτεί σαν άθροισμα τεσσάρων τετραγώνων. Τον 19ο αιώνα ο Jacobi γενίκευσε το θεώρημα του βρίσκοντας έναν τύπο για το πλήθος των διαφορετικών τρόπων με τους οποίους μπορεί να γραφτεί ένας φυσικός ως άθροισμα τεσσάρων τετραγώνων. Θα σκιαφραφήσουμε μια απόδειξη του τύπου αυτού με χρήση των mofular μορφών. Μια διαφορετική απόδειξη του μπορεί να βρει κανείς στο [Ireland-Rosen, [14], κεφ. 17].

Για κάθε ζεύγος φυσικών n και k, ορίζουμε το αριθμό αναπαράστασης $r(n,k)$ ως εξής:

$$r(n,k) = |\{u = (u_1, ..., u_k) \in \mathbb{Z}^k : n = u_1^2 + ... + u_k^2\}|.$$

Παρατηρούμε ότι αν $i + j = k$, τότε

$$r(n,k) = \sum_{\ell+m=n, \ell, m \geq 0} r(\ell, i) r(m, j).$$

Ο τύπος αυτός μοιάζει σαν τον τύπο για τους συντελεστές του γινομένου δύο δυναμοσειρών. Άρα, θεωρώντας την γεννήτρια συνάρτηση

$$\theta(\tau, k) = \sum_{n=0}^{\infty} r(n,k) q^n, q = e^{2\pi i \tau}, \tau \in \mathbb{H},$$

μπορεί να κανείς να συνάγει τους τύπους

$$\theta(\tau, k_1)\theta(\tau, k_2) = \theta(\tau, k_1 + k_2).$$

και

$$\theta(\tau + 1, k) = \theta(\tau, k).$$

Άρα, θέτοντας $\theta(\tau,1)=\theta(\tau)$, ορίζουμε μια περιοδική συνάρτηση. Η θ ικανοποιεί τους μετασχηματισμούς

$$\theta\left(-\frac{1}{4\tau}\right)=\sqrt{-2\mathrm{i}\tau}\theta(\tau),$$

$$\theta\left(\frac{\tau}{4\tau+1}\right)=\sqrt{4\tau+1}\theta(\tau)$$

και

$$\theta(\tau,4)=\theta(\tau)^4,$$

οι οποίοι συνεπάγονται τον τύπο

$$\theta\left(\frac{\tau}{4\tau+1},4\right)=(4\tau+1)^2\theta(\tau,4).$$

Άρα παίρνουμε

$$\theta(\gamma(\tau),4)=(cz+d)^2\theta(\tau,4)$$

για

$$\gamma=\pm\begin{pmatrix}1&1\\0&1\end{pmatrix}$$

και

$$\gamma=\pm\begin{pmatrix}1&0\\4&1\end{pmatrix}.$$

Η ομάδα που αντιστοιχεί στο πρόβλημα των τεσσάρων τετραγώνων είναι η ομάδα $\Gamma_\theta=\Gamma_0(4)$. Για την σειρά Eisenstein $G_2(\tau)$, χρησιμοποιούμε τον τύπο

$$G_2(\tau)=2\zeta(2)-8\pi^2\sum_{n=1}^{\infty}\sigma(n)q^n,$$

όπου $q=e^{2\pi\mathrm{i}\tau}$ και

$$\sigma(n)=\sum_{d|n,d>0}d.$$

Ορίζοντας

$$G_{2,N}(\tau)=G_2(\tau)-NG_2(N\tau),$$

τότε $G_{2,N}\in M_2(\Gamma_0(N))$. Συνάγουμε τους τύπους

$$G_{2,2}(\tau)=-\frac{\pi^3}{3}\left(1+24\sum_{n=1}^{\infty}(\sum_{d|n,d>0,dodd}d)q^n\right)$$

και

$$G_{2,4}(\tau)=-\pi^2\left(1+8\sum_{n=1}^{\infty}(\sum_{d|n,d>0}d)q^n\right),$$

όπου το άθροισμα στην $G_{2,4}$ εκτείνεται πάνω από τα d που δεν διαιρούνται από 4. Χρησιμοποιώντας το γεγονός ότι $G_{2,2}\in M_2(\Gamma_0(2))\subset M_2(\Gamma_0(4))$, $G_{2,4}\in M_2(\Gamma_0(4))$, οι $G_{2,2}$, $G_{2,4}$ είναι γραμμικά ανεξάρτητες και $\dim M_2(\Gamma_0(4))=2$, εξάγουμε μια σχέση

$$\theta(\cdot,4)=aG_{2,2}+bG_{2,4}$$

για κάποιους μιγαδικούς a και b. Χρησιμοποιώντας ότι $\theta(\tau,4) = 1+8q+...$ υπολογίζουμε $a=0$ και $b=-1/(\pi)^2$, οπότε παίρνουμε τον τύπο

$$r(n,4) = 8\sum_{d|n, d>0} d$$

για κάθε $n \geq 1$, όπου το άθροισμα εκτείνεται πάνω από τα d που δεν διαιρούνται από το 4. Ιδιαίτερα, αν το 4 δεν διαιρεί το n, τότε $r(n,4) = 8\sigma_1(n)$.

Η ίδια τεχνική μπορεί να εφαρμοστεί και για το πρόβλημα των δύο, έξι και οκτώ τετραγώνων. Για άρτιους $s \geq 10$ η μέθοδος αυτή δίνει μια ασυμπτωτική λύση.

Για τις λεπτομέρειες των αποδείξεων των παραπάνω αποτελεσμάτων, παραπέμπουμε στους [Diamond-Shurman, [8], κεφ.1].

4.7β′ Το πρόβλημα των διαμερίσεων

Η αριθμητική συνάρτηση $p(n)$ μετρά το πλήθος των διαμερίσεων του n, δηλαδή των πλήθος των τρόπων με τους οποίους μπορεί να γραφετί ο n ως άθροισμα θετικών ακεραίων $\leq n$. Σκοπός μας είναι να περιγράψουμε με ποιον τρόπο μπορεί να συναχθεί η σειρά Rademacher για την συνάρτηση $p(n)$.

Ο Euler έδειξε ότι για την $p(n)$ ισχύει το απειρογινόμενο:

$$F(x) = \sum_{n=0}^{\infty} p(n)x^n = \prod_{m=1}^{\infty} \frac{1}{1-x^m},$$

όπου θεωρούμε πως $p(0)=1$. Η σειρά και το γινόμενο συγκλίνουν στον δίσκο $|x|<1$. Οι Hardy και Ramanujan έδειξαν πως

$$p(n) \sim \frac{e^{K\sqrt{n}}}{4\sqrt{3}n}$$

καθώς το $n \to \infty$, όπου $K = \pi\sqrt{2/3}$. Επίσης, έδειξαν ότι

$$p(n) = \sum_{k<a\sqrt{n}} P_k(n) + O(n^{-1/4}),$$

όπου a σταθερά και το $P_1(n)$ κυριαρχεί στην σειρά, με τάξη $e^{K\sqrt{n}}/(4\sqrt{3}n)$. Το 1937 ο Lehmer έδειξε την σύγκλιση της σειράς

$$\sum_{k=1}^{\infty} P_k(n).$$

Το 1937 ο Rademacher κατάφερε να βρει έναν ακριβή τύπο για την $p(n)$. Η απόδειξη του χρησιμοποιεί την κυκλική μέθοδο των Hardy, Ramanujan και Littlewood, καθώς και την συνάρτηση $\eta(z)$.

Το σημείο εκκίνησης είναι ο τύπος του Euler, ο οποίος δίνει

$$\frac{F(x)}{x^{n+1}} = \sum_{k=0}^{\infty} \frac{p(k)x^k}{x^{n+1}},$$

για $|x|<1$ και για ≥ 0. Το Laurent αυτό ανάπτυγμα δείχνει ότι η $F(x)/x^{n+1}$ έχει πόλο στο $x=0$, με υπόλοιπο $p(n)$, άρα, από το θεώρημα του Cauchy συνάγουμε τον τύπο

$$p(n) = \frac{1}{2\pi \mathrm{i}} \int_C \frac{F(x)}{x^{n+1}} dx,$$

όπου το C είναι μια θετικά προσανατολισμένη απλή κλειστή καμπύλη που είναι μέσα στον μοναδιαίο δίσκο και περιλαμβάνει το 0. Η ιδέα της κυκλικής μεθόδου έγκειται στο να διαλέξουμε μια καμπύλη η οποία να είναι «κοντά» στις singularities της $F(x)$.

Κάθε ρίζα της μονάδας είναι singularity για την $F(x)$. Η κυκλική μέθοδος διαλέγει μια κυκλική καμπύλη με ακτίνα κοντά στο 1, και την κόβει σε τόξα $C_{h,k}$ κοντά στις ρίζες της μονάδας $e^{2\pi ih/k}$, όπου $0 \leq h < k$, μκδ$(h,k) = 1$ και $k = 1, 2, ..., N$. Το ολοκλήρωμα πάνω στην C γράφεται ως πεπερασμένο άθροισμα

$$\int_C = \sum_{k=1}^{N} \sum_{h=0,(h,k)=1}^{k-1} \int_{C_{H,K}}$$

και αντικαθιστώντας την $F(x)$ τοπικά από συναρτήσεις $\psi_{h,k}(x)$ οι οποίες έχουν την ίδια συμπεριφορά με την $F(x)$ στις singularities, εμφανίζεται ένα σφάλμα το οποίο υπολογίζεται. Οι $\psi_{h,k}(x)$ είναι συναρτήσεις που εμφανίζονται φυσιολογικά από την συναρτησιακή εξίσωση της η, για την οποία ισχύει ότι συνδέεται με την $F(x)$ από τον τύπο

$$F(e^{2\pi i\tau}) = \frac{e^{\frac{\pi i\tau}{12}}}{\eta(\tau)}.$$

Η συναρτησιακή εξίσωση της η δίνει έναν τύπο που περιγράφει την συμπεριφορά της F κοντά στις singularities, και άρα και το σφάλμα. Το 1943, ο Rademacher απλοποίησε την απόδειξη του. Κάνοντας την αλλαγή μεταβλητής $x = e^{2\pi i\tau}$ (μετακινούμενος δηλαδή στο άνω μιγαδικό ημιεπίπεδο $\mathbb{H}$) και ολοκληρώνοντας κατά μήκος ενός καινούριου μονοπατιού, το οποίο περιλελάμβανε κομμάτια από τους κύκλους Ford, απλοποίησε τα σφάλματα που εμφανίζονταν. Ο εντυπωσιακός τελικός τύπος του Rademacher παρατίθεται εδώ απλά για λόγους πληρότητας:

$$p(n) = \frac{1}{\pi\sqrt{2}} \sum_{k=1}^{\infty} A_k(n)\sqrt{k} \frac{d}{dn} \left(\frac{sinh\{\frac{\pi}{k}\sqrt{\frac{2}{3}\left(n - \frac{1}{24}\right)}\}}{\sqrt{n - \frac{1}{24}}} \right),$$

όπου οι $A_k(n)$ δίνονται από τον τύπο

$$A_k(n) = \sum_{0 \leq h < k,(h,k)=1} e^{\pi is(h,k)} - e^{2\pi inh/k}.$$

Για μια λεπτομερή απόδειξη παραθέτουμε στον [Apostol, [2], κεφ.5].

4.8 Γενικεύσεις

Παραθέτουμε εν συντομία κάποιες γενικεύσεις των modular forms.

4.8α′ Siegel modular forms

Οι Siegel modular forms είναι μορφές που συνδέονται με μεγαλύτερες συμπλεκτικές ομάδες, με την έννοια που οι modular forms που ορίσαμε συνδέονται με την $\mathrm{SL}_2(\mathbb{R})$. Με άλλα λόγια, είναι μορφές που συνδέονται με αβελιανές varieties, με την ίδια έννοια που οι modular μορφές που ορίσαμε συνδέονται με τις ελλειπτικές καμπύλες. Αυτός είναι και ο λόγος που modular μορφές αυτές ονομάζονται και ελλειπτικές modular μορφές.

4.8β′ Hilbert modular forms

Οι Hilbert modular forms είναι συναρτήσεις n μιγαδικών μεταβλητών, που ικανοποιούν μια modular σχέση για 2×2 πίνακες.

Πιο συγκεκριμμένα, έστω $K \subset \mathbb{R}$ ένα πραγματικό σώμα αριθμών βαθμού n πάνω από το $\mathbb{Q}$. Έστω $z = (z_1, ..., z_n) \in \mathbb{H}^n$, και

$$\left(\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}, ..., \begin{pmatrix} a_n & b_n \\ c_n & d_n \end{pmatrix} \right) \in SL_2(\mathbb{R})^n,$$

το οποίο μπορούμε να συμβολίσουμε και ως

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

με $a = (a_1, ..., a_n)$, κλπ. Ο $\mathrm{SL}_2(\mathbb{R})^n$ δρα στο $\mathbb{H}^n$ με την δράση:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : z \longrightarrow \frac{az+b}{cz+d}.$$

Εμφυτεύουμε με τον φυσιολογικό τρόπο (δηλαδή, μέσω των n εμφυτεύσεων του K στο $\mathbb{R}$) την $\mathrm{SL}_2(K)$ στην $\mathrm{SL}_2(\mathbb{R})^n$. Με παρόμοιο τρόπο ορίζεται μια modular ομάδα Γ. Το πρόβλημα της συμπαγοποίησης του $\Gamma\backslash\mathbb{H}^n$ και των χώρων πηλίκων που εμφανίζονται οδηγεί στην Baily-Borel συμπαγοποίηση, και οι χώροι πηλίκα που εμφανίζονται είναι singular αβελιανές varieties.

Έστω k ένα άρτιος φυσικός. Μια Hlibert modular form βάρους k είναι μια ολόμορφη συνάρτηση στο $\mathbb{H}^n$ που ικανοποιεί την αλγεβρική σχέση

$$f(z) = N(cz+d)^{-k} f(\gamma z), \gamma \in \Gamma,$$

όπου

$$N(cz+d)^{-k} = \prod_{i=1}^{n} (c_i z_i + d_i)^{-k}.$$

Ένα από τα πιο σημαντικά αποτελέσματα της αντίστοιχης θεωρίας είναι το αποτέλεσμα των Doi και Naganuma, το οποίο, δοσμένης μιας modular μορφής f για την $\mathrm{SL}_2(\mathbb{Z})$, εγγυάται την ύπαρξη μιας Hilbert modular μορφής της οποίας η L-συνάρτηση περιγράφεται από την modular μορφή της f (κεφ.5, παρακάτω).

Για τις λεπτομέρειες των παραπάνω, καθώς και για μια εκτενέστερη συζήτηση πάνω στις Hilbert modular forms, δείτε τον [Bump, [5],κεφ.1].

4.8γ′ Θήτα συναρτήσεις

Οι Θήτα συναρτήσεις είναι ειδικές περιοδικές συναρτήσεις που σχετίζονται με τις modular μορφές και τις τετραγωνικές μορφές. Στην προηγούμενη παράγραφο είδαμε ένα παράδειγμα μιας Θήτα συνάρτησης. Μια εκτενής ανάλυση τους περιέχεται στον [Serre, [27], κεφ.7], καθώς και στο κεφάλαιο "Classical Automorphic Forms" του Kowalski στο [Bump, et al., [6], κεφ.3].

4.8δ′ Automorphic forms

Στο άνω μιγαδικό ημιεπίπεδο, το οποίο θεωρούμε εφοδιασμένο με την υπερβολική μετρική

$$ds^2 = \frac{dx^2 + dy^2}{y^2},$$

ορίζεται η υπερβολική Laplacian

$$\Delta = -y^2 \left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2} \right).$$

Μια Maass form είναι μια συνάρτηση στο $\mathbb{H}$, η οποία είναι ιδιομορφή της Laplacian, είναι $\mathrm{SL}_2(\mathbb{R})$-αναλλοίωτη και έχει πολυωνυμικής τάξης συμπεριφορά στα cusps. Οι modular forms και οι Maass forms είναι παραδείγματα των automorphic μορφών.

Ο τελεστής Δ έχει πολλές σημαντικές ιδιότητες. Για παράδειγμα, είναι συμμετρικός, θετικός ως προς την υπερβολική μετρική $y^{-2}dxdy$ (δηλαδή $\langle \Delta f, f \rangle \geq 0$), και, το σημαντικότερο, μετατίθεται με τους τελεστές Hecke T_n. Ένα από τα πιο σημαντικά ερωτήματα σχετικά με τον τελεστή Δ είναι η μελέτη του φάσματος του, και συνδέεται με τον διάσημο τύπο του ίχνους του Selberg.

Η θεωρία των automorphic forms (ειδικότερα, η φασματική θεωρία τους) αναπτύχθηκε και μελετήθηκε κυρίως από τους Maass και Selberg. Η σύνδεση τους με την θεωρία αναπαραστάσεων αναπτύχθηκε από τους Gelfand και Fomin. Σήμερα, η θεωρία των automorphic representations είναι από τους πιο ενεργούς ερευνητικούς κλάδους, και συνδέεται με το Πρόγραμμα Langlands.

Σαν πόρισμα της θεωρίας των automorphic representations προκύπτει ότι υπάρχουν ακριβώς τρία είδη automorphic μορφών στο $\Gamma\backslash\mathbb{H}$:

(i) Οι ολόμορφες, δηλαδή οι modular μορφές, $f(\gamma z) = \chi(\gamma)(cz+d)^k f(z)$, όπου ο $\chi : \Gamma \to \mathbb{C}^\times$ είναι ένας χαρακτήρας (ένας ορισμός λίγο γενικότερος απ' αυτόν που έχουμε δώσει).

(ii) Οι ιδιομορφές της Laplacian, δηλαδή οι Maass μορφές.

(iii) Η σταθερή $f(z) = 1$.

Η έννοια της automorphic form γενικεύεται για ομάδες Lie. Μια πλήρης μελέτη των automorphic forms και της representation θεωρίας τους υπάρχει στον [Bump, [5]]. Μια σύντομη έκθεση της φασματικής θεωρίας για την Δ υπάρχει στο [Bump, et al., [6], κεφ.8].

Τέλος, ένα από τα πολλά θέματα της πλούσιας θεωρίας των modular μορφών που δεν έχουμε μελετήσει ακόμα (παρότι την έχουμε θίξει) είναι η βαθύτερη σχέση της αλγεβρικής γεωμετρίας με τις modular μορφές. Για παράδειγμα, έχουμε το παρακάτω θεώρημα:

Θεώρημα 4.8.1. *Υπάρχει μια αμφιμονοσήμαντη αντιστοιχία ανάμεσα στις cusp forms ύψους* 2 *για την* $\Gamma_0(N)$ *και τις ολόμορφες* 1*-μορφές της επιφάνειας Riemann* $X_0(N)$.

Μια απόδειξη του θεωρήματος μπορεί να βρεθεί στους [Diamond-Shurman, [8], κεφ.3] και στον [Κοντογεώργης, [41], κεφ.3], ενώ μια σκιαγράφηση του υπάρχει στον [Milne, [22], κεφ. 11]. Το αποτέλεσμα αυτό δίνει σαν πόρισμα, εφαρμόζωντας το Riemann-Roch, τον τύπο

$$dim S_2(\Gamma_0(N)) = g(X_0(N)).$$

Δείτε επίσης τον [Bump, [5], κεφ. 1] για μια συζήτηση πάνω σε αυτό.

Για την σύνδεση των modular μορφών ύψους 2 με την αλγεβρική γεωμετρία, η αντίστοιχη θεωρία είναι πιο απλή από την γενική περίπτωση, αν και είναι ήδη πολύ βαθιά, και είναι γνωστή ως θεωρία Eichler-Shimura. Κάποια σημαντικά στοιχεία αυτής της θεωρίας, μεταξύ των οποίων και τις σχέσεις Eichler-Shimura, θα μελετήσουμε στις επόμενες παραγράφους.

4.9 Η modular καμπύλη $X_0(N)$

Έστω N ένας θετικός ακέραιος. Θα ορίσουμε την modular καμπύλη ως εξής: Διαλέγουμε μία ελλειπτική καμπύλη E υπέρ το $\mathbb{Q}(t)$ ώστε $j(E) = t$. Στην συνέχεια διαλέγουμε ένα σημείο τάξης N επί της E και θεωρούμε την κυκλική ομάδα C που γεννά αυτό. Στην συνέχεια θεωρούμε το σταθερό σώμα K του $\overline{\mathbb{Q}(t)}$ το οποίο σταθεροποιείται από την ομάδα

$$\{\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}(t)}/\mathbb{Q}(t)) : \sigma(C) = C\}.$$

Το σώμα αυτό θα είναι το σώμα συναρτήσεων μιας ομαλής προβολικής καμπύλης την οποία θα ονομάσουμε $X_0(N)$.

Θα αποδείξουμε ότι το $\mathbb{Q}$ είναι αλγεβρικά κλειστό μέσα στο σώμα συναρτήσεων K, δηλαδή $K \cap \bar{\mathbb{Q}} = \mathbb{Q}$. Επίσης θα αποδείξουμε ότι μέχρι ισομορφισμού το σώμα K είναι ανεξάρτητο της επιλογής ελλειπτικής καμπύλης και ομάδας C.

Έστω k ένα σώμα χαρακτηριστικής που δεν διαιρεί το N. Αν k' είναι μία επέκταση του k η οποία περιέχει την ομάδα μ_N των N-οστών ριζών της μονάδας, θα συμβολίζουμε με χ τον κυκλοτομικό χαρακτήρα που ορίζεται από την δράση της $\mathrm{Gal}(k'/k)$ στο μ_N:

$$\sigma(\zeta) = \zeta^{\chi(\sigma)}, \sigma \in \mathrm{Gal}(k'/k), \zeta \in \mu_N.$$

Αν E είναι μια ελλειπτική καμπύλη υπέρ το k. Θεωρούμε το σύνολο $E[N] \subset E(\bar{k})$ των σημείων της τάξης N και συμβολίζουμε με $k(E[N])$ την πεπερασμένη επέκταση Galois του k η οποία παράγεται από τις συντεταγμένες των σημείων του $E[N]$. Σταθεροποιούμε μία βάση του $E[N]$ και με αυτό τον τρόπο έχουμε μία πιστή αναπαράσταση

$$\rho : \mathrm{Gal}(k(E[N])/k) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Κάνοντας χρήση των ιδιοτήτων του Weil pairing μπορούμε να διαπιστώσουμε ότι το σώμα $k(E[N])$ περιέχει το μ_N και επιπλέον

$$\det \rho = \chi.$$

Έτσι αν $k \subset \mu_N$ έχουμε ότι

$$\rho : \mathrm{Gal}(k(E[N])/k) \hookrightarrow \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}).$$

Θεώρημα 4.9.1. *Αν η ελλειπτική καμπύλη E είναι ελλειπτική καμπύλη υπέρ το $\mathbb{C}(t)$ με $j(E) = t$ τότε η αναπαράσταση*

$$\rho : \mathrm{Gal}(\mathbb{C}(E[N])/\mathbb{C}(t)) \xrightarrow{\cong} \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$$

είναι ισομορφισμός.

Παρατηρούμε ότι αν μια ελλειπτική καμπύλη ορίζεται υπέρ του σώματος $\mathbb{Q}(\mu_N)(t)$ τότε

$$\rho : \mathrm{Gal}(\mathbb{Q}(E[N])/\mathbb{Q}(\mu_N)(t)) \xrightarrow{\cong} \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$$

είναι επίσης ισομορφισμός, αφού είναι 1-1 και επιπλέον

$$[\mathbb{Q}(t, E[N]) : \mathbb{Q}(\mu_N)(t)] \geq [\mathbb{C}(t, E[N]) : \mathbb{C}(t)].$$

Ας υποθέσουμε ότι E είναι μια ελλειπτική καμπύλη η οποία ορίζεται υπέρ του $\mathbb{Q}(t)$ με $j(E) = t$. Τότε μπορούμε να την θεωρήσουμε και ως ελλειπτική καμπύλη υπέρ του $\mathbb{Q}(\mu_N)(t)$ και να έχουμε μια αναπαράσταση στο $E[N]$:

$$\rho : \mathrm{Gal}(\mathbb{Q}(t, E[N])/\mathbb{Q}(t)) \hookrightarrow \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$$

η οποία να στέλνει την υποομάδα $\mathrm{Gal}(\mathbb{Q}(E[N])/\mathbb{Q}(\mu_N)(t))$ επί της $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Αφού όμως $\det \rho = \chi$ η εικόνα της ρ περιέχει ένα πλήρες σύστημα αντιπροσώπων από σύμπλοκα της $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ στην $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ και συνεπώς έχουμε δείξει ότι:

Πόρισμα 4.9.2. *Αν E είναι μια ελλειπτική καμπύλη υπέρ του $\mathbb{Q}(t)$ με $j(E) = t$ τότε η αναπαράσταση στο $E[N]$ είναι ένας ισομορφισμός:*

$$\rho : \mathrm{Gal}(\mathbb{Q}(t, E[N])/\mathbb{Q}(t)) \xrightarrow{\cong} \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

και $\bar{\mathbb{Q}} \cap \mathbb{Q}(t, E[N]) = \mathbb{Q}(\mu_N)$.

Μπορούμε να αποδείξουμε το ότι $\bar{\mathbb{Q}} \cap \mathbb{Q}(t, E[N]) = \mathbb{Q}(\mu_N)$ ως εξής: Θέτουμε $L = \bar{\mathbb{Q}} \cap \mathbb{Q}(t, E[N])$ και υποθέτουμε ότι το L περιέχει γνήσια το $\mathbb{Q}(\mu_N)(t)$, τότε

$$[\mathbb{C}(t, E[N]) : \mathbb{C}(t)] \leq [\mathbb{Q}(t, E[N]) : L(t)] < |\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})|,$$

άτοπο.

Παρατηρούμε ότι η ταύτιση της ομάδας Galois $\mathrm{Gal}(\mathbb{Q}(t, E[N]))$ με την γενική γραμμική ομάδα προυποθέτει την επιλογή μιας βάσης για το $E[N] = \mathbb{Z}/N\mathbb{Z} \oplus \mathbb{Z}/N\mathbb{Z}$. Αν έχουμε ένα στοιχείο τάξης N στην E μπορούμε να υποθέσουμε ότι αυτό παράγει μια κυκλική ομάδα τάξης N η οποία είναι ο δεύτερος παράγοντας της παραπάνω διάσπασης του $E[N]$.

Έτσι σε αυτή την περίπτωση η υποομάδα H που διατηρεί την κυκλική υποομάδα αναλλοίωτη είναι η

$$H := \left\{ \begin{pmatrix} a & 0 \\ b & d \end{pmatrix} : a, d \in (\mathbb{Z}/N\mathbb{Z})^*, b \in \mathbb{Z}/N\mathbb{Z} \right\}.$$

Σχηματίζουμε το σώμα $K := \mathbb{Q}(t, E[N]))^H$. Η ορίζουσα απεικονίζει την H επί του $(\mathbb{Z}/N\mathbb{Z})^*$ άρα $\mathbb{Q}(\mu_N) \cap K = \mathbb{Q}$ (γιατί η ομάδα $\mathrm{Gal}(\mathbb{Q}(\mu_N)/\mathbb{Q})$ είναι ομάδα πηλίκο της H).

Αντικαθιστώ την σχέση $\mathbb{Q}(\mu_N) = \bar{\mathbb{Q}} \cap \mathbb{Q}(t, E[N]))$ και καταλήγω στο ότι

$$\bar{\mathbb{Q}} \cap K = \mathbb{Q}.$$

Επιπλέον μπορούμε να αποδείξουμε ότι μέχρι ισομορφισμού ορισμένου υπέρ το $\mathbb{Q}(t)$ το σώμα K είναι ανεξάρτητο της επιλογής της ομάδας C. Πράγματι, κάθε αλλαγή βάσης στο $E[N]$ έχει ως συνέπεια την συζυγία της ομάδας H μέσα στην $\mathrm{Gal}(\mathbb{Q}(t, E[N]))$ και συνεπώς οδηγούμαστε σε ένα συζυγές σώμα του K μέσα στην $\mathbb{Q}(t, E[N])$.

Παραμένει να εξετάσουμε την εξάρτηση του K από την επιλογή της ελλειπτικής καμπύλης E. Γενικά αν E είναι μια ελλειπτική καμπύλη ορισμένη υπέρ του σώματος k που έχει χαρακτηριστική p, $p \nmid N$, συμβολίζουμε με $k(E[N])/\pm)$ την επέκταση του k που παράγεται από τις x-συντεταγμένες των αφινικών σημείων της $E[N]$. Το $k(E[N]/\pm)$ είναι τότε το σταθερό σώμα της ομάδας

$$\{\sigma \in \mathrm{Gal}(k(E[N]/k) : \sigma(P) = \pm P \text{ για κάθε } P \in E[N]\}.$$

Στην περίπτωση που μας ενδιαφέρει βλέπουμε ότι το σώμα $\mathbb{Q}(t, E[N]/\pm)$ αντιστοιχεί στην υποομάδα $\{\pm I\}$ της $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ συνεπώς

$$\mathbb{Q}(t, E[N]/\pm) \cong \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}.$$

Έστω E' μια άλλη ελλειπτική καμπύλη υπέρ του $\mathbb{Q}(t)$ με $j(E') = t$. Τότε η E, E' διαφέρουν κατά μία τετραγωνική συστροφή και το ίδιο κάνουν και οι σχετισμένες αναπαραστάσεις

$$\mathrm{Gal}(\overline{\mathbb{Q}(t)}/\mathbb{Q}(t)) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$$

αρκεί να διαλέξουμε τις βάσεις των $E[N]$ και $E'[N]$ με συμβατό τρόπο. Άρα τα σώματα $\mathbb{Q}(t, E[N]/\pm)$ και $\mathbb{Q}(t, E'[N]/\pm)$ ταυτίζονται και οι ισομορφισμοί των ομάδων Galois στην $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$ ταυτίζονται. Όμως η ομάδα H που μόλις ορίσαμε περιέχει την $\pm$ και συνεπώς έχουμε την ανεξαρτησία από την ελλειπτική καμπύλη.

4.9α′ Άλλες modular καμπύλες

Μπορούμε να ορίσουμε σώματα συναρτήσεων σε διαφορετικές υποομάδες H της $\mathrm{Gal}(\mathbb{Q}(t, E[N]))$ αρκεί

(i) $-I \in H$ (ανεξαρτησία από την επιλογή ελλειπτικής καμπύλης με $j(E) = t$.

(ii) $\det : H \to (\mathbb{Z}/N\mathbb{Z})^*$ είναι επί (το $\mathbb{Q}$ είναι αλγεβρικά κλειστό στο σώμα συναρτήσεων της H.)

Με αυτό τον τρόπο ορίζουμε την $X_1(N)$ η οποία είναι η αλγεβρική καμπύλη που αντιστοιχεί στο σταθερό σώμα της

$$H := \left\{ \begin{pmatrix} a & 0 \\ b & \pm 1 \end{pmatrix} : a, d \in (\mathbb{Z}/N\mathbb{Z})^*, b \in \mathbb{Z}/N\mathbb{Z} \right\}.$$

4.10 Moduli interpretation

Έστω k ένα αλγεβρικά κλειστό σώμα και θεωρούμε ζευγάρια $(\mathcal{E}, \mathcal{C})$ τα οποία αποτελούνται από μία ελλειπτική καμπύλη $\mathcal{E}$ ορισμένη υπέρ το k και μία κυκλική υποομάδα του $\mathcal{E}[N]$, τάξης N. Ένας ισομροφισμός ανάμεσα σε ζευγάρια

$$(\mathcal{E}_1, \mathcal{C}_1) \to (\mathcal{E}_2, \mathcal{C}_2),$$

είναι ένας ισμορφισμός $\mathcal{E}_1 \to \mathcal{E}_2$ ο οποίος επιπλέον στέλνει την $\mathcal{C}_1$ στην $\mathcal{C}_2$. Θα συμβολίζουμε με $[\mathcal{E}, \mathcal{C}]$ την κλάση ισομορφισμού του ζευγαριού $(\mathcal{E}, \mathcal{C})$ και το σύνολο των κλάσεων με $\mathrm{Ell}_0(N)(k)$. Επίσης αν $S \subset \mathbb{P}^1(k)$ είναι υποσύνολο της προβολικής ευθείας θα συμβολίζουμε με $\mathrm{Ell}_0(N)(k)_S$ της κλάσεις ελλειπτικών καμπυλών ώστε $j(\mathcal{E}) \notin S$.

Μία διαφορετική σχέση ισοδυναμίας μπορεί να προκύψει ανάμεσα στα ζευγάρια $(\mathcal{E}, \mathcal{P})$ που αποτελούνται από μία ελλειπτική καμπύλη ορισμένη πάνω από το k και ένα σημείο $\mathcal{P} \in \mathcal{E}[n]$, όπου θεωρούμε τα ζευγάρια

$$(\mathcal{E}_1, \mathcal{P}_1) \to (\mathcal{E}_2, \mathcal{P}_2),$$

ισόμορφα αν υπάρχει ένας ισομορφισμός $\mathcal{E}_1 \to \mathcal{E}_2$ ο οποίος επιπλέον στέλνει το $\mathcal{P}_1$ στην $\mathcal{P}_2$. Είναι ενδιαφέρον να παρατηρήσουμε ότι $[\mathcal{E}, \mathcal{P}] = [\mathcal{E}, -P]$. Θα συμβολίζουμε με $\mathrm{Ell}_1(N)(k)$ το σύνολο των κλάσεων ισοδυναμίας και με $\mathrm{Ell}_1(N)(k)_S$ τις κλάσεις με $j(\mathcal{E}) \notin S$.

Παρατηρούμε ότι αν X είναι μια modular καμπύλη και E είναι μία ελλειπτική καμπύλη υπέρ του $\mathbb{Q}(t)$ τότε μπορούμε να την δούμε και ως ελλειπτική καμπύλη πάνω από το σώμα συναρτήσεων της modular καμπύλης X αφού αν $j(E) = t$ τότε το $\mathbb{Q}(t)$ είναι υπόσωμα του σώματος συναρτήσεων της modular καμπύλης.

Επιπλέον ένα σημείο $x \in X(\mathbb{C})$ καθορίζει ένα διακριτό δακτύλιο εκτίμησης $\mathcal{O}_x$ του μιγαδικού σώματος συναρτήσεων τις $X(\mathbb{C})$, τις συναρτήσεις που δεν έχουν πόλο στο x. Μπορούμε να ρωτήσουμε αν η E ορισμένη πάνω από το $\mathcal{O}_x$ έχει καλή αναγωγή modulo το μέγιστο ιδεώδες του $\mathcal{O}_x$. Αν όντως έχει καλή αναγωγή τότε έχουμε μια ελλειπτική καμπύλη E_x ορισμένη υπέρ το $\mathcal{O}_x/x\mathcal{O}_x \cong \mathbb{C}$. Μπορούμε να επεκτείνουμε (με περισσότερους από ένα τρόπους) τον $\mathcal{O}_x$ σε ένα διακριτό δακτύλιο εκτίμησης του σώματος $\mathbb{C}(t, E[N])$ και να θεωρήσουμε την αναγωγή του $E[N] \mapsto E_x[N]$ η οποία είναι 1-1. Έτσι αν το P είναι ένα σημείο τάξης N στην E και C είναι η ομάδα που αυτό παράγει τότε ορίζονται οι αναγωγές τους Px και C_x οι οποίες έχουν τάξη N.

Αν $S \subset \mathbb{P}^1(\mathbb{C})$ τότε με $\mathbb{P}^1_S$ συμβολίζουμε το $\mathbb{P}^1(\mathbb{C}) - S$ και $X(\mathbb{C})_S = X(\mathbb{C}) - j^{-1}(S)$. Για παράδειγμα αν $S = \{\infty\}$ τότε $X_0(N)(\mathbb{C}_S = Y_0(N)(\mathbb{C})$.

Πρόταση 4.10.1. *Έστω E μια ελλειπτική καμπύλη ορισμένη υπέρ το $\mathbb{Q}(t)$ με $j(E) = t$ και έστω S το σύνολο των σημείων του $\mathbb{P}^1(\mathbb{C})$ στα οποία η E έχει κακή αναγωγή. Σταθεροποιούμε μια διατεταγμένη βάση του $E[N]$ υπέρ του $\mathbb{Z}/N\mathbb{Z}$, και έστω P το δεύτερο στοιχείο αυτής της βάσης και C η κυκλική υποομάδα που αυτό παράγει. Τότε η συνάρτηση $x \to [E_x, C_x]$ ορίζει 1-1 και επί συνάρτηση ανάμεσα στο $X_0(N)(\mathbb{C})_S$ και στο $\mathrm{Ell}_0(N)(k)_S$. Παρόμοια αντιστοιχία υπάρχει ανάμεσα στις $X_1(N)(\mathbb{C})_S$ και στο $\mathrm{Ell}_1(N)(k)_S$.*

Απόδειξη. Παρατηρούμε ότι το σύνολο των σημείων καλής αναγωγής θα περιέχει τα $0, 1728, \infty$. Πράγματι μια εξίσωση ελλειπτικής καμπύλης με $j(E) = t$ είναι η

$$y^2 + yx = x^3 - \frac{36}{t - 1728}x - \frac{1}{t - 1728}$$

η οποία έχει κακή αναγωγή στα παραπάνω σημεία· η διακρίνουσα της είναι $t^2/(t - 1728)^3$. Κάθε άλλη ελλειπτική καμπύλη με $j(E) = t$ θα είναι μια συστροφή της παραπάνω εξίσωσης και η διακρίνουσα της θα διαφέρει με μία 6-δύναμη στοιχείου του $\mathbb{Q}(t)^*$.

Ταυτίζουμε την ομάδα $\mathrm{Gal}(\mathbb{Q}(t, E[N])/\mathbb{Q}(t))$ με την ομάδα $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ και την $\mathrm{Gal}(\mathbb{C}(t, E[N])/\mathbb{C}(t))$ με την $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. Θεωρούμε το

$$K = \mathbb{Q}(t, E[N])^H,$$

και η $X_0(N)$ ορίζεται να είναι η καμπύλη που αντιστοιχεί στο $\mathbb{C} \otimes K$. Επίσης θεωρούμε X μια καμπύλη που να έχει σώμα συναρτήσεων $\mathbb{C} \otimes \mathbb{Q}(t, E[N])$, και έστω

$$\pi : X \to X_0(N)$$

ο επαγώμενος μορφισμός.

Αν έχουμε $t_0 \mathbb{P}^1(\mathbb{C})_S$, $x_0 \in X_0(N)(\mathbb{C})$ υπέρ του t_0 και ένα σημείο $\hat{x_0} \in X(\mathbb{C})$ υπέρ του x_0 τότε έχουμε μια 1-1 και επί συνάρτηση:

$$\frac{\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})}{H \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})} \to \{\text{ίνα του } X_0(N)(\mathbb{C}) \text{ υπέρ το } t_0\}, \tag{4.1}$$

$$g(H \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})) \mapsto \pi(g\hat{x_0}),$$

γιατί η επέκταση $\mathbb{C}(t, E[N])/\mathbb{C}(t)$ είναι αδιακλάδιστη εκτός του S. Από την άλλη οι συναρτήσεις

$$\frac{\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})}{H \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})} \to \frac{\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})}{H}, \tag{4.2}$$

$$g(H \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})) \mapsto gH,$$

και

$$\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}) \to \{\text{κυκλικές υποοομάδες της } E \text{ τάξης } N\ \} \tag{4.3}$$

$$gH \mapsto gC$$

είναι επίσης 1-1 και επί και το ίδιο είναι και η συνάρτηση που προκύπτει από την αναγωγή modulo m_x:

(4.4)

$$\{\text{κυκλικές υποομάδες της } E \text{ τάξης } N\ \} \to \{\text{κυκλικές υποομάδες της } E_{x_0} \text{ τάξης N}\}$$

Αν $x = \pi(g\hat{x_0})$ τότε $E_x = E_{x_0}$ και $(gC)_{x_0} = C_x$ (οι ταυτίσεις αυτές είναι φυσιολογικές αφού το σώμα υπολοίπων $\mathbb{C}$ είναι υποδακτύλιος των $\mathcal{O}_x, \mathcal{O}_{x_0}$. Συνεπώς συνθέτοντας την αντίστροφο της (4.1) με τις (4.2),(4.3),(4.4) έχουμε ότι η συνάρτηση

$$\{\text{ίνα της } X_0(N)(\mathbb{C}) \text{ υπέρ } t_0\} \to \{\text{κυκλικές υποομάδες της } E_{x_0} \text{ με τάξη } N\}$$

$$x \mapsto C_x$$

είναι 1-1 και επί. Αφού $j(E_{x_0}) = t_0 \neq 0, 1728$, έχουμε ότι $\mathrm{Aut}(E_{x_0}) = \{\pm 1\}$ και ένας αυτομορφισμός της E_{x_0} στέλνει κάθε κυκλική υποομάδα της E_{x_0} στον εαυτό της. Συνεπώς

$$\left\{ \begin{array}{c} \text{κυκλικές υποομάδες της } E_{x_0} \\ \text{τάξης } N \end{array} \right\} \to \{[\mathcal{E}, \mathcal{C}] \in \mathrm{Ell}_0(N)(\mathbb{C}_S : j(\mathcal{E} = t_0\}, \}$$

$$\mathcal{C} \mapsto [E_{x_0}, \mathcal{C}]$$

είναι επίσης 1-1 και επί και συνθέτοντας με την προηγούμενη συνάρτηση καταλήγουμε σε στο ότι $x \mapsto [E_x, C_x]$ είναι 1-1 και επί από την ίνα του $X_0(N)(\mathbb{C})$ υπέρ $t_0 \in \mathbb{P}^1(\mathbb{C})_S$ στο υποσύνολο του $\mathrm{Ell}_0(N)(\mathbb{C})$ που αποτελείται από κλάσεις ισοδυναμίας ζευγών ελλειπτικών καμπυλών με δεδομένη $j(E) = t$. □

4.10α′ Απόδειξη θεωρήματος 4.9.1

Θα αποδείξουμε το θεώρημα βασισμένοι στην

Πρόταση 4.10.2. *Υπάρχει μία ελλειπτική καμπύλη E υπέρ $\mathbb{C}(t)$ η οποία να έχει $j(E) = t$ ώστε*

$$[\mathbb{C}(t, E[N]/\pm) : \mathbb{C}(t)] = |\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}/\{\pm I\}|.$$

Πράγματι, έστω μια ελλειπτική καμπύλη E' υπέρ του $\mathbb{C}(t)$ με $j(E') = t$. Τότε η E' διαφέρει από την E με μία τετραγωνική συστροφή συνεπώς $\mathbb{C}(t, E[N]/\pm) = \mathbb{C}(t, E'[N]/\pm)$. Άρα

$$[\mathbb{C}(t, E'[N]/\pm) : \mathbb{C}(t)] = [\mathbb{C}(t, E[N]/\pm) : \mathbb{C}(t)] = |\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}/\{\pm I\}|.$$

Η εμφύτευση

$$\mathrm{Gal}(\mathbb{C}(t, E'[N]/\pm)/\mathbb{C}(t) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}/\{\pm I\}$$

είναι ισομορφισμός. Συνεπώς η εικόνα της αναπαράστασης

$$\mathrm{Gal}(\mathbb{C}(t, E'[N])/\mathbb{C}(t) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$$

περιέχει ένα σύνολο από αντιπροσώπους συμπλόκων της $\{\pm I\}$ στην $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$, και περιέχει ή τον πίνακα $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ ή τον αντίστροφό του. Όμως $A^2 = -I$ άρα η εικόνα είναι όλο το $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

Θα χρησιμοποιήσουμε τώρα την θεωρία των modular μορφών. Θεωρούμε την ομάδα $\Gamma(N)$ που ορίστηκε στο κεφάλαιο 3. Παρατηρούμε ότι η ομάδα πηλίκο

$$\frac{\Gamma(1)}{\{\pm 1\}\Gamma(N)} \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}/\{\pm 1\}$$

είναι η ομάδα Galois της επέκτασης των σωμάτων των modular συναρτήσεων $\mathcal{M}(\Gamma(N))/\mathcal{M}(\Gamma(1))$ και η ταύτιση είναι η

$$\theta : \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z}/\{\pm 1\} \to \mathrm{Gal}\big(\mathcal{M}(\Gamma(N))/\mathcal{M}(\Gamma(1))\big)$$

$$\gamma \mapsto \theta([\gamma])(f) = f \circ \gamma^t,$$

όπου η $[\gamma]$ είναι η κλάση του γ modulo ± 1 και γ^t είναι ο ανάστροφος του πίνακα της γ.

Γνωρίζουμε ότι το σώμα $\mathcal{M}(\Gamma(1))$ παράγεται υπέρ του $\mathbb{C}$ από μία συνάρτηση την j-invariant. Και αφού

$$j = 1728\frac{g_2^3}{g_2^3 - 27g_3^2},$$

η συνάρτηση j είναι συνάρτηση από τα lattices τα οποία όμως παραμετρικοποιούνται από το υπερβολικό επίπεδο $\mathbb{H}$. Με αυτό τον τρόπο το σώμα $\mathcal{M}(\Gamma(N))$ προκύπτει ως επέκταση Galois του σώματος $\mathbb{C}(j)$. Θεωρούμε την ελλειπτική καμπύλη

$$E : y^2 = 4x^3 - \frac{27j}{j - 1728}x - \frac{27j}{j - 1728}$$

υπέρ του σώματος $\mathbb{C}(j)$. Θα αποδείξουμε ότι το σώμα $\mathbb{C}(j, E[N]/\pm)$ ταυτίζεται με το $\mathcal{M}(\Gamma(N))$ όταν και τα δύο σώματα θεωρούνται εντός σταθερής αλγεβρικής κλειστότητας του $\mathbb{C}(j)$.

Θα χρειαστούμε την θεωρία παραμετροποίησης του Weierstrass: Αν το L είναι ένα lattice του $\mathbb{L}$ τότε η ελλειπτική καμπύλη:

$$\mathcal{E}^{\mathrm{Wst}} : Y^2 = 4X^3 - g_2(L)X - g_3(L)$$

παραμετρικοποιείται μέσω της συνάρτησης

$$\wp(z, L) = \frac{1}{z^2} + \sum_{\substack{\omega \in L \\ \omega \neq 0}} \left(\frac{1}{(z+\omega)^2} - \frac{1}{\omega^2} \right).$$

Δηλαδή η συνάρτηση

$$\begin{aligned} \mathbb{C}/L &\to \mathcal{E}^{\mathrm{Wst}} \\ z+L &\mapsto (\wp(z,L),\wp'(z,L)) \end{aligned}$$

είναι ένα προς ένα και επί (τα $u \in L$ τότε θεωρούμε ότι απεικονίζονται στο επ άπειρο σημείο). Υποθέτουμε ότι $j(L) \neq 0, 1728$ και θεωρούμε την ελλειπτική καμπύλη:

$$\mathcal{E} : y^2 = 4x^3 - \frac{27j(L)}{j(L)-1728}x - \frac{27j(L)}{j(L)-1728}$$

Με $(g_2(L)/g_3(L))^{3/2}$ θα συμβολίζουμε μία σταθεροποιημένη ρίζα του $(g_2(L)/g_3(L))^3$. Παρατηρούμε ότι

$$\frac{g_2(L)^3}{g_3(L)^2} = \frac{27j(L)}{j(L)-1728}$$

και ότι η αλλαγή μεταβλητής:

$$X = \frac{g_3(L)}{g_2(L)}x, Y = \left(\frac{g_3(L)}{g_2(L)}\right)^{3/2} y$$

μετασχηματίζει την εξίσωση της $\mathcal{E}$ στην εξίσωση της $\mathcal{E}^{\mathrm{Wst}}$. Συνεπώς η συνάρτηση

$$z+L \mapsto \left(\frac{g_3(L)}{g_2(L)}\wp(z,L), \left(\frac{g_3(L)}{g_2(L)}\right)^{3/2}\wp'(z,L)\right)$$

είναι μία παραμετροποίση της $\mathcal{E}$.

Αν $\{\omega_1,\omega_2\}$ είναι μία βάση του L τότε οι ποσότητες

$$x_{r,s}(L) = \frac{g_3(L)}{g_2(L)}\wp\left(\frac{r\omega_1+s\omega_2}{N}, L\right)$$

είναι οι συντεταγμένες των N-torsion points της $\mathcal{E}$.

Γνωρίζουμε ότι ως συνάρτηση του z, η $\wp(z,L)$ είναι άρτια, περιοδική ως προς L και βαθμού 2 ως συνάρτηση $\mathbb{C}/L \to \mathbb{P}^1(\mathbb{C})$. Συνεπώς

$$x_{r,s}(\mathcal{L}) = x'_{r,s}(\mathcal{L}) \Leftrightarrow (r,s) \equiv \pm(r',s') \mod N.$$

Θα συμβολίζουμε με $\mathcal{R}$ το σύνολο των τροχιών της $(\mathbb{Z}/n\mathbb{Z})^2 - \{(0,0\}$ υπό την συνάρτηση πολλ/σμου με -1. Παρατηρούμε ότι αν τα $(r,s) \in \mathbb{Z}^2$ διατρέχουν ένα σύνολο αντιπροσώπων των κλάσεων του $\mathcal{R}$ τότε οι τιμές $x_{r,s}(L)$ είναι διαφορετικές.

Θα συμβολίζουμε με $P(w;A,b) \in \mathbb{Z}[w,A,B]$ το N-οστό πολυώνυμο διαίρεσης, το οποίο έχει την ιδιότητα $P(w_0,A,B) = 0$ αν και μόνο αν το w_0 είναι η x-συντεταγμένη ενός αφινικού N-torsion point της ελλειπτικής καμπύλης $y^2 = 4x^3 + Ax + B$. Εφαρμόζοντας την ιδιότητα αυτή του πολυωνύμου P για την ελλειπτική καμπύλη $\mathcal{E}$ έχουμε ότι

$$P(x_{r,s}\left(\mathcal{L}; \frac{27j(\mathcal{L})}{j(\mathcal{L})-1728}, \frac{27j(\mathcal{L})}{j(\mathcal{L})-1728}\right) = 0$$

στην περίπτωση που $j(\mathcal{L}) \neq 0, 1728$. Ειδικότερα, θέτουμε $\mathcal{L} = \mathcal{L}_z$ με $j(z) \neq 0, 1728$ και θεωρούμε

$$f_{r,s}(z) = \frac{g_2(z)}{g_3(z)}\wp\left(\frac{r+sz}{N}; \mathcal{L}_z\right) \quad r,s \in \mathbb{Z}, (r,s) \not\equiv (0,0) \mod N,$$

τότε $f_{r,s}(z) = x_{r,s}(\mathcal{L}_z)$ και συνεπώς

$$P\left(f_{r,s}(z); \frac{27j(z)}{j(z)-1728}, \frac{27j(z)}{j(z)-1728}\right) = 0.$$

Η παραπάνω εξίσωση είναι αληθής για όλα τα $z \neq 0, 1728$ άρα είναι αληθής και χωρίς αυτή την εξαίρεση δηλαδή

$$P\left(f_{r,s}; \frac{27j}{j-1728}, \frac{27j}{j-1728}\right) = 0$$

στο σώμα των μερομόρφων συναρτήσεων του $\mathbb{H}$. Δηλαδή οι συναρτήσεις $f_{r,s}$ είναι οι x-συντεταγμένες των αφινικών N-torsion points της ελλειπτικής καμπύλης E υπέρ του $\mathbb{C}(t)$ από την οποία ξεκινήσαμε.

Πρόταση 4.10.3. *Το σύνολο των x-συντεταγμένων των αφινικών N-torsion points στην ελλειπτική καμπύλη*

$$E : y^2 = 4x^3 - \frac{27j(z)}{j(z)-1728}x - \frac{27j(z)}{j(z)-1728}$$

ταυτίζεται με το σύνολο των συναρτήσεων

$$f_{r,s}(z) = \frac{g_2(z)}{g_3(z)}\wp\left(\frac{r+sz}{N}; \mathcal{L}_z\right)$$

σε κάθε αλγεβρική κλειστότητα του $\mathbb{C}(j)$ που τις περιέχει. Συνεπώς

$$\mathbb{C}(j, E[N]/\pm) = \mathbb{C}(j, f_{r,s}).$$

Απόδειξη. Καθώς το (r,s) διατρέχει ένα σύνολο αντιπροσώπων του $\mathcal{R}$ οι συναρτήσεις $f_{r,s}$ είναι διαφορετικές αφού παίρνουν διαφορετικές τιμές στα z ώστε $j(z) \neq 0, 1728$. Αφού κάθε συνάρτηση $f_{r,s}$ είναι η x-συντεταγμένη ενός αφινικού Ntorsion point της E και αφού το σύνολο των συναρτήσεων όπως και το πλήθος των διαφορετικών συντεταγμένων είναι ίσο με τον πληθάριθμο του $\mathcal{R}$, καταλήγουμε ότι οι συναρτήσεις $f_{r,s}$ εξαντλούν τις x-συντεταγμένες των N-torsion points. □

Πρόταση 4.10.4. *Ως σώματα έχουμε $\mathcal{M}(\Gamma(N)) = \mathbb{C}(j, f_{r,s})$.*

Απόδειξη. Παρατηρούμε ότι

(i) $f_{(r,s)} \circ \gamma = f_{(r,s)\gamma}$ για $\gamma \in \mathrm{SL}_2(\mathbb{Z})$.

(ii) Υπάρχει μία μερόμορφη συνάρτηση στο D που επεκτείνει τις μερόμορφες συναρτήσεις $F_{r,s}$ στο D^o που ορίζονται με $f_{r,s}(z) = F_{r,s}(e^{2\pi iz/N})$.

Οι ιδιότητες αυτές εξασφαλίζουν ότι $f_{r,s} \in \mathcal{M}(\Gamma(N)$. Για να δείξουμε ότι πράγματι το γεννούν χρησιμοποιούμε την (1). Αν ο εγκλεισμός $\mathbb{C}(j, f_{r,s}) \subset \mathcal{M}(\Gamma(N))$ ήταν γνήσιος τότε το σώμα $\mathbb{C}(j, f_{r,s})$ θα σταθεροποιούνταν από μια μη τετριμμένη υποομάδα της ομάδας Galois

$$\Gamma(1)/\{\pm I\}\Gamma(N) \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}.$$

Όμως μια υποομάδα του $\mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$ που δρα τετριμμένα στο $\mathcal{R}$ είναι αναγκαστικά τετριμμένη. □

Η απόδειξη της πρότασης 4.10.2 και συνεπώς του θεωρήματος 4.9.1 προκύπτει με συνδυασμό των προτάσεων 4.10.3,4.10.4.

4.11 Modular καμπύλες ως πηλίκα του υπερβολικού χώρου

Στην παράγραφο 3.5 ορίσαμε την έννοια της modular καμπύλης ως συμπαγοποίηση ενός πηλίκου του υπερβολικού χώρου. Σε αυτή την παράγραφο θα δούμε ότι οι δύο ορισμοί είναι ισοδύναμοι.

Δεδομένης μιας modular καμπύλης $X(H)$ θα κατασκευάσουμε μία διακριτή υποομάδα Γ της $\mathrm{SL}_2(\mathbb{Z})$ ώστε οι επιφάνειες Riemann $X(H)$ και $\Gamma\backslash\mathbb{H}^*$ να είναι ισόμορφες. Εξ ορισμού η ομάδα H είναι μία υποομάδα της $\mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$ που ικανοποιεί $-I \in H$ και $\det : H \to (\mathbb{Z}/N\mathbb{Z})^*$ είναι επί. Θεωρούμε την ομάδα $\Gamma \subset \mathrm{SL}_2(\mathbb{Z})$ να είναι η ανάστροφη ομάδα της $H \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$ υπό την συνάρτηση αναγωγής $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$.

Πρόταση 4.11.1. *Οι επιφάνειες Riemann $X(H)(\mathbb{C})$ και $\Gamma\backslash\mathbb{H}^*$ είναι ισόμορφες.*

Απόδειξη. Θεωρούμε μία ελλειπτική καμπύλη E υπέρ του σώματος $\mathbb{C}(j)$. Ταυτίζουμε την ομάδα $\mathrm{Gal}(\mathbb{Q}(j, E[N])/\mathbb{Q}(j))$ με την $\mathrm{GL}(2.\mathbb{Z}/N\mathbb{Z})$ κάνοντας επιλογή μίας βάσης του $E[N]$. Το σώμα συναρτήσεων της $X(H)$ υπέρ του $\mathbb{Q}$ είναι το υπόσωμα K του $\mathbb{Q}(j, E[N])/\pm)$ που σταθεροποιείται από την H, ενώ το σώμα συναρτήσεων της $X(H)(\mathbb{C})$ είναι το $\mathbb{C}K$. Η ταύτιση των ομάδων $\mathrm{Gal}(\mathbb{Q}(j, E[N])/\mathbb{Q}(j))$ και $\mathrm{GL}(2.\mathbb{Z}/N\mathbb{Z})$ μας επιτρέπει την ταύτιση

$$\mathrm{Gal}(\mathbb{C}(j, E[N])/\mathbb{C}(j)) \cong \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}.$$

ενώ οι υποθέσεις για την H εξασφαλίζουν ότι το $\mathbb{C}K$ είναι το υπόσωμα του $\mathbb{C}(j, E[N])/\pm)$ που σταθεροποιείται από την ομάδα $H \cap \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})/\{\pm I\}$. Αφού $\mathbb{C}(j, E[N]/\pm) = \mathcal{M}(\Gamma(N))$ έχουμε ότι $\mathbb{C}K = \mathcal{M}(\Gamma)$ και το αποτέλεσμα προκύπτει από το γεγονός ότι μια επιφάνεια Riemann προσδιορίζεται μέχρι ισομορφισμού από το σώμα μερομόρφων συναρτήσεων της. □

Ορισμός 4.11.2. *Θεωρούμε ζευγάρια $(\mathcal{T}, \mathcal{C})$ αποτελούμενα από ένα μονοδιάστατο μιγαδικό τόρο $\mathcal{T}$ και μια κυκλική υποομάδα του $\mathcal{C}$ τάξης N. Ένας ισομορφισμός από το ζευγάρι $(\mathcal{T}_1, \mathcal{C}_1)$ σε ένα ζευγάρι $(\mathcal{T}_2, \mathcal{C}_2)$ είναι ένας μιγαδικός αναλυτικός ισομορφισμός από τον $\mathcal{T}_1 \to \mathcal{T}_2$ ο οποίος απεικονίζει την $\mathcal{C}_1$ επί της $\mathcal{C}_2$. Η κλάση ισοδυναμίας του ζευγαριού θα συμβολίζεται με $[\mathcal{T}, \mathcal{C}]$ και το σύνολο των κλάσεων ισομορφίας με $\mathrm{Tori}_0(N)$.*

Με εντελώς ανάλογο τρόπο ορίζονται οι κλάσεις ισοδυναμίας ζευγών $(\mathcal{C}, \mathcal{P})$, όπου το $\mathcal{P}$ είναι ένα σημείο του $\mathcal{C}$ τάξης N. Το σύνολο των κλάσεων ισοδυναμίας θα συμβολίζεται με $\mathrm{Tori}_1(N)$.

Πρόταση 4.11.3. *Έστω E μία ελλειπτική καμπύλη υπέρ του σώματος $\mathbb{Q}(j)$ που να έχει invariant j. Έστω $S \subset \mathbb{P}^1(\mathbb{C})$ το σύνολο των θέσεων όπου η E έχει κακή αναγωγή. Σταθεροποιούμε μία διατεταγμένη βάση για το $E[N]$ υπέρ του $\mathbb{Z}/N\mathbb{Z}$, και θεωρούμε το δεύτερο στοιχείο P αυτής της βάσης και την ομάδα C τάξης N που παράγεται από το P. Τότε υπάρχει ένας ισομορφισμός των επιφανειών Riemann $X_0(N)(\mathbb{C}) \cong \Gamma_0(N)\backslash\mathbb{H}^*$ ώστε το διάγραμμα*

$$\begin{array}{ccc} X_0(N)(\mathbb{C})_S & \longrightarrow & \mathrm{Ell}_0(N)(\mathbb{C})_S \\ \downarrow & & \downarrow \\ \Gamma_0(N)\backslash\mathbb{H} & \longrightarrow & \mathrm{Tori}_0(N), \end{array}$$

να είναι αντιμεταθετικό. Στο διάγραμμα η πάνω οριζόντια συνάρτηση στέλνει το $x \to [E_x, C_x]$. *Η κάτω οριζόντια συνάρτηση έχει την μορφή*

$$[z] \mapsto [\mathbb{C}/\mathcal{L}_z, \langle 1/N + \mathcal{L}_z \rangle],$$

και στέλνει την κλάση $[z]$ *στην κλάση του μιγαδικού τόρου* $\mathbb{C}/\mathcal{L}_z$ *και την κυκλικής υποομάδας* $\langle 1/N + \mathcal{L}_z \rangle$. *Η αριστερή κάθετη συνάρτηση είναι ο περιορισμός στο* S *του ισομορφισμού* $X_0(N)(\mathbb{C}) \cong \Gamma_0(N)\backslash\mathbb{H}^*$. *Η δεξιά συνάρτηση ταυτίζει ελλειπτικές καμπύλες και υποομάδες τους με μιγαδικούς τόρους και υποομάδες τους.*

Ανάλογα θεωρήματα μπορούμε να διατυπώσουμε αντικαθιστώντας το $X_0(N)$ με $X_1(N)$ κτλ.

4.12 Hecke Correspondences

Μια correspondence σε μια προβολική καμπύλη X είναι μία τριάδα $T = (Z, \phi, \psi)$ αποτελούμενη από μια προβολική αλγεβρική καμπύλη Z και ϕ, ψ είναι μη σταθερές συναρτήσεις $Z \to X$. Θα λέμε ότι η correspondence ορίζεται υπέρ το σώματος k όταν X, Z, ϕ, ψ ορίζονται όλα στο k. Ένας αυτομορφισμός δ της καμπύλης X είναι ειδική περίπτωση correspondence όπου $Z = X, \phi = \mathrm{id}_X, \psi = \delta$.

4.12α′ Οι Hecke correspondence στην $X_0(N)$

Το N θα είναι ένας θετικός ακέραιος ο p θα είναι πρώτος αριθμός και το M το ελάχιστο κοινό πολλαπλάσιο των N, p. Διαλέγουμε μια ελλειπτική καμπύλη E υπέρ του σώματος $\mathbb{Q}(t)$ με invariant t και σταθεροποιούμε μια βάση του $E[M]$ υπέρ του $\mathbb{Z}/M\mathbb{Z}$ και ως συνήθως ταυτίζουμε την $\mathrm{Gal}(\mathbb{Q}(t, E[M])/\mathbb{Q}(t))$ με την ομάδα $\mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$. Θεωρούμε την υποομάδα

$$H_p = \left\{ \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z}) : c \equiv 0 \mod N, b \equiv 0 \mod p \right\}.$$

Η ομάδα H_p πληρεί τις απαιτήσεις που είχαμε θέσει στην ενότητα 4.9α′ δηλαδή $-I \in H_p$ και $\det(H_p) = (\mathbb{Z}/M\mathbb{Z})^*$. Συνεπώς το σταθερό σώμα της H_p είναι το σώμα συναρτήσεων μιας ομαλής προβολικής καμπύλης που ορίζεται υπέρ του σώματος $\mathbb{Q}$ και την οποία θα την συμβολίζουμε με $X_0(N, p)$. Η Hecke correspondence T_p είναι μια correspondence ορισμένη υπέρ του $\mathbb{Q}$ της μορφής

$$T_p = (X_0(N, p), \phi_p, \psi_p),$$

όπου θα πρέπει να ορίσουμε τους μορφισμούς ϕ_p, ψ_p.

Ορισμός του ϕ_p. Θα συμβολίζουμε με K_p και K τα σταθερά σώματα της H_p και της ομάδας

$$H = \left\{ \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z}) : c \equiv 0 \mod N \right\}.$$

Είναι σαφές ότι $H_p \subset H$ οπότε τα σταθερά σώματα θα ικανοποιούν την $K \subset K_p$. Ο τελευταίος εγκλεισμός σωμάτων συναρτήσεων αντιστοιχεί σε ένα μορφισμό καμπυλών

$$\phi_p : X_0(N, p) = X(H_p) \to X(H).$$

Όμως η $X(H)$ είναι ισόμορφη με την $X_0(N)$ γιατί ο πυρήνας της συνάρτησης αναγωγής

$$\mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z}) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z})$$

είναι υποομάδα της H και η εικόνα της H στην $\mathrm{GL}(2.\mathbb{Z}/N\mathbb{Z})$ είναι η κάτω τριγωνική ομάδα. Συνεπώς ο ϕ_p είναι μορφισμός από την $X_0(N,p)$ στην $X_0(N)$.

Ορισμός του ψ_p. Θα ορίσουμε ένα υπόσωμα $K' \hookrightarrow K_p$, όπου το K' είναι ισόμορφο με το K αλλά είναι διαφορετικό από το K. Προκειμένου να ορίσουμε το K' χρησιμοποιούμε την ταύτιση του $\mathrm{Gal}(\mathbb{Q}(t, E[M])/\mathbb{Q})$ με την ομάδα $\mathrm{GL}_2(\mathbb{Z}/M\mathbb{Z})$ η οποία προκύπτει με την επιλογή μιας βάσης του $E[M]$ πάνω από το $\mathbb{Z}/M\mathbb{Z}$, δηλαδή σε μία διάσπαση

$$E[M] = C_1 \oplus C_2,$$

όπου C_i είναι κυκλικές ομάδες τάξης M.

Έστω C η κυκλική υποομάδα του C_2 τάξης N, και έστω Π η κυκλική υποομάδα του C_1 τάξης p. Τότε εκ κατασκευής η H_p σταθεροποιεί τις C, Π συνεπώς οι ομάδες αυτές ορίζονται υπέρ του K_p. Ειδικότερα, αφού η Π ορίζεται υπέρ του K_p, υπάρχει μια ελλειπτική καμπύλη E/Π ορισμένη υπέρ του K_p και μία ισογένεια

$$\lambda : E \to E/\Pi,$$

ορισμένη υπέρ του K_p με πυρήνα Π. Επιπλέον η ελλειπτική καμπύλη E/Π έχει μια κυκλική υποομάδα τάξης N ορισμένη υπέρ του K_p, την $\lambda(C)$. Θέτουμε $t' = j(E/\Pi) \in K_p$, και επιπλέον θεωρούμε μια ελλειπτική καμπλύλη E' υπέρ του $\mathbb{Q}(t')$ με invariant t'. Συνεπώς υπάρχει ένας ισομορφισμός $\theta : E/\Pi \to E'$ ορισμένος υπέρ του $\bar{K}_p$ ο οποίος είναι μοναδικός μέχρι προσήμου αφού το t' είναι υπερβατικό συνεπώς διαφορετικό από τα $0, 1728$. Η ομάδα $C' = \theta(\lambda(C))$ είναι κυκλική υποομάδα της E' τάξης N η οποία επιπλέον είναι ανεξάρτητη της επιλογής του προσήμου για τον θ. Η C' είναι επίσης ορισμένη υπέρ του K_p αφού η $\lambda(C)$ είναι και $\sigma \circ \theta\sigma^{-1} = \pm\theta$ για κάθε $\sigma \in \mathrm{Gal}(\bar{K}_p/K_p)$. Συνεπώς το K_p περιέχει το σώμα K' το οποίο σταθεροποιείται από την ομάδα

$$\{\sigma \in \mathrm{Gal}(\overline{\mathbb{Q}(t')}/\mathbb{Q}(t')) : \sigma(C') = C'\}.$$

Αφού το K' είναι ισόμορφο με το σώμα συναρτήσεων της $X_0(N)$ έχουμε τον επιθυμητό μορφισμό ψ_p από το $X_0(N,p)$ στην $X_0(N)$.

Με ανάλογο τρόπο ορίζεται η correspondence $T_p = (X_1(N), \phi_p, \psi_p)$.

4.12β′ Moduli interpretation των Hecke correspondences

Δεδομένης μίας correspondence $T = (Z, \phi, \psi)$επί μίας προβολικής αλγεβρικής καμπύλης X θα συμβολίζουμε με T την συνάρτηση

$$X(k) \to \mathrm{Div}(X(k))$$

$$x \mapsto \sum_{\substack{z \in Z \\ \phi(z) = x}} \mathrm{mult}_z \phi\psi(z),$$

όπου $\mathrm{mult}_z\phi$ είναι ο δείκτης διακλάδωσης της ϕ στο z. Στην περίπτωση των Hecke correspondences θα περιγράψουμε με ακριβή τρόπο την παραπάνω correspondence σε όρους των divisors.

Ας υποθέσουμε ότι $\mathcal{E}$ είναι μια ελλειπτική καμπύλη υπέρ ενός αλγεβρικά κλειστού σώματος k και έστω Λ μία υποομάδα της $\mathcal{E}$ τάξης p. Θα συμβολίζουμε με $\mathcal{E}/\Lambda$ για την ελλειπτική καμπύλη πηλίκο που είναι εικόνα μιας διαχωρίσιμης ισογένειας με πυρήνα Λ. Παρατηρούμε ότι η καμπύλη $\mathcal{E}/\Lambda$ είναι μοναδική μέχρι ισομορφισμού. Επιπλέον αν η $\lambda : \mathcal{E} \to \mathcal{E}/\Lambda$ είναι διαχωρίσιμη ισογένεια με πυρήνα Λ και $\mathcal{C}$ είναι κυκλική υποομάδα της $\mathcal{E}$ τάξης N που τέμνει την Λ τετριμμένα (αυτό ισχύει πάντα αν $(N,p)=1$) τότε έχουμε μια καλά ορισμένη κλάση

$$[\mathcal{E}/\Lambda, (\mathcal{C}+\Lambda/\Lambda] \in \mathrm{Ell}_0(N)(k),$$

θέτοντας $[\mathcal{E}/\Lambda, (\mathcal{C}+\Lambda/\Lambda] = [\lambda(\mathcal{E}), \lambda(\mathcal{C})]$ η οποία είναι ανεξάρτητη από την επιλογή της ισογένειας λ.

Πρόταση 4.12.1. *Έστω E μια ελλειπτική καμπύλη υπέρ του σώματος $\mathbb{Q}(t)$ με invariant t. Θεωρούμε τα σύνολα S, S', S'' του $\mathbb{P}^1(\mathbb{C})$ που περιέχουν τις θέσεις κακής αναγωγής της E ώστε*

$$\phi_p^{-1}(X_0(N)(\mathbb{C})_S) \subset X_0(N,p)(\mathbb{C})_{S'}$$

και

$$\psi_P(X_0(N,p)(\mathbb{C})_{S'}) \subset X_0(N)(\mathbb{C})_{S''}.$$

Σταθεροποιούμε μια διατεταγμένη βάση για το $E[N]$ υπέρ του $\mathbb{Z}/N\mathbb{Z}$ και έστω P το δεύτερο στοιχείο της βάσης και C η κυκλική ομάδα που παράγει το P. Το παρακάτω διάγραμμα είναι αντιμεταθετικό:

$$\begin{array}{ccc} X_0(N)(\mathbb{C})_S & \xrightarrow{T_p} & \mathrm{Div}(X_0(N)(\mathbb{C})_{S''}) \\ \downarrow & & \downarrow \\ \mathrm{Ell}_0(N)(\mathbb{C}) & \longrightarrow & \mathrm{Div}(\mathrm{Ell}_0(N)(\mathbb{C}). \end{array}$$

Η αριστερή κάθετη απεικόνιση είναι η $x \mapsto [E_x, C_x]$ ενώ η δεξιά είναι η επαγώμενη συνάρτηση στην ομάδα των divisors. η δεύτερη οριζόντια συνάρτηση είναι η

$$[\mathcal{E}, \mathcal{C}] \mapsto \sum_{\substack{E[p]:\Lambda]=p \\ \mathcal{C}\cap\Lambda=\{0\}}} [\mathcal{E}/\Lambda, (\mathcal{C}+\Lambda)/\Lambda],$$

όπου το άθροισμα λογαριάζεται πάνω σε όλες τις υποομάδες Λ δείκτη p στην $\mathcal{E}[p]$ που τέμνουν την $\mathcal{C}$ με τετριμμένο τρόπο.

Παρόμοιο αποτέλεσμα έχουμε αν αντικαταστήσουμε παντού την X_0 με X_1 οπότε η τελευταία γραμμή είναι η συνάρτηση

$$[\mathcal{E}, \mathcal{P}] \mapsto \sum_{\substack{E[p]:\Lambda]=p \\ \langle\mathcal{P}\rangle\cap\Lambda=\{0\}}} [\mathcal{E}/\Lambda, \mathcal{P}+\Lambda],$$

Απόδειξη. Για κάθε $x \in X_0(N)(\mathbb{C})_S$ ο τύπος

$$T_P(x) = \sum_{\substack{z\in Z \\ \phi_p(z)=x}} (\mathrm{mult}_z\phi_p)\psi_p(z)$$

μπορεί να απλοποιηθεί στον

$$T_p(x) = \sum_{x \in \phi_p^{-1}(x)} \psi_p(z),$$

γιατί ο μορφισμός $\phi_p : X_0(N,p) \to X_0(N)$ είναι αδιακλάδιστη εκτός του S. Πράγματι η αντίστοιχη επέκταση σωμάτων K_p/K περιέχεται στην επέκταση σωμάτων $\mathbb{Q}(t, E[M])/\mathbb{Q}(t)$ και είναι αδιακλάδιστη εκτός των θέσεων που η E έχει κακή αναγωγή.

Θεωρούμε τριάδες $(\mathcal{E}, \mathcal{C}, \Lambda)$, όπου $\mathcal{E}$ είναι μια ελλειπτική καμπύλη υπέρ του $\mathbb{C}$, η $\mathcal{C}$ είναι κυκλική υποομάδα της $\mathcal{E}$ τάξης N, και η Λ είναι κυκλική υποομάδα της $\mathcal{E}$ τάξης p που τέμνει την $\mathcal{C}$ με τετριμμένο τρόπο. Θα συμβολίζουμε με $[\mathcal{E}, \mathcal{C}, \Lambda]$ την κλάση ισομορφισμού μιας τέτοιας κλάσης και με $\mathrm{Ell}_0(N,p)(\mathbb{C})$ το σύνολο των κλάσεων ισομορφισμού. Ορίζουμε συναρτήσεις $\phi, \psi : \mathrm{Ell}_0(N,p)(\mathbb{C}) \to \mathrm{Ell}_0(N)(\mathbb{C})$ με

$$\phi([\mathcal{E}, \mathcal{C}, \Lambda]) = [\mathcal{E}, \mathcal{C}]$$

και

$$\psi([\mathcal{E}, \mathcal{C}, \Lambda]) = [\mathcal{E}/\Lambda, (\mathcal{C} + \Lambda)/\Lambda].$$

Η συνάρτηση

$$[\mathcal{E}, \mathcal{C}] \mapsto \sum_{\substack{[\mathcal{E}[p]:\Lambda]=p \\ \mathcal{C} \cap \Lambda = \{0\}}} [\mathcal{E}/\Lambda, (\mathcal{C} + \Lambda)/\Lambda]$$

έχει την μορφή

$$x \mapsto \sum_{x \in \phi^{-1}(x)} \psi(z).$$

Συνεπώς αρκεί να δείξουμε ότι τα διαγράμματα

$$\begin{array}{ccc} X_0(N,p)(\mathbb{C})_{S'} & \xrightarrow{\phi_p} & X_0(N)(\mathbb{C})_S \\ \downarrow & & \downarrow \\ \mathrm{Ell}_0(N,p)(\mathbb{C}) & \xrightarrow{\phi} & \mathrm{Ell}_0(N)(\mathbb{C}) \end{array}$$

και

$$\begin{array}{ccc} X_0(N,p)(\mathbb{C})_{S'} & \xrightarrow{\psi_p} & X_0(N)(\mathbb{C})_{S''} \\ \downarrow & & \downarrow \\ \mathrm{Ell}_0(N,p)(\mathbb{C}) & \xrightarrow{\psi} & \mathrm{Ell}_0(N)(\mathbb{C}) \end{array}$$

είναι αντιμεταθετικά όπου οι αριστερές κάθετες συναρτήσεις είναι οι $x \mapsto [E_x, C_x]$ και οι δεξιές κάθετες συναρτήσεις δίνονται από

$$X_0(N,p)(\mathbb{C})_{S'} \to \mathrm{Ell}_0(N,p)(\mathbb{C})$$

$$z \mapsto [E_z, C_z, \Pi_z].$$

Η ομάδα Π είναι μια υποομάδα της E τάξης p η οποία τέμνει με τετριμμένο τρόπο την C, ενώ ο δείκτης z συμβολίζει την αναγωγή modulo το μέγιστο ιδεώδες του διακριτού δακτυλίου εκτίμησης που αντιστοιχεί στο z στο μιγαδικό σώμα συναρτήσεων της $X_0(N,p)$.

Το να δείξουμε ότι το πρώτο διάγραμμα είναι αντιμεταθετικό ανάγεται στο να δείξουμε ότι

$$[E_z, C_z] = [E_{\phi_p(z)}, C_{\phi_p(z)}],$$

το οποίο προκύπτει από την αντιμεταθετικότητα της αναγωγής. Για το δεύτερο διάγραμμα, θέτουμε $t' = j(E/\Pi)$, διαλέγουμε μια ελλειπτική καμπύλη E' υπέρ του $\mathbb{Q}(t')$ με invariant t', την εικόνα του $(C+\Pi)/\Pi$ υπό τον ισομορφισμό $E/\Pi \to E'$. Θα πρέπει να ελέγξουμε ότι

$$[E_z/\Pi_z, (C_z+\Pi_z)/\Pi_z] = [E'_{\psi_p(z)}, C'_{\psi_p(z)}]. \tag{4.5}$$

Αυτό το κάνουμε σε δύο βήματα:

$$[E_z/\Pi_z, (C_z+\Pi_z)/\Pi_z] = [(E/\Pi)_z, ((C+\Pi)/\Pi)_z] \tag{4.6}$$

λόγω της συμβατότητας της αναγωγής με τις ισογένειες. Στην συνέχεια θεωρούμε ένα ισομορφισμό $\theta : E\Pi \to E'$, ώστε $C' = \theta((C+\Pi)/\Pi)$. Η αναγωγή του θ δίνει ένα ισομορφισμό από το $(E/\Pi)_z$ στο $(E')_{\psi_p(z)}$ ο οποίος στέλνει το $((C+\Pi)/\Pi)_z$ στο $(C')_{\psi_p(z)}$ συνεπώς

$$[E_z/\Pi_z, (C_z+\Pi_z)/\Pi_z] = [(E')_{\psi_p(z)}, (C')_{\psi_p(z)}]. \tag{4.7}$$

Το αποτέλεσμα προκύπτει από τις (4.5),(4.6),(4.7). □

4.12γ′ Οι Hecke correspondences στο υπερβολικό επίπεδο

Για $d \in (\mathbb{Z}/N\mathbb{Z})^*$ θα συμβολίζουμε με $\langle d\rangle$ ένα στοιχείο του $\Gamma_0(N)$ με κάτω δεξιά στοιχείο ισοδύναμο με $d \mod N$.

Πρόταση 4.12.2. *Υπάρχει ένα αντιμεταθετικό διάγραμμα*

$$\begin{array}{ccc} X_0(N)(\mathbb{C}) & \xrightarrow{T_p} & \mathrm{Div}(X_0(N)(\mathbb{C}) \\ \downarrow & & \downarrow \\ \Gamma_0(N)\backslash\mathbb{H}^* & \longrightarrow & \mathrm{Div}(\Gamma_0(N)\backslash\mathbb{H}^*) \end{array}$$

όπου η κάτω οριζόντια γραμμή είναι η συνάρτηση:

$$[z] \mapsto \begin{cases} \sum_{\nu=0}^{p-1}[(z+\nu)/p] + [pz] & \text{αν } p \nmid N \\ \sum_{\nu=0}^{p-1}[(z+\nu)/p] & \text{αν } p \mid N \end{cases}$$

Απόδειξη. Το θεώρημα προκύπτει αν θεωρήσουμε τα lattice $\mathcal{L}_z$ και τις φυσιολογικές υποομάδες τους $\mathcal{C} = \langle 1/N + \mathcal{L}_z\rangle$. □

4.13 Hecke correspondences και ο αυτομορφισμός του Frobenious

Θεωρούμε ένα πρώτο που δεν διαιρεί το N, και σταθεροποιούμε ένα πρώτο ιδεώδες $\mathfrak{p}$ του $\bar{\mathbb{Q}}$ το οποίο επεκτείνει το p. Το σώμα υπολοίπων του $\mathfrak{p}$ είναι το $\bar{\mathbb{F}}_p$. Θα συμβολίζουμε με μία περισπωμένη την αναγωγή $\mod \mathfrak{p}$. Αν $\mathcal{E}$ είναι μια ελλειπτική καμπύλη υπέρ του $\bar{\mathbb{Q}}$ με καλή αναγωγή στο $\mathfrak{p}$ θα συμβολίζουμε την αναγωγή $\tilde{\mathcal{E}}$ η οποία είναι μια καμπύλη ορισμένη υπέρ του $\bar{\mathbb{F}}_p$.

Ορίζουμε τα σύνολα $\mathrm{Ell}_1(N)(\bar{\mathbb{Q}})$ και $\mathrm{Ell}_1(N)(\bar{\mathbb{F}}_p)$, αντικαθιστώντας το σώμα των μιγαδικών αριθμών με τα $\bar{\mathbb{Q}}$ και $\bar{\mathbb{F}}_p$. Το σύνολο $\mathrm{Ell}_1(N)(\bar{\mathbb{Q}})_{\mathrm{gd}}$ αποτελείται από το υποσύνολο των κλάσεων $\mathrm{Ell}_1(N)(\bar{\mathbb{Q}})$ που έχουν καλή αναγωγή στο $\mathfrak{p}$. Υπό την προϋπόθεση ότι $p \nmid N$ έχουμε μια καλά ορισμένη συνάρτηση

$$\mathrm{Ell}_1(N)(\bar{\mathbb{Q}})_{\mathrm{gd}} \to \mathrm{Ell}_1(N)(\bar{\mathbb{F}}_p)$$

$$[\mathcal{E}, \mathcal{P}] \mapsto [\tilde{\mathcal{E}}, \tilde{\mathcal{P}}]$$

αφού η αναγωγή modulo $\mathfrak{p}$ είναι ένα προς ένα στα N-torsion points.

Υπενθυμίζουμε ότι μια ελλειπτική καμπύλη $\mathcal{E}$ υπέρ του $\bar{\mathbb{Q}}$ έχει ordinary καλή αναγωγή αν $\tilde{\mathcal{E}}[p]$ έχει τάξη p. Αν η $\mathcal{E}$ έχει ordinary καλή αναγωγής τότε η αναγωγή modulo $\mathfrak{p}$ ορίζει έναν επιμορφισμό

$$\mathcal{E}[p] \to \tilde{\mathcal{E}}[p]$$

με πυρήνα μια υποομάδα του $\mathcal{E}[p]$ τάξης (ή δείκτη) p. Επιπλέον η $\mathcal{E}[p]$ έχει ακριβώς p το πλήθος άλλες υποομάδες με δείκτη p.

Θα χρησιμοποιούμε έναν εκθέτη p για να συμβολίζουμε την εικόνα ενός αντικειμένου κάτω από την δράση του Frobenious του $\bar{\mathbb{F}}_p$ και ένα εκθέτη p^{-1} για να συμβολίζουμε την εικόνα κάτω από τον αντίστροφο του Frobenious.

Πρόταση 4.13.1. *Έστω μια ελλειπτική καμπύλη $\mathcal{E}$ ορισμένη υπέρ του σώματος $\bar{\mathbb{Q}}$ με ordinary καλή αναγωγή στο $\mathfrak{p}$ και έστω Λ_0 ο πυρήνας της συνάρτησης αναγωγής*

$$\mathcal{E}[p] \to \tilde{\mathcal{E}}[p].$$

Αν Λ είναι υποομάδα της $\mathcal{E}[p]$ δείκτου p τότε

$$[\widetilde{\mathcal{E}/\Lambda}, \widetilde{\mathcal{P}+\lambda}] = \begin{cases} [\tilde{\mathcal{E}}^p, \tilde{\mathcal{P}}^p, & \text{αν } \Lambda = \Lambda_0 \\ [\tilde{\mathcal{E}}^{p^{-1}}, p\tilde{\mathcal{P}}^{p^{-1}}], & \text{αν } \Lambda \neq \Lambda_0 \end{cases}$$

Απόδειξη. Έστω $\lambda_0 : \mathcal{E} \to \mathcal{E}/\Lambda_0$ την ισογένεια με πυρήνα Λ_0 και $\mu_0 : \mathcal{E}/\Lambda_0 \to \mathcal{E}$ την δυική ισογένεια. Η εικόνα της $(\mathcal{E}/\Lambda_0)[p]$ κάτω από την μ_0 είναι η Λ_0. Πράγματι, αφού η μ_0 είναι μια p-ισογένεια, η εικόνα της $(\mathcal{E}/\Lambda_0)[p]$ υπό την μ_0 είναι μια μια ομάδα τάξης p. Αν αυτή η ομάδα δεν ήταν υποομάδα της Λ_0 τότε η εικόνα της $(\mathcal{E}/\Lambda_0)[p]$ υπό την $\lambda_0 \circ \mu_0$ δεν θα ήταν 0 το οποίο έρχεται σε αντίφαση με το ότι $\lambda_0 \circ \mu_0$ είναι πολλαπλασιασμός με p. Θεωρούμε το αντιμεταθετικό διάγραμμα:

$$\begin{array}{ccccc} \mathcal{E}[p] & \xrightarrow{\lambda_0} & (\mathcal{E}/\Lambda_0)[p] & \xrightarrow{\mu_0} & \mathcal{E}[p] \\ \downarrow & & \downarrow & & \downarrow \\ \tilde{\mathcal{E}}[p] & \xrightarrow{\tilde{\lambda}_0} & (\widetilde{\mathcal{E}/\Lambda_0})[p] & \xrightarrow{\tilde{\mu}_0} & \tilde{\mathcal{E}}[p] \end{array},$$

όπου οι κάθετοι μορφισμοί είναι αναγωγές modulo $\mathfrak{p}$ και συνεπώς επί. Αφού η εικόνα της $(\mathcal{E}/\Lambda_0)[p]$ υπό την μ_0 είναι Λ_0, η αντιμεταθετικότητα του διαγράμματος επιβάλει ότι η $\tilde{\mu}_0$ είναι 0 στην $(\widetilde{\mathcal{E}/\Lambda_0})[p]$. Επιπλέον η $\tilde{\mathcal{E}}$ είναι ordinary εξ υποθέσεως, και αφού η $\widetilde{\mathcal{E}/\Lambda_0}$ είναι ισογενής με την $\tilde{\mathcal{E}}$, είναι επίσης ισογενής. Το γεγονός ότι η $\tilde{\mu}_0$ είναι 0 στην $(\mathcal{E}/\Lambda_0)[p]$ μας δίνει ότι η $\tilde{\mu}_0$ είναι μια διαχωρίσιμη p-ισογένεια. Όμως ο πολλαπλασιασμός με p είναι αδιαχωρίσιμος. Άρα η $\tilde{\lambda}_0$ είναι αδιαχωρίσιμη (και μάλιστα γνήσια) ισογένεια βαθμού p, και μπορούμε να γράψουμε $\tilde{\lambda}_0 = \theta \circ \beta$,

όπου β είναι ο ενδομορφισμός του Frobenious βαθμού p και $\theta : E^p \to \widetilde{\mathcal{E}/\Lambda_0}$ είναι ισομορφισμός. Συνεπώς

$$[\widetilde{\mathcal{E}/\Lambda_0}, \widetilde{\mathcal{P}+\Lambda_0}] = [\tilde{\lambda}(\tilde{\mathcal{E}}), \tilde{\lambda}_0(\tilde{\mathcal{P}})] = [\beta(\tilde{\mathcal{E}}, \beta(\tilde{\mathcal{P}})] = [\tilde{\mathcal{E}}^p, \tilde{\mathcal{P}}^p].$$

Θα μελετήσουμε τώρα την περίπτωση $\Lambda \neq \Lambda_0$. Διαλέγουμε μια ισογένεια $\lambda : \mathcal{E} \to \mathcal{E}/\Lambda$ με πυρήνα Λ και θεωρούμε την καμπύλη $\lambda(\mathcal{E}) = \mathcal{E}/\Lambda$ μαζί με την υποομάδα της $\lambda(\Lambda_0)$ τάξης p. Αφού η $\lambda(\mathcal{E})$ είναι ισογενής με την $\mathcal{E}$, έχει ordinary αναγωγή modulo $\mathfrak{p}$ και συνεπώς ο πυρήνας της αναγωγής modulo $\mathfrak{p}$ στην $\lambda(\mathcal{E})[p]$ είναι μια υποομάδα τάξης p. Υπολογίζουμε

$$\widetilde{\lambda(\Lambda_0)} = \tilde{\lambda}(\tilde{\Lambda}_0) = \tilde{\lambda}(\{0\}) = \{0\}.$$

Άρα η $\lambda(\Lambda_0)$ περιέχεται σε αυτή την υποομάδα και συνεπώς ταυτίζεται με αυτή αφου και οι δύο έχουν τάξη p. Μπορούμε να εφαρμόσουμε στις $\lambda(\mathcal{E})$ και $\lambda(\Lambda_0)$ ότι αποδείξαμε για τις $\mathcal{E}$ και Λ_0:

$$[\lambda(\widetilde{\mathcal{E})/\lambda(\Lambda_0)}, \lambda(\widetilde{\mathcal{P})+\lambda(\Lambda_0)}] = [\widetilde{\lambda(E)}^p, \widetilde{\lambda(\mathcal{P})}^p]. \tag{4.8}$$

Αν όμως $\mu : \lambda(\mathcal{E} \to \lambda(\mathcal{E})/\lambda(\Lambda_0)$ είναι οποιαδήποτε ισογένεια με πυρήνα $\lambda(\Lambda_0)$, τότε εξ ορισμού

$$[\lambda(\mathcal{E})/\lambda(\Lambda_0), \lambda(\mathcal{P}) + \lambda(\Lambda_0)] = [(\mu \circ \lambda)(\mathcal{E}), (\mu \circ \lambda)(\mathcal{P})].$$

Διαλέγουμε την μ να είναι η δυική ισογένεια της λ και τότε

$$[(\mu \circ \lambda)(\mathcal{E}), (\mu \circ \lambda)(\mathcal{P})] = [\mathcal{E}, p\mathcal{P}].$$

Συνεπώς η (4.8) μπορεί να γραφεί ως

$$[\tilde{\mathcal{E}}, p\tilde{\mathcal{P}}] = [\widetilde{\mathcal{E}/\Lambda)}^p, \widetilde{\mathcal{P}+\Lambda}^p]. \tag{4.9}$$

Εφαρμόζοντας τον αντίστροφο του Frobenious στην (4.9) καταλήγουμε στο επιθυμιτό αποτέλεσμα. □

Θα συμβολίζουμε με $\mathrm{Ell}_1(N)(\bar{\mathbb{Q}})_{\mathrm{ord}}$ το υποσύνολο του $\mathrm{Ell}_1(N)(\bar{\mathbb{Q}})_{\mathrm{gd}}$ των κλάσεων $[\mathcal{E}, \mathcal{P}]$ οι οποίες έχουν ordinary καλή αναγωγή στο $\mathfrak{p}$. Η συνάρτηση αναγωγής μεταξύ κλάσεων ισομορφισμού

$$\mathrm{Ell}_1(N)(\bar{\mathbb{Q}})_{\mathrm{ord}} \to \mathrm{Ell}_1(N)(\bar{\mathbb{F}}_p)$$

$$[\mathcal{E}, \mathcal{P}] \mapsto [\tilde{\mathcal{E}}, \tilde{\mathcal{P}}],$$

επεκτείνεται με μοναδικό τρόπο σε ομομορφισμό

$$\mathrm{red}_{\mathfrak{p}} : \mathrm{Div}(\mathrm{Ell}_1(N)(\bar{\mathbb{Q}})_{\mathrm{ord}}) \to \mathrm{Div}(\mathrm{Ell}_1(N)(\bar{\mathbb{F}}_p)).$$

Πρόταση 4.13.2 (Eichler-Shimura)**.** *Έστω $\sigma_{\mathfrak{p}} \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ ένα Frobenious στοιχείο στο $\mathfrak{p}$. Τότε*

$$T_p = \sigma_{\mathfrak{p}} + p\langle p \rangle \sigma_{\mathfrak{p}}^{-1},$$

όπου και οι δύο πλευρές θεωρούνται ως συναρτήσεις

$$\mathrm{Ell}_1(N)(\bar{\mathbb{Q}})_{\mathrm{ord}} \to \mathrm{Div}(\mathrm{Ell}_1(N)(\bar{\mathbb{Q}})_{\mathrm{ord}})/\mathrm{Ker}(\mathrm{red}_{\mathfrak{p}}).$$

Απόδειξη. Θεωρούμε μια ελλειπτική καμπύλη $\mathcal{E}$ υπέρ του $\bar{\mathbb{Q}}$ με ordinary αναγωγή στο $\mathfrak{p}$, και έστω $\mathcal{P}$ ένα σημείο τάξης N στην $\mathcal{E}$. Θα πρέπει να δείξουμε ότι $T_p([\mathcal{E},\mathcal{P}])$ και $\sigma_\mathfrak{p} + p\langle p\rangle\sigma_\mathfrak{p}^{-1}([\mathcal{E},\mathcal{P}])$ έχουν την ίδια εικόνα μέσω της $\mathrm{red}_\mathfrak{p}$. Έχουμε υπολογίσει ότι

$$T_p([\mathcal{E},\mathcal{P}]) = \sum_\Lambda [\mathcal{E}/\Lambda, \mathcal{P}+\Lambda],$$

όπου το άθροισμα διατρέχει τις υποομάδες $\Lambda \subset \mathcal{E}[p]$ δείκτου p που έχουν τετριμμένη τομή με την κυκλική ομάδα που παράγεται από το $\mathcal{P}$. Από την άλλη

$$\sigma_\mathfrak{p} + p\langle p\rangle\sigma_\mathfrak{p}^{-1}([\mathcal{E},\mathcal{P}]) = [\mathcal{E}^{\sigma_\mathfrak{p}}, \mathcal{P}^{\sigma_\mathfrak{p}}] + p[\mathcal{E}^{\sigma_\mathfrak{p}^{-1}}, \mathcal{P}^{\sigma_\mathfrak{p}^{-1}}].$$

Έτσι θα πρέπει να ελέγξουμε ότι

$$\sum_\Lambda [\widetilde{\mathcal{E}/\Lambda}, \widetilde{\mathcal{P}+\Lambda}] = [\tilde{\mathcal{E}}^p, \tilde{\mathcal{P}}^p] + p[\tilde{\mathcal{E}}^{p^{-1}}, p\tilde{\mathcal{P}}^{p^{-1}}].$$

Το οποίο προκύπτει από την πρόταση 4.13.1 αφού το άθροισμα στο αριστερό μέλος έχει $p+1$ όρους και ακριβώς ένας περιέχει τον πυρήνα της $\mathcal{E}[p] \to \tilde{\mathcal{E}}[p]$. □

Δεδομένης μιας ομαλής προβολικής καμπύλης X και μιας correspondence $T = (Z,\phi,\psi)$ στην X θα χρησιμοποιούμε το ίδιο σύμβολο T για να θεωρούμε τον ενδομορφισμό $\psi_P \circ \phi^*$ στην Ιακωβιανή πολλαπλότητα $\mathrm{Jac}(X)$. Αν το k είναι αλγεβρικά κλειστό τότε η συνάρτηση επί των σημείων $\mathrm{Jac}(X)(k) \to \mathrm{Jac}(X)(k)$ που αντιστοιχεί στην T προκύπτει επεκτείνοντας την T στους divisors της Q βαθμού 0, και στην συνέχεια θεωρούμε την συνάρτηση επί των κλάσεων divisors.

Θα ασχοληθούμε με την περίπτωση $X = X_1(N)$, $T = T_p$. Θα συμβολίζουμε την Ιακωβιανή πολλαπλότητα $\mathrm{Jac}(X_1(N))$ απλά με $J_1(N)$. Αν ℓ είναι πρώτος και n θετικός ακέραιος τότε ο δακτύλιος ενδομορφισμών της $J_1(N)$ δρα στην αβελιανή ομάδα $J_1(N)[\ell^n]$. Το ίδιο κάνει και η ομάδα $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ αφού η $J_1(N)$ ορίζεται υπέρ του $\mathbb{Q}$.

Θεώρημα 4.13.3 (Eichler-Shimura)**.** *Έστω $\sigma_\mathfrak{p} \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ ένα Frobenious στοιχείο στο $\mathfrak{p}$. Τότε για $\ell \neq p$ και $n \geq 1$*

$$T_p = \sigma_\mathfrak{p} + p\langle p\rangle\sigma_\mathfrak{p}^{-1}$$

ως ενδομορφισμοί του $J_1(N)[\ell^n]$.

Απόδειξη. Θεωρούμε την αναγωγή $\widetilde{X_1(N)}$ της $X_1(N)$ modulo p. Ως συνάρτηση επί των σημείων η αναγωγή $X_1(N)(\bar{\mathbb{Q}}) \to \widetilde{X_1(N)}(\bar{\mathbb{F}}_p)$ είναι συμβατή με την συνάρτηση $[\mathcal{E},\mathcal{P}] \mapsto [\tilde{\mathcal{E}},\tilde{\mathcal{P}}]$ κατά την παρακάτω έννοια.

Θα συμβολίζουμε με $\mathbb{Z}[t]_{(p)}$ τον εντοπισμό του $\mathbb{Z}[t]$ στο πρώτο ιδεώδες που παράγεται από το p. Θα λέμε ότι μια ελλειπτική καμπύλη E ορισμένη υπέρ του $\mathbb{Q}(t)$ θα έχει καλή αναγωγή στο p αν υπάρχει μια γενικευμένη εξίσωση Weierstrass για την E υπέρ του $\mathbb{Z}[t]_{(p)}$ με διακρίνουσα μονάδα του $\mathbb{Z}[t]_{(p)}$. Η αναγωγή αυτής της εξίσωσης modulo $p\mathbb{Z}[t]_{(p)}$ ορίζει μια ελλειπτική καμπύλη $\tilde{E}$ υπέρ του $\mathbb{F}_p(t)$. Θεωρούμε μια ελλειπτική καμπύλη E υπέρ του $\mathbb{Q}(t)$ με invariant t και καλή αναγωγή στο p. Για παράδειγμα μπορούμε να θεωρήσουμε την

$$y^2 + xy = x^3 - \frac{36}{t-1728}x - \frac{1}{t-1728}$$

με διακρίνουσα $t^2/(t-1728)^3$. Έστω P ένα σημείο τάξης N στην E, έστω $\tilde{P} \in \tilde{E}[N]$ η αναγωγή του modulo $\mathfrak{p}$, και $\tilde{K}$ το σταθερό σώμα του

$$\{\sigma \in \mathrm{Gal}(\overline{\mathbb{F}_p(t)}/\mathbb{F}_p(t) : \sigma(P) = \pm P\},$$

όπου $\overline{\mathbb{F}_p(t)}$ συμβολίζει μια διαχωρίσιμη αλγεβρική κλειστότητα του $\mathbb{F}_p(t)$. Η καμπύλη $\widetilde{X_1(N)}$ χαρακτηρίζεται μέχρι ισομορφισμού ως η ομαλή προβολική καμπύλη υπέρ του $\mathbb{F}_p$ με σώμα συναρτήσεων το $\tilde{K}$. Επιπλέον θεωρώντας την $\tilde{E}$ ως ελλειπτική καμπύλη υπέρ του $\tilde{K}$ έχουμε μια συνάρτηση αναγωγής

$$\tilde{E}(\bar{\mathbb{F}}_p)_{S'} \to \mathrm{Ell}_1(N)(\bar{\mathbb{F}}_p)_{S'}$$

$$x \mapsto [(\tilde{E})_x, (\tilde{P})_x]$$

για κάθε υποσύνολο $S' \subset \mathbb{P}^1(\bar{\mathbb{F}})$ που περιέχει τις θέσεις όπου η $\tilde{E}$ έχει κακή αναγωγή. Έστω S η αντίστροφη εικόνα του S' υπό την συνάρτηση αναγωγής $\mathbb{P}^1(\bar{\mathbb{Q}}) \to \mathbb{P}^1(\bar{\mathbb{F}})$. Το διάγραμμα αναγωγής:

$$\begin{array}{ccc} X_1(N)(\bar{\mathbb{Q}})_S & \longrightarrow & \mathrm{Ell}_1(N)(\bar{\mathbb{Q}}) \\ \downarrow & & \downarrow \\ \widetilde{X_1(N)}(\bar{\mathbb{F}})_{S'} & \longrightarrow & \mathrm{Ell}_1(N)(\bar{\mathbb{F}}_p) \end{array}$$

είναι αντιμεταθετικό.

Στην συνέχεια θα πάρουμε S' να είναι το σύνολο των θέσεων όπου η $\tilde{E}$ έχει κακή η supersingular (όχι ordinary) αναγωγή. Το σύνολο S' είναι πεπερασμένο. Η αντιμεταθετικότητα του παραπάνω διαγράμματος μας επιτρέπει να αντικαταστήσουμε τα $\mathrm{Ell}_1(N)(\bar{\mathbb{Q}})_{\mathrm{ord}}$ και $\mathrm{Ell}_1(N)(\bar{\mathbb{F}}_p)$ με $X_1(N)(\bar{\mathbb{Q}})_S$ και $\widetilde{X_1(N)}(\bar{\mathbb{F}})_{S'}$.

Θα συμβολίζουμε με $\widetilde{J_1(N)}$ την αναγωγή της $J_1(N)$ modulo p και θα την ταυτίζουμε με την Ιακωβιανή της $\widetilde{X_1(N)}$. Υπάρχει ένα αντιμεταθετικό διάγραμμα:

$$\begin{array}{ccc} \mathrm{Div}^0(X_1(N)(\bar{\mathbb{Q}}_S) & \longrightarrow & J_1(N)(\bar{\mathbb{Q}}) \\ \downarrow & & \downarrow \\ \mathrm{Div}^0(\widetilde{X_1(N)}(\bar{\mathbb{F}}_{S'}) & \xrightarrow{\alpha} & \widetilde{J_1(N)}(\bar{\mathbb{F}}_p) \end{array}$$

όπου τα κάθετα βέλη συμβολίζουν την αναγωγή modulo $\mathfrak{p}$ και τα οριζόντια στέλνουν divisors βαθμού 0 στις κλάσεις τους.

Αφού το S' είναι πεπερασμένο η α είναι επί. Έστω $L \in J_1(N)(\bar{\mathbb{Q}}$ ένα σημείο με τάξη δύναμη του ℓ. Θα πρέπει να δείξουμε ότι

$$(T_p - \sigma_{\mathfrak{p}} + p\langle p\rangle\sigma_{\mathfrak{p}}^{-1})(L) = 0. \tag{4.10}$$

Στην πραγματικότητα αρκεί να το δείξουμε μετά από αναγωγή modulo $\mathfrak{p}$ αφού αυτή είναι 1-1 στην ℓ-torsion. Γράφουμε $\tilde{L} = \alpha(\tilde{D})$ με $D \in \mathrm{Div}^0(X_1(N)(\bar{\mathbb{Q}}_S)$. Σύμφωνα με την πρόταση 4.13.2 το $(T_p - \sigma_{\mathfrak{p}} + p\langle p\rangle\sigma_{\mathfrak{p}}^{-1})(D)$ είναι 0 modulo $\mathfrak{p}$ και συνεπώς ισχύει η (4.10).

□

Κλείνοντας το κεφάλαιο αυτό, σημειώνουμε το ακόλουθο θεώρημα του Igusa, το οποίο συνδέει τα μοντέλα για τις modular καμπύλες $X_0(N)$ (και με αντίστοιχο τρόπο και για τις $X_1(N)$) με την συμπεριφορά των μοντέλων αυτών στις αναγωγές modulo τους πρώτους διαιρέτες του N.

Θεώρημα 4.13.4 (Igusa)**.** *Οι modular καμπύλες $X_0(N)$ επιδέχονται ένα μη-ιδιόμορφο προβολικό μοντέλο το οποίο ορίζεται με εξισώσεις υπέρ του σώματος $\mathbb{Q}$, του οποίου η αναγωγή modulo πρώτους $p \nmid N$ είναι επίσης μη ιδιόμορφη.*

Ισοδύναμα υπάρχει μια proper, smooth καμπύλη

$$\mathcal{X}_0(N) \to \mathrm{Spec}(\mathbb{Z}[1/N]),$$

ώστε για κάθε $p \in \mathrm{Spec}(\mathbb{Z}[1/N])$ η αναγωγή $\mathcal{X}_0(N) \times_{\mathrm{Spec}Z} \bar{\mathbb{F}}_p$ να είναι ο moduli χώρος καμπυλών με μία κυκλική υποομάδα τάξης N.

Κεφάλαιο 5

L-συναρτήσεις και modularity

Σε αυτό το τελευταίο κεφάλαιο, προσεγγίζουμε την μελέτη των ελλειπτικών καμπυλών και των modular forms μέσω των L-συναρτήσεων. Υπάρχουν πολλοί λόγοι για να υιοθετήσει κανείς μια τέτοια προσέγγιση. Για παράδειγμα, αν μας δοθεί μια πολλαπλασιαστική ακολουθία a_n, τότε η σειρά Dirichlet

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s}$$

συμπεριφέρεται «καλά» ως προς την πολλαπλασιαστικότητα. Επίσης, θα δούμε ότι η ίδια η πολλαπλασιαστικότητα που εμφανίζεται στους συντελεστές Fourier μιας modular μορφής (ξέρουμε, από την πρόταση 4.5.20, ότι αυτή η πολλαπλασιαστικότητα υπάρχει για τις κανονικοποιημένες ομοιόμορφες ιδιομορφές των τελεστών Hecke) συνεπάγεται την ύπαρξη ενός γινομένου Euler για την modular μορφή. Επίσης, θα ορίσουμε μια L-σειρά για κάθε καμπύλη E/K, και θα δούμε πως η βαθύτερη μελέτη της συνάφειας μεταξύ των ελλειπτικών καμπυλών και των modular forms μας οδηγεί στην μελέτη των σχέσεων ανάμεσα στις L-σειρές τους. Εδώ υπάρχει ένα πλήθος από πολύ σημαντικά αποτελέσματα και εικασίες, με εξέχον το διάσημο Modularity Θεώρημα. Στην τελευταία παράγραφο αυτού του κεφαλαίου εξηγούμε το θεώρημα αυτό, δίνοντας ορισμένες ισοδύναμες διατυπώσεις του.

Σημείωση: Χρησιμοποιούμε τον συνήθη συμβολισμό s για την μιγαδική μεταβλητή μιας συνάρτησης που ορίζεται σε ένα δεξί ημιεπίπεδο του $\mathbb{C}$ της μορφής $\Re(\cdot) > a$, καθώς και τον $s = \sigma + \mathrm{i}t$ για το πραγματικό και το φανταστικό μέρος της μεταβλητής.

5.1 L-συναρτήσεις

Αρχικώς, θα μελετήσουμε κάποια γενικά στοιχεία της θεωρίας των σειρών Dirichlet και των L-συναρτήσεων που θα μας φανούν χρήσιμα στην συνέχεια.

Το πρότυπο της μελέτης των L-συναρτήσεων είναι η συνάρτηση ζ του Rie-

mann, που για $\Re(s) > 1$ δίνεται από τον τύπο

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Η $\zeta(s)$, ως μιγαδική συνάρτηση που ορίζεται στο ημιεπίπεδο $\Re(s) > 1$, έχει τρεις σημαντικές ιδιότητες:

(i) Όπως έδειξε ο Euler, έχει ένα (Euler) γινόμενο

$$\zeta(s) = \prod_{p} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

(ii) Επεκτείνεται μερόμορφα σε όλο το μιγαδικό επίπεδο (Riemann). Η $\zeta(s)$ επιδέχεται αναλυτική επέκταση στο $\mathbb{C}$, εκτός από το $s = 1$, όπου έχει απλό πόλο.

(iii) Ικανοποιεί μια συναρτησιακή εξίσωση. Πιο συγκεκριμμένα, αν θέσουμε $\xi(s) = \pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})\zeta(s)$, τότε

$$\xi(s) = \xi(1 - s).$$

Ως εκ τούτου, μπορούμε να δώσουμε τον εξής αφελή «ορισμό» :
«Μια μιγαδική συνάρτηση που ορίζεται σε κάποιο ημιεπίπεδο $\Re(s) > a$ του $\mathbb{C}$ μέσω μιας Dirichlet σειράς θα λέγεται L-συνάρτηση αν ικανοποιεί τις εξής ιδιότητες:

(i) Έχει ένα Euler γινόμενο.

(ii) Επεκτείνεται μερόμορφα σε όλο το $\mathbb{C}$.

(iii) Ικανοποιεί μια συναρτησιακή εξίσωση.»

Για να πάρει κανείς περισσότερες L-συναρτήσεις, πρέπει να ορίσει τους χαρακτήρες Dirichlet. Υπενθυμίζουμε εδώ τα πολύ βασικά στοιχεία της θεωρίας τους.

Ορισμός 5.1.1. *Ένα χαρακτήρας Dirichlet modulo N είναι ένα ομομορφισμός πολλαπλασιαστικών ομάδων*

$$\chi : G_N \equiv G = \left(\frac{\mathbb{Z}}{N\mathbb{Z}}\right)^* \longrightarrow \mathbb{C}^*.$$

Το κατά σημείο γινόμενο χαρακτήρων Dirichlet είναι χαρακτήρας Dirichlet. Το σύνολο των χαρακτήρων Dirichlet modulo N με το κατά σημείο γινόμενο έχει δομή ομάδας, η οποία ονομάζεται δυική της G και συμβολίζεται με $\hat{G}$. Το ταυτοτικό στοιχείο της $\hat{G}$ είναι ο χαρακτήρας που απεικονίζει κάθε στοιχείο της G στο 1, και συμβολίζεται με 1_N. Η G είναι πεπερασμένη, άρα η εικόνα της θα είναι μέσα στην S^1, και η αντίστροφη απεικόνιση ενός χαρακτήρα Dirichlet είναι η συζυγής της:

$$\chi^{-1}(n) = \bar{\chi}(n) = \overline{\chi(n)}.$$

Γενικά, ισχύει ότι

$$G \simeq \hat{G}$$

και άρα οι Dirichlet χαρακτήρες της G είναι $\phi(N)$ στο πλήθος. Επίσης, ισχύουν οι σχέσεις ορθογωνιότητας

$$\sum_{n\in G}\chi(n)=\begin{cases}\phi(N) & \chi=1_N,\\ 0 & \chi\neq 1_N\end{cases}$$

$$\sum_{\chi\in\hat{G}}\chi(n)=\begin{cases}\phi(N) & n=1,\\ 0 & n\neq 1\end{cases}$$

Αν $d|N$, τότε κάθε χαρακτήρας Dirichlet χ modulo d επάγει έναν χαρακτήρα χ_N modulo N μέσω της σχέσης

$$\chi_N(n \mod N)=\chi(n \mod d),$$

για κάθε n σχετικά πρώτο προς τον N. Αν $\pi_{N,d}:G_N\to G_d$ είναι η συνήθης προβολή, η παραπάνω σχέση γράφεται $\chi_N=\chi\circ\pi_{N,d}$. Για κάθε χαρακτήρα χ modulo N, υπάρχει ένας ελάχιστος d διαιρέτης του N τέτοιος ώστε $\chi=\chi_d\circ\pi_{N,d}$, ο οποίος λέγεται conductor του χαρακτήρα. Ένας χαρακτήρας modulo N λέγεται ανάγωγος αν ο conductor του είναι ο N.

Επίσης, κάθε χαρακτήρας modulo N επεκτείνεται σε μια συνάρτηση $(\mathbb{Z}/N\mathbb{Z})\to\mathbb{C}$ θέτοντας $\chi(n)=0$ για τα μη αντιστρέψιμα στοιχεία της $(\mathbb{Z}/N\mathbb{Z})$, και σε μια συνάρτηση $\chi:\mathbb{Z}\to\mathbb{C}$ με φυσικό τρόπο. Η επαγόμενη συνάρτηση αυτή είναι πλήρως πολλαπλασιαστική. Ορίζουμε επίσης το άθροισμα Gauss που αντιστοιχεί στον χαρακτήρα χ modulo N να είναι το

$$\tau(\chi)=\sum_{n=0}^{N-1}\chi(n)e^{2\pi in/N}.$$

Το $\tau(\chi)$ ενός πρωταρχικού χαρακτήρα χ ικανοποιεί την σχέση $\tau(\chi)\overline{\tau(\chi)}=N$. Ειδικότερα, το άθροισμα Gauss ενός πρωταρχικού χαρακτήρα δεν μηδενίζεται.

Κατασκευή 5.1.2. Ένας λόγος που ενδιαφερόμαστε για τους χαρακτήρες Dirichlet είναι διότι διασπούν τους χώρους $M_k(\Gamma_1(N))$ σε ευθέα αθροίσματα υποχώρων που μελετώνται ανεξάρτητα. Για κάθε χαρακτήρα Dirichlet modulo N ορίζουμε τον χ-ιδιόχωρο του $M_k(\Gamma_1(N))$ να είναι ο

$$M_k(N,\chi)=\{f\in M_k(\Gamma_1(N)) : f|_k\gamma=\chi(d_\gamma)f,\forall\gamma\in\Gamma_0(N)\},$$

όπου με d_γ συμβολίζουμε το κάτω δεξιά στοιχείο του πίνακα γ. Ειδικότερα, $M_k(N,1_N)=M_k(\Gamma_0(N))$. Επίσης, $M_k(N,\chi)=\{0\}$, εκτός αν $\chi(1)=(-1)^k$. Ο χώρος $M_k(\Gamma_1(N))$ γράφεται τώρα ως ευθύ άθροισμα

$$M_k(\Gamma_1(N))=\bigoplus_{\chi}M_k(N,\chi),$$

και το ίδιο ισχύει για τις cusp forms και τους χώρους πηλίκα τους, δηλαδή τις σειρές Eisenstein .

Ορισμός 5.1.3. *Τα στοιχεία του $M_k(N,\chi)$ ονομάζονται modular forms βάρους k και ύψους N που αντιστοιχούν στον χαρακτήρα χ.*

Για κάθε χαρακτήρα Dirichlet modulo N ορίζουμε την Dirichlet L-συνάρτηση του να είναι η

$$L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}=\prod_p\left(1-\frac{\chi(p)}{p^s}\right)^{-1},$$

η οποία συγκλίνει για $\Re(s)>1$, και όπου η δεύτερη ισότητα εκφράζει το γεγονός ότι η $L(s,\chi)$ έχει ένα γινόμενο Euler, το οποίο έπεται από την πολλαπλασιαστικότητα του χ. Η $L(s,\chi)$ επεκτείνεται ολόμορφα στο s-επίπεδο για $\chi\neq 1_N$, και για $\chi=1_N$ παίρνουμε την

$$L(s,1_N)=\zeta(s)\prod_{p|N}(1-p^{-s}).$$

Όταν $\chi(-1)=1$, η $L(s,\chi)$ ικανοποιεί την συναρτησιακή εξίσωση

$$\pi^{-\frac{s}{2}}\Gamma(\frac{s}{2})N^sL(s,\chi)=\pi^{-\frac{1-s}{2}}\Gamma(\frac{1-s}{2})\tau(\chi)L(1-s,\overline{\chi}),$$

και για $\chi(-1)=-1$, η $L(s,\chi)$ ικανοποιεί την συναρτησιακή εξίσωση

$$\pi^{-\frac{s+1}{2}}\Gamma(\frac{s+1}{2})N^sL(s,\chi)=-\mathrm{i}\pi^{-\frac{2-s}{2}}\Gamma(\frac{2-s}{2})\tau(\chi)L(1-s,\overline{\chi}).$$

Άρα, οι σειρές Dirichlet ορίζουν όντως L-συναρτήσεις κατά τον «ορισμό» που αρχικά δώσαμε. Πριν κλείσουμε την γενική μελέτη των L-συνηαρτήσεων, θα χρειαστούμε ακόμα μία έννοια, αυτήν του μετασχηματισμού Mellin.

Έστω a_n μια ακολουθία μιγαδικών αριθμών, με $a_n=O(n^k)$ για κάποιο k. Θεωρούμε τις a_n είτε ως συντελεστές της δυναμοσειράς

$$f(q)=\sum_{n=1}^{\infty}a_nq^n,$$

η οποία συγκλίνει απολύτως τουλάχιστον για $|q|<1$, είτε ως συντελεστές της σειράς Dirichlet

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

Το ερώτημα που έχουμε να απαντήσουμε είναι ποια σχέση συνδέει τις $f(q)$ και $L(s,f)$. Την απάντηση δίνει ο μετασχηματισμός Mellin. Υπενθυμίζουμε ότι η $\Gamma(s)$ συνάρτηση δίνεται από τον τύπο

$$\Gamma(s)=\int_0^{\infty}e^{-x}x^{s-1}dx,\Re(s)>0.$$

Πρόταση 5.1.4 (Μετασχηματισμός Mellin). *Για κάθε $c>0$ και $x>0$,*

$$e^{-x}=\frac{1}{2\pi\mathrm{i}}\int_{\sigma-\mathrm{i}\infty}^{\sigma+\mathrm{i}\infty}\Gamma(s)x^{-s}ds.$$

(Το ολοκλήρωμα λαμβάνεται κατά μήκος της κάθετης γράμμης).

Απόδειξη. Η συνάρτηση $\Gamma(s)$ είναι μερόμορφη στο $\mathbb{C}$, και οι πόλοι της είναι απλοί, ακριβώς στα σημεία $s = -n$, $n = 0, 1, 2, ...$, με αντίστοιχα ολοκληρωτικά υπόλοιπα $(-1)^n/n!$.

Θεωρούμε τώρα το ολοκλήρωμα πάνω στην σφαίρα του Riemann, και χρησιμοποιώντας το θεώρημα ολοκληρωτικών υπολοίπων παίρνουμε

$$\begin{aligned}\int_{\sigma-\mathrm{i}\infty}^{\sigma+\mathrm{i}\infty} \Gamma(s)x^{-s}ds &= 2\pi\mathrm{i}\sum_{n=0}^{\infty} res_{s=-n}x^{-s}\Gamma(s) = 2\pi\mathrm{i}\sum_{n=0}^{\infty}\frac{(-x)^n}{n!} \\ &= 2\pi\mathrm{i}\cdot e^{-x},\end{aligned}$$

οπότε έχουμε το ζητούμενο. □

Πρόταση 5.1.5. *Έστω a_n μια ακολουθία μιγαδικών αριθμών με $a_n = O(n^k)$ για κάποιο σταθερό k. Έστω επίσης οι σειρές $f(q)$ και $L(s)$ που δίνονται από τους τύπους*

$$f(x) = \sum_{n=1}^{\infty} a_n e^{-nx}, L(s, f) \equiv L(s) = \sum_{n=1}^{\infty}\frac{a_n}{n^s}.$$

Τότε

$$\Gamma(s)L(s) = \int_0^{\infty} f(x)x^{s-1}dx$$

για $\Re(s) > \max\{0, k+1\}$, και

$$f(x) = \frac{1}{2\pi\mathrm{i}}\int_{\sigma-\mathrm{i}\infty}^{\sigma+\mathrm{i}\infty} L(s)\Gamma(s)x^{-s}ds$$

για $\Re(s) > \max\{0, k+1\}$ και $x > 0$.

Απόδειξη. (Σκιαγράφηση) Τελείως τυπικά, έχουμε

$$\int_0^{\infty} f(x)x^{s-1}dx = \int_0^{\infty}\sum_{n=1}^{\infty} a_n e^{-nx}x^{s-1}dx$$

$$= \sum_{n=1}^{\infty}\int_0^{\infty} a_n e^{-nx}x^{s-1}dx = \sum_{n=1}^{\infty}\frac{a_n}{n^s}\int_0^{\infty} e^{-x}x^{s-1}dx$$

$$= \sum_{n=1}^{\infty}\frac{a_n}{n^s}\Gamma(s) = \Gamma(s)L(s).$$

Η μόνη δικαιολόγιση που χρειάζεται για τους υπολογισμούς αυτούς είναι στην αλλαγή του αθροίσματος με την ολοκλήρωση, η οποία είναι επιτρεπτή λόγω της ομοιόμορφης σύγκλισης του ολοκληρώματος.

Ο δεύτερος ισχυρισμός τώρα έπεται από την πρόταση 5.1.4. □

Οι συναρτήσεις f και $L(s, f)\Gamma(s)$ ονομάζονται οι μετασχηματισμοί Mellin η μία της άλλης. Πιο γενικά:

Ορισμός 5.1.6. *Ο μετασχηματισμός Mellin της συνάρτησης $f(x)$ είναι η συνάρτηση $g(s)$ που δίνεται από τον τύπο*

$$g(s) = \int_{x=0}^{\infty} f(x)x^{s-1}dx$$

Τότε, για τις f και g ισχύει ο τύπος αντιστροφης

$$f(x) = \frac{1}{2\pi \mathrm{i}} \int_{\sigma-\mathrm{i}\infty}^{\sigma+\mathrm{i}\infty} g(s)x^{-s}ds.$$

Σαν επόμενο βήμα, θα εφαρμόσουμε την θεωρία που αναπτύξαμε εν συντομία εδώ στις ελλεπτικές καμπύλες και (ιδιαίτερα) στις modular forms.

5.2 L-σειρές ελλειπτικών καμπυλών

Το πρώτο βήμα τώρα είναι να δούμε με ποιον τρόπο μπορούμε να αντιστοιχίσουμε σε μια ελλειπτική καμπύλη E μια L-συνάρτηση. Θέλουμε η L να περιέχει όσο γόνεται περισσότερη πληροφορία για την συμπεριφορά της E. Η ιδέα είναι ότι μια ελλειπτική καμπύλη που ορίζεται πάνω από το K θα πρέπει να χαρακτηρίζεται από το πλήθος των λύσεων της στις αναγωγές της.

Στην παράγραφο 9 του δευτέρου κεφαλαίου αντιστοιχίσαμε στην E μια Z-συνάρτηση. Υπενθυμίζουμε τα αποτελέσματα που δώσαμε εκεί για πεπερασμένα σώματα, υιοθετόντας τον γενικότερο συμβολισμό των εκτιμήσεων.

Έστω E/K μια ελλειπτική καμπύλη, όπου K ένα σώμα αριθμών, και μια εκτίμηση $\upsilon \in M_K^0$, στην οποία η E έχει καλή αναγωγή. Συμβολίζουμε με k_υ το αντίστοιχο residue σώμα του K στην υ, με $\tilde{E}_\upsilon$ την αναγωγή της E στην υ και με $q_\upsilon = |k_\upsilon|$ την νόρμα του πρώτου ιδεώδους που αντιστοιχεί στην υ. Η Z-συνάρτηση της $\tilde{E}_\upsilon/k_\upsilon$ είναι η δυναμοσειρά

$$Z(\tilde{E}_\upsilon/k_\upsilon; T) = exp\left(\sum_{n=1}^{\infty} |\tilde{E}_\upsilon(k_{\upsilon,n})|\frac{T^n}{n}\right),$$

όπου $k_{\upsilon,n}$ είναι η μοναδική επέκταση του k_υ βαθμού n. Οι εικασίες του Weil που δείξαμε για τις ελλειπτικές καμπύλες (θεώρημα 2.9.8) λένε ότι

$$Z(\tilde{E}_\upsilon/k_\upsilon; T) = \frac{L_\upsilon(T)}{(1-T)(1-q_\upsilon T)},$$

όπου $L_\upsilon(T) = 1 - a_\upsilon T + q_\upsilon T^2 \in \mathbb{Z}[T]$ και $a_\upsilon = q_\upsilon + 1 - |\tilde{E}_\upsilon(k_\upsilon)|$ το ίχνος του Frobenius. Επεκτείνουμε τον ορισμό του $L_\upsilon(T)$ έτσι ώστε να συμπεριλαμβάνει και τις κακές αναγωγές, θέτοντας $L_\upsilon(T) = 1-T$ αν η E έχει split πολλαπλασιαστική αναγωγή στην υ, $L_\upsilon(T) = 1+T$ αν η E έχει nonsplit πολλαπλασιαστική αναγωγή στην υ και $L_\upsilon(T) = 1$ αν η E έχει προσθετική (ασταθή) αναγωγή στην υ.

Σε κάθε περίπτωση, παρατηρούμε ότι ισχύει

$$L_\upsilon(1/q_\upsilon) = |\tilde{E}_{ns}(k_\upsilon)|/q_\upsilon.$$

Ορισμός 5.2.1. *Η L-σειρά της E/K είναι το Euler γινόμενο*

$$L(s, E/K) = \prod_{\upsilon \in M_K^0} L_\upsilon(q_\upsilon^{-s})^{-1}.$$

Το γινόμενο που ορίζει την $L(s, E/K)$ συγκλίνει και ορίζει μια αναλυτική συνάρτηση για $\Re(s) > \frac{3}{2}$. Αυτό έπεται από το γεγονός ότι $|a_\upsilon| \leq 2\sqrt{q_\upsilon}$. Για να ορίζει η L-σειρά μιας ελλειπτικής καμπύλης μια L-συνάρτηση, θα πρέπει κατ' αρχάς να επεκτείνεται μερόμορφα σε όλο το $\mathbb{C}$.

Εικασία 5.2.2 (Hasse-Weil)**.** *Η $L(s, E/K)$ επεκτείνεται αναλυτικά στο $\mathbb{C}$ και ικανοποιεί μια συναρτησιακή εξίσωση που συσχετίζει την τιμή $L(s, E/K)$ με την τιμή $L(2 - s, E/K)$.*

Οι Deuring και Weil έδειξαν πως η εικασία 5.2.2 αληθεύει αν η E έχει CM, οι Eichler και Shimura έδειξαν ότι αληθεύει για $E/\mathbb{Q}$ οι οποίες επιδέχονται modular παραμετρικοποίηση, οπότε το Modularity Θεώρημα (παράγραφος 5.4. παρακάτω) συνεπάγεται την 5.2.2 για τις ρητές ελλειπτικές καμπύλες.

Ο conductor της E/K είναι ένα (ακέραιο) ιδεώδες του K που συγκεντρώνει την πληροφορία για τις κακές αναγωγές της E, και είναι αναλλοίωτος για ισογενείς ελλειπτικές καμπύλες. Για την απλοποίηση του επόμενου ορισμού, υποθέτουμε πως $\text{χαρ}(K) \neq 2, 3$.

Ορισμός 5.2.3. *Για κάθε $\upsilon \in M_K^0$ ορίζουμε τον εκθέτη f_υ του conductor της E στην υ να είναι $f_\upsilon = 0$ αν η E έχει καλή αναγωγή στην υ, $f_\upsilon = 1$ αν η E έχει πολλαπλασιαστική αναγωγή στην υ και $f_\upsilon = 2$ αν η E έχει προσθετική αναγωγή στην υ.*

Ορισμός 5.2.4. *Ο (γεωμετρικός) conductor της E/K είναι το ακέραιο ιδεώδες*

$$N_{E/K} = \prod_{\upsilon \in M_K^0} \mathfrak{p}_\upsilon^{f_\upsilon}.$$

όπου $\mathfrak{p}$ είναι το πρώτο ιδεώδες του R που αντιστοιχεί στην υ.

Επικεντρωνόμαστε τώρα στην περίπτωση $K = \mathbb{Q}$. Στην περίπτωση αυτήν, μπορούμε να υποθέσουμε πως ο $N_E = N_{E/\mathbb{Q}}$ είναι ένας θετικός ακέραιος. Συμβολίζουμε με $L(s, E)$ την $L(s, E/\mathbb{Q})$. Η $L(s, E)$ γράφεται στην μορφή

$$L(s, E) = \prod_{p \nmid \Delta} \frac{1}{1 - a_p p^{-s} + p^{1-2s}} \prod_{p|\Delta} \frac{1}{1 - ap^{-s}},$$

όπου $a = 0, 1$ ή -1 ανάλογα με την αναγωγή που έχει η καμπύλη στον p.

Ορίζουμε την συνάρτηση

$$\xi_E(s) = N_E^{s/2}(2\pi)^{-s}\Gamma(s)L(s, E).$$

Η $\xi_E(s)$ μας επιτρέπει να διατυπώσουμε πιο ισχυρά την 5.2.2. Όμως, αφού η 5.2.2. ισχύει για $K = \mathbb{Q}$, το επόμενο μπορούμε να το αποκαλέσουμε θεώρημα.

Θεώρημα 5.2.5. *Έστω $E/\mathbb{Q}$ μια ελλειπτική καμπύλη. Η $\xi_E(s)$ έχει μια αναλυτική επέκταση σε ολόκληρο το μιγαδικό επίπεδο και ικανοποιεί μια συναρτησιακή εξίσωση της μορφής*

$$\xi_E(s) = \pm\xi_E(2 - s),$$

(όπου το πρόσημο εξαρτάται από την τάξη της ρίζας της $L(s, E)$ στο $s = 1$).

Μια ακόμη σημαντική εικασία σχετικά με την συμπεριφορά της $L(s, E)$ είναι η ακόλουθη διάσημη

Εικασία 5.2.6 ((Birch-Swinnerton-Dyer, Ασθενής μορφή)**.** *Έστω $E/\mathbb{Q}$. Η τάξη της ρίζας της $L(s,E)$ στο σημείο $s=1$ είναι ίση με την rank της $E(\mathbb{Q})$.*

Η εικασία αυτή μπορεί να φαίνεται κάπως αυθαίρετη. Διατυπώνουμε έναν διαισθητικό λόγο για την ερμηνεία αυτής της εικασίας: όσο μεγαλύτερο είναι το rank μιας ρητής ελλειπτικής καμπύλης, τόσες περισσότερες λύσεις έχει στο $\mathbb{Q}$, οπότε αναμένει κανείς να έχει περισσότερες λύσεις στις αναγωγές της E modulo τους περισσότερους πρώτους p, δηλαδή η τιμή $|E(\mathbb{F}_p)|$ αναμένεται να είναι μεγάλη για τους περισσότερους πρώτους p. Όμως

$$\begin{aligned} L(1,E) &= \prod_{p\nmid\Delta}\frac{1}{1-a_pp^{-1}+p^{-1}}\prod_{p|\Delta}\frac{1}{1-ap^{-1}} \\ &= \prod_{p\nmid\Delta}\frac{p}{p+1-a_p}\prod_{p|\Delta}\frac{1}{1-ap^{-1}} \\ &= \prod_{p\nmid\Delta}\frac{p}{|E(\mathbb{F}_p)|}\prod_{p|\Delta}\frac{1}{1-ap^{-1}}. \end{aligned}$$

Οι όροι στο δεύτερο γινόμενο είναι πεπερασμένοι, οπότε το «πόσο γρήγορα» φθίνει η $L(s,E)$ στο $s=1$ (άρα δηλαδή και το πόσο μεγαλύτερη είναι η τάξη της ρίζας στο $s=1$) είναι ανάλογο του μεγέθους της $|E(\mathbb{F}_p)|$, για όλους τους πρώτους p. Βέβαια, το επιχείρημα αυτό είναι κάπως αυθαίρετο. Κατ΄ αρχάς, δεν ξέρουμε προς το παρόν κατά πόσον η $L(s,E)$ ορίζεται στο σημείο $s=1$. Όπως θα δούμε παρακάτω, αυτό έπεται από το θεώρημα των Wiles και Taylor.

Η εικασία (Birch-Swinnerton-Dyer ισχυροποιείται περισσότερο. Σ΄ αυτό το σημείο, παραθέτουμε απλώς την ισχυρότερη αυτήν διατύπωση της, χωρίς να εισέλθουμε σε περαιτέρω λεπτομερή σχολιασμό της ερμηνείας των ποσοτήτων που εμφανίζονται:

Εικασία 5.2.7 ((Birch-Swinnerton-Dyer, Ισχυρή μορφή)**.** *Έστω $E/\mathbb{Q}$, και r η τάξη της $E(\mathbb{Q})$. Τότε*

$$\lim_{s\to1}\frac{L(s,E)}{(s-1)^r}=\frac{2^r\Omega|TS(E/\mathbb{Q})R(E/\mathbb{Q})\Pi_pc_p}{|E_{tors}(\mathbb{Q})^2|}.$$

Αρκετές ειδικές περιπτώσεις είναι αποδεδειγμένες για την εικασία αυτήν.
1) Το 1977 οι Coates και Wiles έδειξαν πως αν η $E/\mathbb{Q}$ έχει μιγαδικό πολλαπλασιασμό και η $E(\mathbb{Q})$ είναι άπειρη, τότε $L(1,E)=0$.
2) Το 1986 οι Gross και Zagier έδειξαν πως αν η $E/\mathbb{Q}$ είναι modular (παράγραφος 5.4) και η $L(s,E)$ έχει απλή ρίζα στο $s=1$, τότε η $E(\mathbb{Q})$ είναι άπειρη.

Το Modularity Θεώρημα βέβαια εγγυάται πλέον πως κάθε $E/\mathbb{Q}$ είναι modular, οπότε η συνθήκη αυτή μπορεί να αγνοηθεί.

Ορισμός 5.2.8. *Μια μιγαδική συνάρτηση f είναι φραγμένη σε κάθετες λωρίδες αν για κάθε ζευγάρι πραγματικών $a<b$, η $f(s)$ είναι φραγμένη στην λωρίδα $a\le\Re(s)\le b$ καθώς $\Im(s)\to\pm\infty$.*

Έστω λοιπόν τώρα μια $E/\mathbb{Q}$, και N ο γεωμετρικός conductor της. Μεταφέροντας την $L(s,E)$ στον μοναδιαίο δίσκο στην μορφή $\sum a_nq^n$, ορίζουμε, για κάθε πρώτο p που δεν διαιρεί τον N και για πρωταρχικό χαρακτήρα χ στο $\mathbb{Z}/p\mathbb{Z}$ την L-σειρά

$$\Lambda(s,E,\chi)=N^{s/2}\left(\frac{p}{2\pi}\right)^s\Gamma(s)\sum_{n=1}^{\infty}a_n\chi(n)q^n\equiv N^{s/2}\left(\frac{p}{2\pi}\right)^s\Gamma(s)Ł(s,E,\chi),$$

όπου

$$Ł(s,E)=\sum_{n=1}^{\infty}a_nq^n.$$

Εικασία 5.2.9 (Ισχυρή Hasse-Weil)**.** *Για κάθε πρώτο p σχετικά πρώτο προς τον N και για κάθε πρωταχικό χαρακτήρα χ στο $\mathbb{Z}/p\mathbb{Z}$, η $\Lambda(s,E,\chi)$ επεκτείνεται αναλυτικά στο $\mathbb{C}$. είναι φραγμένη σε οριζόντιες λωρίδες και ικανοποιεί την συναρτησιακή εξίσωση*

$$\Lambda(s,E,\chi)=\pm\frac{\tau(\chi)\chi(-N)}{\tau(\overline{\chi})}N^{1-s}\Lambda(2-s,E,\overline{\chi}).$$

Θα δούμε στην παράγραφο 5.4 τον τρόπο με τον οποίον συνδέεται η Ισχυρή εικασία Hasse-Weil με το Modularity Θεώρημα.

Οι σειρές $Ł(s,E,\chi)$ ονομάζονται twists της $Ł(s,E)$. Στην επόμενη παράγραφο θα εφαρμόσουμε την ίδια διαδικασία στις L-σειρές των modular μορφών, και θα δούμε με ποιον τρόπο οι twisted L-σειρές οδηγούν στο σημαντικό θεώρημα του Weil.

5.3 L-σειρές modular μορφών

Θα δούμε τώρα πως μπορούμε να ορίσουμε μια φυσιολογική L-σειρά για μια $f\in M_k(\Gamma_1(N))$. Έστω

$$f(z)=\sum_{n=0}^{\infty}a_nq^n$$

το Fourier ανάπτυγμα της f. Η αριθμητική συνάρτηση που καθορίζει την f είναι η ακολουθία $(a_n)_{n=1}^{\infty}$, οπότε ο επόμενος ορισμός είναι αναμενόμενος.

Ορισμός 5.3.1. *Η Dirichlet σειρά της f είναι η*

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

Παρατηρείστε ότι ο ορισμός αυτός «ξεχνάει» τον όρο a_0. Η συμπεριφορά της $L(s,f)$ θα δούμε ότι καθορίζεται ουσιαστικά από το μέγεθος των a_n καθώς και τις πολλαπλασιαστικές τους ιδιότητες. Πιο συγκεκριμμένα, έχουμε την εξής

Πρόταση 5.3.2. *Αν $f\in S_k(\Gamma_1(N))$, τότε η $L(s,f)$ συγκλίνει απολύτως για κάθε s με $\Re(s)>\frac{k}{2}+1$. Αν η f δεν είναι cusp, τότε συγκλίνει απολύτως για $\Re(s)>k$.*

Απόδειξη. Όμοια με την τεχνική που αποδείξαμε τις προτάσεις 4.3.21 και 4.3.22, δείχνει κανείς ότι αν $f\in S_k(\Gamma_1(N))$ τότε $a_n=O(n^{k/2})$, και αν η f δεν είναι cusr τότε $a_n=O(n^{k-1})$ (αλλιώς, μπορούμε να δείξουμε πρώτα ότι η ποσότητα $\Im(z)^{k/2}|f(z)|$ είναι φραγμένη στο $\mathbb{H}$). Αν f cusp, ο υπολογισμός

$$\left|\frac{a_n}{n^s}\right|=O(n^{\frac{k}{2}-\Re(s)}),$$

δίνει το ζητούμενο, και αντίστοιχα ο υπολογισμός

$$\left|\frac{a_n}{n^s}\right|=O(n^{k-1-\Re(s)})$$

για f που δεν είναι cusp (δηλαδή είναι Eisenstein). □

Άρα η $L(s,f)$ συγκλίνει όντως σε κάποιο ημιεπίπεδο του $\mathbb{C}$ της επιθυμητής μορφής. Η επόμενη πρόταση δείχνει ότι η $L(s,f)$ μιας κανονικοποιημένης ομοιόμορφης ιδιομορφής των τελεστών Hecke έχει και ένα Euler γινόμενο.

Πρόταση 5.3.3. *Έστω μια δυναμοσειρά*

$$f = \sum_{n=1}^{\infty} a_n q^n$$

με $a_1 = 1$. *Τότε, οι συντελεστές ικανοποιούν τις ταυτότητες*

(i)
$$a_n a_m = a_{nm}$$
για $\mu\kappa\delta(m,n) = 1$ *και,*

(ii)
$$a_{p^{n+1}} = a_p a_{p^n} - p^{2k-1} a_{p^{n-1}}$$
για p *πρώτο και* $n \geq 1$ *αν και μόνο αν η* $L(s,f)$ *έχει το Euler γινόμενο*

$$L(s,f) = \prod_p \frac{1}{1 - a_p p^{-s} + p^{2k-1-2s}}.$$

Απόδειξη. Υποθέτουμε πρώτα ότι η ακολουθία a_n ικανοποιεί τις δοσμένες πολλαπλασιαστικές ιδιότητες. Η πρώτη ιδιότητα μας επιτρέπει να γράψουμε της $L(s,f)$ ως γινόμενο πάνω στους πρώτους:

$$L(s,f) = \sum_{n=1}^{\infty} \frac{a_n}{n^s} = \prod_p \sum_{m=0}^{\infty} \frac{a_{p^m}}{p^{ms}}.$$

Πολλαπλασιάζοντας το μέσα άθροισμα με $1 - a_p p^{-s} + p^{2k-1-2s}$, παίρνουμε

$$(1 - a_p p^{-s} + p^{2k-1-2s}) \left(\sum_{m=0}^{\infty} \frac{a_{p^m}}{p^{ms}} \right)$$

$$= \sum_{m=0}^{\infty} \frac{a_{p^m}}{p^{ms}} - \sum_{m=0}^{\infty} \frac{a_p a_{p^m}}{p^{(m+1)s}} + \sum_{m=0}^{\infty} \frac{a_{p^m}}{p^{2k-1-(m+2)s}}$$

$$= a_1 + \frac{a_p}{p^s} - \frac{a_p a_1}{p^s} + \sum_{m=2}^{\infty} (a_{p^m} - a_p a_{p^{m-1}} + a_{p^{m-2}} p^{2k-1}) \frac{1}{p^{ms}} = 1,$$

όπου στην τελευταία ισότητα χρησιμοποιηθήκε η δεύτερη ιδιότητα και το ότι $a_1 = 1$. Άρα, έχουμε την ανάλυση της $L(s,f)$ στο Euler γινόμενο

$$L(s,f) = \prod_p \sum_{m=0}^{\infty} \frac{a_{p^m}}{p^{ms}} = \prod_p \frac{1}{1 - a_p p^{-s} + p^{2k-1-2s}}.$$

Είναι απλό να δει κανείς τώρα ότι το επιχείρημα μας λειτουργεί και αντίστροφα. □

Είδαμε λοιπόν πως υπό καλές προυποθέσεις η $L(s,f)$ έχει και γινόμενο Euler. Το τελευταίο βήμα είναι να δείξουμε πως η $L(s,f)$ επεκτείνεται μερόμορφα στο $\mathbb{C}$ και ικανοποιεί μια συναρτησιακή εξίσωση. Πρώτα θα μελετήσουμε στις επόμενες προτάσεις την περίπτωση της $\Gamma(1)$, η οποία αναλύθηκε πλήρως από τον Hecke:

Πρόταση 5.3.4. *Έστω f μια cusp form ύψους $2k$ για την $\Gamma(1)$. Τότε:*

(i) *Η $L(s,f)$ επεκτείνεται μερόμορφα στο $\mathbb{C}$.*

(ii) *Αν θέσουμε*
$$\Lambda(s,f) = (2\pi)^{-s}\Gamma(s)L(s,f),$$
τότε
$$\Lambda(2k-s,f) = (-1)^k\Lambda(s,f)$$
για κάθε $s \in \mathbb{C}$.

Απόδειξη. Στο ολοκλήρωμα
$$\Gamma(s) = \int_0^\infty e^{-x}x^{s-1}dx, \Re(s) > 0,$$
που ορίζει την συνάρτηση $\Gamma(s)$, αντικαθιστούμε όπου x με $2\pi nx$, και παίρνουμε τον τύπο
$$n^{-s} = (2\pi)^s\Gamma(s)^{-1}\int_0^\infty x^{s-1}e^{-2\pi nx}dx.$$
Έστω $f(z) = \sum a_n q^n$. Πολλαπλασιάζοντας τον παραπάνω τύπο για το n^{-s} με a_n και αθροίζοντας για $n \geq 1$ παίρνουμε
$$\begin{aligned} L(s,f) = \sum_{n=1}^\infty \frac{a_n}{n^s} &= \sum_{n=1}^\infty \left(a_n(2\pi)^s\Gamma(s)^{-1}\int_0^\infty x^{s-1}e^{-2\pi nx}dx\right) \\ &= (2\pi)^s\Gamma(s)^{-1}\int_0^\infty x^{s-1}\sum_{n=1}^\infty a_n e^{-2\pi nx}dx \\ &= (2\pi)^s\Gamma(s)^{-1}\int_0^\infty x^{s-1}f(\mathrm{i}x)dx. \end{aligned}$$
Όμως, $a_n = O(n^k)$, άρα η ποσότητα
$$\sum_{n=1}^\infty a_n \int_0^\infty x^{s-1}e^{-2\pi nx}dx$$
συγκλίνει απολύτως για $\Re(s) > k+1$, δηλαδή επιτρέπεται η αλλαγή σειράς και ολοκληρώματος. Σπάμε το ολοκλήρωμα για την $L(s,f)$ σε δύο μέρη. Για $x > 1$, το ολοκλήρωμα θα συγκλίνει για κάθε $s \in \mathbb{C}$. Για $x < 1$, το αντικαθιστούμε από το $1/x$, και καθώς η f ικανοποιεί την συναρτησιακή σχέση
$$f\left(\frac{\mathrm{i}}{x}\right) = (\mathrm{i}x)^{2k}f(\mathrm{i}x),$$
έχουμε
$$(2\pi)^{-s}\Gamma(s)L(s,f) = \int_0^\infty x^{s-1}f(\mathrm{i}x)dx$$

$$= \int_0^1 x^{s-1} f(\mathrm{i}x)dx + \int_1^\infty x^{s-1} f(\mathrm{i}x)dx$$

$$= \int_\infty^1 \left(\frac{1}{x}\right)^{s-1} f\left(\frac{\mathrm{i}}{x}\right) d\left(\frac{1}{x}\right) + \int_1^\infty x^{s-1} f(\mathrm{i}x)dx$$

$$= \int_1^\infty (-1)^k x^{2k-s-1} f(\mathrm{i}x)dx + \int_1^\infty x^{s-1} f(\mathrm{i}x)dx$$

$$= \int_1^\infty \left((-1)^k x^{2k-s-1} + x^{s-1}\right) f(\mathrm{i}x)dx$$

$$\Longrightarrow L(s,f) = (2\pi)^s \Gamma(s)^{-1} \int_1^\infty \left((-1)^k x^{2k-s-1} + x^{s-1}\right) f(\mathrm{i}x)dx,$$

η οποία ισχύει τουλάχιστον για $\Re(s) > k+1$.

Όμως, η $\Gamma(s)^{-1}$ είναι ολόμορφη στο $\mathbb{C}$, και το ολοκλήρωμα συγκλίνει απόλυτα και ομοιόμορφα στα συμπαγή του $\mathbb{C}$ (παρατηρείστε πως επειδή η f είναι cusp, η $|f(\mathrm{i}x)|$ συγκλίνει στο 0 με τάξη $e^{-2\pi x}$ για $x \to \infty$). Άρα, αυτό το ολοκλήρωμα δίνει την επιθυμητή αναλυτική επέκταση της $L(s,f)$ στο $\mathbb{C}$.

Τέλος, επειδή η ποσότητα

$$\epsilon(s,x) = x^{s-1} + (-1)^k x^{2k-s-1}$$

ικανοποιεί την σχέση $\epsilon(2k-s,x) = (-1)^k \epsilon(s,x)$, έπεται ότι η ποσότητα

$$\Lambda(s,f) = (2\pi)^{-s}\Gamma(s)L(s,f) = \int_1^\infty \epsilon(s,x) f(\mathrm{i}x)dx$$

ικανοποιεί την ίδια σχέση $\Lambda(2k-s,f) = (-1)^k \Lambda(s,f)$. □

Η επόμενη πρόταση εξετάζει την περίπτωση που η modular μορφή δεν είναι cusp.

Πρόταση 5.3.5. *Έστω μια $f \in M_{2k}(\Gamma(1))$ ($k \geq 2$), η οποία δεν είναι cusp form. Τότε, η $L(s,f)$ επεκτείνεται αναλυτικά στο $\mathbb{C}$ εκτός των σημείων $s = 0$, όπου έχει απλό πόλο, και $s = 2k$, στο οποίο έχει απλό πόλο με ολοκληρωτικό υπόλοιπο*

$$res_{s=2k} L(s,f) = \frac{(-1)^k a_0 (2\pi)^{2k}}{\Gamma(2k)},$$

Επίσης, αν θέσουμε $\Lambda(s,f) = (2\pi)^{-s}\Gamma(s)L(s,f)$, τότε ικανοποιείται η συναρτησιακή εξίσωση

$$\Lambda(2k-s,f) = (-1)^k \Lambda(s,f)$$

Απόδειξη. Χρησιμοποιώντας την ίδια μέθοδο με αυτήν που εφαρμόσαμε στην πρόταση 5.3.4 για τις cusp forms, συνάγουμε τον γενικότερο τύπο

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

$$= \int_1^\infty \left((-1)^k x^{2k-s-1} + x^{s-1}\right)\left(f(\mathrm{i}x) - a_0\right) dx - a_0 \left(\frac{1}{s} + \frac{(-1)^k}{2k-s}\right).$$

Και πάλι αυτός ο τύπος, που ισχύει αρχικά για $\Re(s) > 2k$, δίνει την επιθυμητή αναλυτική επέκταση στο $\mathbb{C}$, τους πόλους, τα ολοκληρωτικά υπόλοιπα και την συναρτησιακή σχέση. □

Για την περίπτωση που $f \in S_k(\Gamma_1(N))$, ο Mellin μετασχηματισμός g της f επεκτείνεται και πάλι αναλυτικά σε ολόκληρο το μιγαδικό επίπεδο, και ικανοποιεί και πάλι μια αντίστοιχη συναρτησιακή εξίσωση. Πιο συγκεκριμμένα, αν $f \in S_k(\Gamma_1(N))$, θέτουμε $\Lambda_N(s) = N^{s/2}(2\pi)^s g(s)$, και η $\Lambda_N(s)$ ικανοποιεί μιας εξίσωση της μορφής

$$\Lambda_N(s) = \pm\Lambda_N(k-s).$$

Περισσότερες λεπτομέρειες σχετικά με αυτήν την περίπτωση υπάρχουν στο [Diamond-Shurman, [8], κεφ.5].

Ένα σημαντικό ερώτημα είναι κατά πόσον ισχύουν οι αντίστροφοι ισχυρισμοί των παραπάνω. Σε αυτήν την κατεύθυνση, υπάρχουν τα αντίστροφα θεωρήματα των Hecke και Weil.

Στην απόδειξη των προτάσεων 5.3.4 και 5.3.5 είδαμε πόσο σημαντικό ρόλο παίζει η εξίσωση

$$f\left(-\frac{1}{z}\right) = (z)^{2k} f(z)$$

για την απόδειξη της συναρτησιακής σχέσης. Μια ολόμορφη f όμως είναι modular form για την $\Gamma(1)$ αν ικανοποιεί την παραπάνω σχέση και είναι 1-περιοδική. Η 1-περιοδικότητα μας επέτρεψε να ορίσουμε την L-σειρά της f, και η δεύτερη συναρτησιακή σχέση έδωσε την συναρτησιακή σχέση της L-σειράς. Ο Hecke έδειξε ότι η συναρτησιακή σχέση της L-σειράς δίνει την συναρτησιακή σχέση της f, και άρα η f είναι modular.

Το θεώρημα αυτό γενίκευσε το 1967 ο Weil στην περίπτωση της $\Gamma_0(N)$. Στην περίπτωση αυτήν έχουμε περισσότερες σχέσεις να ελέγξουμε για την f, μιας και έχουμε περισσότερους γεννήτορες. Στο υπόλοιπο αυτής της παραγράφου ασχολούμαστε με αυτά τα αποτελέσματα.

Έστω $a = (a_1, a_2, a_3, ...)$ μια ακολουθία μιγαδικών αριθμών τέτοια ώστε $a_n = O(n^M)$ για κάποια πραγματική σταθερά $M > 0$ και $k > 0$ ένας ακέραιος. Ορίζουμε τις συναρτήσεις

$$L(s,a) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}, \Lambda(s,a) = (2\pi)^{-s}\Gamma(s)L(s,a), f(z,a) = \sum_{n=1}^{\infty} a_n q^n,$$

όπου $q = e^{2\pi i z}$. Η $L(s,a)$ συγκλίνει για $\Re(s) > M+1$, και η $f(z)$ συγκλίνει για $\Im(z) > 0$. Εφαρμόζωντας τον μετασχηματισμό Mellin έχουμε το

Θεώρημα 5.3.6 (Hecke). *Έστω μια ακολουθία $a = (a_n)_{n=0}^{\infty}$ με $a_n = O(n^M)$ για κάποια πραγματική σταθερά $M > 0$ και $L(s,a)$, $\Lambda(s,a)$ και $f(z,a)$ όπως παραπάνω. Έστω ότι η $\Lambda(s,a)$ έχει αναλυτική επέκταση σε όλο το $\mathbb{C}$, είναι φραγμένη σε λωρίδες και ικανοποιεί την συναρτησιακή εξίσωση*

$$\Lambda(2k-s,a) = (-1)^k \Lambda(s,a).$$

Τότε, η $f(z) = f(z,a)$ είναι cusp form ύψους $2k$ για την $\Gamma(1)$. Αν η $L(s,a)$ έχει και ένα Euler γινόμενο (όπως στην πρόταση 5.3.3), τότε η $f(z)$ είναι κανονικοποιημένη ιδιομορφή των τελεστών Hecke.

Απόδειξη. Για την απόδειξη θα χρειαστεί να χρησιμοποιήσουμε το εξής θεώρημα από την μιγαδική ανάλυση:

Θεώρημα 5.3.7 (Αρχή Phragmen-Lindelöf)). *Έστω $f(z)$ μια συνάρτηση η οποία είναι ολόμορφη σε ένα άνω κομμάτι μιας λωρίδας, δηλαδή σε ένα χωρίο της μορφής*

$$\sigma_1 \leq \Re(s) \leq \sigma_2, \Im(s) > c,$$

έτσι ώστε για να ισχύει $\sigma_1 \leq \sigma \leq \sigma_2$ να υπάρχει ένας $a > 0$ για τον οποίον να ισχύει

$$f(\sigma + \mathrm{i}t) = O(e^{t^a}).$$

Έστω ακόμα ότι για $\sigma = \sigma_1$ ή $\sigma = \sigma_2$ ισχύει

$$f(\sigma + \mathrm{i}t) = O(t^M),$$

για κάποιο $M > 0$. Τότε

$$f(\sigma + \mathrm{i}t) = O(t^M)$$

ομοιόμορφα στο σ για κάθε $\sigma \in [\sigma_1, \sigma_2]$.

Επίσης, θα χρειαστούμε την εξής Stirling-εκτίμηση για την $\Gamma(s)$:

$$|\Gamma(\sigma + \mathrm{i}i)| \sim \sqrt{2\pi}|t|^{\sigma-1/2}e^{-\pi|t|/2}$$

για $t \to \pm\infty$.

Παρατηρείστε ότι ο τελευταίος ισχυρισμός του θεωρήματος έπεται από την πρόταση 5.3.3 (ή το πόρισμα 5.3.8 παρακάτω). Προχωράμε τώρα στην απόδειξη του κύριου ισχυρισμού.

Αφού η f ορίζεται από ένα Fourier ανάπτυγμα, ισχύει $f(z+1) = f(z)$. Η κρίσιμη ιδιότητα λοιπόν την οποία πρέπει να δείξουμε είναι, όπως σημειώσαμε και προηγουμένως, ότι η f ικανοποιεί την συναρτησιακή εξίσωση

$$f\left(-\frac{1}{z}\right) = (z)^{2k} f(z).$$

Θα δείξουμε ότι

$$f(\mathrm{i}y) = (-1)^k y^{-2k} f\left(\frac{\mathrm{i}}{y}\right),$$

για $y > 0$. Τότε, θα έχουμε ότι η ολόμορφη συνάρτηση

$$f\left(-\frac{1}{z}\right) - (z)^{2k} f(z)$$

θα μηδενίζεται σε ένα σύνολο που έχει σημεία συσσώρευσης, άρα θα πρέπει να είναι ταυτοτικά μηδενική. Για την περίπτωση $z = \mathrm{i}y$ εφαρμόζουμε τον τύπο αντιστροφής του Mellin. Για σ αρκετά μεγάλο θα έχουμε

$$\int_0^\infty f(\mathrm{i}y) y^{s-1} dy = \Lambda(s, a),$$

οπότε, από τον τύπο αντιστροφής του Mellin και την συναρτησιακή σχέση της $\Lambda(s, a)$ παίρνουμε

$$f(\mathrm{i}y) = \frac{1}{2\pi\mathrm{i}} \int_{\sigma-\mathrm{i}\infty}^{\sigma+\mathrm{i}\infty} \Lambda(s, a) y^{-s} ds = (\mathrm{i})^{2k} \frac{1}{2\pi\mathrm{i}} \int_{\sigma-\mathrm{i}\infty}^{\sigma+\mathrm{i}\infty} \Lambda(2k - s, a) y^{-s} ds.$$

Η $\Lambda(\sigma+\mathrm{i}t,a)$, για σ αρκετά μεγάλο φθίνει γρήγορα καθώς $t\to\infty$, επειδή είναι γινόμενο απολύτως συγκλινουσών σειρών Dirichlet με μια Γ συνάρτηση που φθίνει γρήγορα από τον τύπο του Stirling. Αν το σ είναι αρκετά μικρότερο από το 0, χρησιμοποιούμε την συναρτησιακή σχέση που συνδέει την $\Lambda(\sigma+\mathrm{i}t,a)$ με την $\Lambda(2k-\sigma-\mathrm{i}t,a)$, η οποία φθίνει γρήγορα καθώς $t\to\infty$. Άρα, αν υποθέσουμε ότι η $\Lambda(s,a)$ είναι φραγμένη σε οριζόντιες λωρίδες, τότε, από το Phragmen-Lindelöf, έπεται ότι $\Lambda(\sigma+\mathrm{i}t,a)\to 0$ καθώς $t\to\infty$ ομοιόμορφα για σ σε οποιοδήποτε συμπαγές. Αυτό μας επιτρέπει, εφαρμόζωντας το θεώρημα του Cauchy, να αντικαταστήσουμε το σ με το $k-\sigma$ και το s με το $k-s$, οπότε και παίρνουμε τον τύπο

$$f(\mathrm{i}y)=(\mathrm{i})^{2k}y^{-2k}\frac{1}{2\pi\mathrm{i}}\int_{\sigma-\mathrm{i}\infty}^{\sigma+\mathrm{i}\infty}\Lambda(s,a)y^s ds=(-1)^k y^{-2k}f\left(\frac{\mathrm{i}}{y}\right).$$

Τέλος, το ότι η f είναι cusp είναι απλό, αφού το Fourier ανάπτυγμα της ξεκινάει από το $a_1q+\ldots$ και η απόδειξη είναι πλήρης. □

Για το θεώρημα του Weil θα χρειαστούμε πρώτα τους εξής ορισμούς: για κάθε $m>0$ θεωρούμε τον πρωταρχικό χαρακτήρα χ στην $(\mathbb{Z}/m\mathbb{Z})^*$, και επεκτείνουμε τον χ στην $\mathbb{Z}/m\mathbb{Z}$ κατά τα γνωστά. Γράφουμε

$$L(s,a,\chi)=\sum_{n=1}^{\infty}\frac{a_n\chi(n)}{n^s},\Lambda(a,f,\chi)=(2\pi)^{-s}\Gamma(s)L(s,a,\chi),$$

$$f(z,a,\chi)=\sum_{n=1}^{\infty}a_n\chi(n)q^n.$$

Με τον ίδιο ακριβώς τρόπο που δείξαμε την πρόταση 5.3.3, αποδεικνύεται το ελαφρώς γενικότερο

Πόρισμα 5.3.8. *Έστω μια $f\in M_k(N,\chi)$,*

$$f=\sum_{n=1}^{\infty}a_nq^n.$$

Τα ακόλουθα είναι ισοδύναμα:
α) Η f είναι κανονικοποιημένη ομοιόμορφη ιδιομορφή.
β) Η $L(s,f,\chi)$ έχει γινόμενο Euler:

$$L(s,f,\chi)=\prod_p\frac{1}{1-a_pp^{-s}+\chi(p)p^{k-1-2s}}.$$

Θεώρημα 5.3.9. *Έστω $f\in M_{2k}(\Gamma_0(N)$ με*

$$f\Big|_k\begin{pmatrix}0&-1\\N&0\end{pmatrix}=\pm(-1)^k.$$

Τότε, για κάθε N τέτοιο ώστε μκδ$(m,N)=1$, η $\Lambda(a,f,\chi)$ ικανοποιεί την συναρτησιακή εξίσωση:

$$\Lambda(s,a,\chi)=\pm\frac{\tau(\chi)\chi(-N)}{\tau(\overline{\chi})}N^{k-s}\Lambda(2k-s,a,\overline{\chi}).$$

Απόδειξη. [Bump, [5], κεφ.1]. □

Το σημαντικότερο όμως αποτέλεσμα είναι το αντίστροφο του θεωρήματος αυτού, το οποίο λέει ότι οι χαρακτήρες μας δίνουν όλες τις απαραίτητες συναρτησιακές εξισώσεις που πρέπει να ικανοποιεί μια ακολουθία ώστε να προέρχεται από μια cusp form της $\Gamma_0(N)$.

Πρώτα, αλλάζουμε πάλι λίγο τον συμβολισμό: αν α είναι ένας πίνακας στην $\mathrm{GL}_2(\mathbb{R})^+$, και f μια συνάρτηση ορισμένη στο $\mathbb{H}$, ορίζουμε

$$f|_k\alpha = (det\alpha)^{k/2}(cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right).$$

Επίσης, όταν το βάρος k θα είναι σταθεροποιημένο, θα συμβολίζουμε με $f|\alpha$ το $f|_k\alpha$. Για μια απλοποιημένη εκδοχή του αντίστροφου θεωρήματος του Weil, η οποία εξασφαλίζει την ύπαρξη μιας f στο $S_{2k}(\Gamma_0(N))$, παραπέμπουμε στον [Milne, [22], κεφ. 9].

Θεώρημα 5.3.10 (Το αντίστροφο θεώρημα του Weil)**.** *Έστω N ένας θετικός ακέραιος, ψ ένας χαρακτήρας Dirichlet modulo N και $a = (a_0, a_1, a_2, ...)$ και $b = (b_0, b_1, b_2, ..)$ δύο ακολουθίες μιγαδικών αριθμών τέτοιες ώστε $a_n = O(n^M)$ και $b_n = O(n^M)$ για κάποια σταθερά $M > 0$. Αν D είναι ένας ακέραιος σχετικά πρώτος προς τον N και χ έναν πρωταρχικός χαρακτήρας Dirichlet modulo D, ορίζουμε κατά τα γνωστά τις $L(s,a,\chi)$, $\Lambda(s,a,\chi)$, $L(s,b,\overline{\chi})$ και $\Lambda(s,b,\overline{\chi})$. Έστω S ένα πεπερασμένο σύνολο πρώτων που περιέχει τους πρώτους διαιρέτες του N. Υποθέτουμε πως όποτε ο conductor D του χ είναι 1 ή ένας πρώτος $\notin S$, οι $\Lambda(s,a,\chi)$ και $\Lambda(s,b,\overline{\chi})$, οι οποίες ορίζονται αρχικώς για $\Re(s)$ αρκούντως μεγάλο, έχουν αναλυτική επέκταση στο $\mathbb{C}$, είναι φραγμένες σε κάθετες λωρίδες και ικανοποιούν την συναρτησιακή εξίσωση*

$$\Lambda(s,a,\chi) = \mathrm{i}^k \chi(N)\psi(D)\frac{\tau(\chi)^2}{D}(D^2N)^{-s+k/2}\Lambda(k-s,b,\overline{\chi}).$$

Τότε, $f(z,a) \in M_k(\Gamma_0(N),\psi)$.

Σημείωση: Ο Weil απέδειξε μια ελαφρώς γενικότερη μορφή του θεωρήματος 6.3.10, επιτρέποντας στις $\Lambda(s,a,\chi)$ και $\Lambda(s,b,\overline{\chi})$ να έχουν πόλους, το οποίο μπορεί να συμβεί αν η f δεν είναι cusp. Για την απόδειξη θα χρειαστούμε το ακόλουθο λήμμα:

Λήμμα 5.3.11. *Έστω f μια ολόμορφη συνάρτηση στο $\mathbb{H}$ και γ ένα ελλειπτικό στοιχείο της $SL_2(\mathbb{R})$ άπειρης τάξης, τέτοιο ώστε $f|\gamma = f$. Τότε $f \equiv 0$.*

Απόδειξη. (του θεωρήματος 5.3.10) Ξέρουμε πως οι σειρές $f(z,a,\chi)$ και $f(z,b,\overline{\chi})$ συγκλίνουν για $z \in \mathbb{H}$. Θα συμβολίζουμε με $f(z,\chi)$ την $f(z,a,\chi)$ και με $g(z,\chi)$ την $f(z,b,\chi)$.

Το πρώτο βήμα είναι να δείξουμε ότι ο τύπος αντιστροφής του Mellin συνεπάγεται ότι αν ο χ είναι ένας πρωταρχικός χαρακτήρας modulo D, όπου $D = 1$ ή ένας πρώτος $\notin S$, τότε

$$f(\cdot,\chi)\left|\begin{pmatrix} 0 & -1 \\ D^2N & 0 \end{pmatrix}\right. = \chi(-N)\psi(D)\frac{\tau(\chi)}{\tau(\overline{\chi})}g(\cdot,\overline{\chi}) \tag{5.1}$$

$$= \chi(N)\psi(D)\frac{g^2(\chi)}{D}g(\cdot,\overline{\chi}).$$

Η απόδειξη είναι παρόμοια με την απόδειξη του θεωρήματος 6.3.6. Αρκεί να δείξουμε ότι τα δύο μέλη της εξίσωσης ταυτίζονται στο θετικό κομμάτι του φανταστικού άξονα. Για σ αρκετά μεγάλο, έχουμε

$$\int_0^\infty f(\mathrm{i}y,a,\chi)y^{s-1}dy=\Lambda(s,a,\chi),$$

άρα, από τον τύπο αντιστροφής του Mellin:

$$f(\mathrm{i}y,\chi)=\frac{1}{2\pi\mathrm{i}}\int_{\sigma-\mathrm{i}\infty}^{\sigma+\mathrm{i}\infty}\Lambda(s,a,\chi)y^{-s}ds$$

$$=(\mathrm{i})^k\chi(N)\psi(D)\frac{\tau(\chi)^2}{D}\frac{1}{2\pi\mathrm{i}}\int_{\sigma-\mathrm{i}\infty}^{\sigma+\mathrm{i}\infty}(D^2N)^{-s+k/2}\Lambda(k-s,b,\overline{\chi})y^{-s}ds.,$$

όπου η τελευταία ισότητα έπεται από την εξίσωση της υπόθεσης. Όπως στην απόδειξη του θεωρήματος 6.3.6, η Αρχή Phragmen-Lindelöf συνεπάγεται ότι $\Lambda(\sigma+ti,a,\chi)\to 0$ καθώς $t\to 0$ για κάθε σ, επιτρέποντας μας έτσι να αλλάξουμε γραμμή ολοκλήρωσης από τα δεξιά στα αριστερά λόγω του θεωρήματος Cauchy, οπότε, αντικαθιστώντας το $k-\sigma$ με σ, έχουμε

$$f(\mathrm{i}y,\chi)=(\mathrm{i})^k\chi(N)\psi(D)\frac{\tau(\chi)^2}{D}(D^2N)^{-k/2}y^{-k}\frac{1}{2\pi\mathrm{i}}\int_{\sigma-\mathrm{i}\infty}^{\sigma+\mathrm{i}\infty}\Lambda(s,b,\overline{\chi})(D^2Ny)^s ds$$

$$=(\mathrm{i})^k\chi(N)\psi(D)\frac{\tau(\chi)^2}{D}(D^2N)^{-k/2}y^{-k}g\left(\frac{\mathrm{i}}{D^2Ny},\overline{\chi}\right),$$

και έχουμε το ζητούμενο.

Για κάθε D και για κάθε πρωταρχικό χαρακτήρα χ modulo D, αν θεωρήσουμε τον πίνακα

$$w_N=\begin{pmatrix}0&-1\\N&0\end{pmatrix}$$

τότε ισχύουν οι τρεις ακόλουθες εξισώσεις:
α)Αν $f|w_N=g$, τότε

$$f(\cdot,\chi)\left|\begin{pmatrix}0&-1\\D^2N&0\end{pmatrix}\right.$$

$$=\chi(N)\frac{\tau(\chi)}{D}\sum_{r\mod D,(r,D)=1}\chi(r)g\left|\begin{pmatrix}D&-r\\-Nm&s\end{pmatrix}\begin{pmatrix}D&r\\0&D\end{pmatrix}\right. \tag{5.2}$$

όπου $Ds-rNm=1$,
β) Αν $g\in S_k(\Gamma_0(N),\overline{\psi})$, τότε

$$g\left|\begin{pmatrix}D&-r\\-Nm&s\end{pmatrix}\right.=\psi(D)g, \tag{5.3}$$

γ)

$$g(\cdot,\overline{\chi})=\frac{\chi(-1)\tau(\overline{\chi})}{D}\sum_{r\mod D,(r,D)=1}\chi(r)g\left|\begin{pmatrix}D&r\\0&D\end{pmatrix}\right.. \tag{5.4}$$

Οι εξισώσεις (5.2) και (5.4) δεν απαιτούν την ολομορφία των f και g. Οι τρεις αυτές εξισώσεις συνεπάγονται την εξίσωση 5.1 που δείξαμε στην προηγούμενη παράγραφο. Για την ισχύ της (2) χρειάζεται, σε πρώτο στάδιο, η συνθήκη $f|w_N = g$, όμως το εμπόδιο αυτό παρακάμπτεται λόγω της απόδειξης της (5.1).

Έστω ένας πρώτος $D \notin S$. Θέλουμε να δείξουμε ότι οι εξισώσεις (5.1), (5.2) και (5.4) συνεπάγονται την εξίσωση (5.3). Αυτό όμως δεν είναι άμεσο, επειδή θεωρούμε εξισώσεις μόνο για τους πρωταρχικούς χαρακτήρες modulo D. Όμως, ισχύει το εξής: αν $c(r)$ είναι μια συνάρτηση ορισμένη στις μη μηδενικές κλάσεις modulo D, τέτοια ώστε $\sum c(r) = 0$, τότε

$$\sum_{r \mod D,(r,D)=1} c(r) g \left| \begin{pmatrix} D & -r \\ -Nm & s \end{pmatrix} \begin{pmatrix} 1 & r/D \\ 0 & 1 \end{pmatrix} \right.$$

$$= \sum_{r \mod D,(r,D)=1} c(r)\psi(D) g \left| \begin{pmatrix} 1 & r/D \\ 0 & 1 \end{pmatrix} \right. ,$$

όπου, για κάθε r, τα $m = m(r)$ και $s = s(r)$ είναι επιλεγμένα ούτως ώστε να ισχύει $Ds - Nmr = 1$. Αυτό έπεται από το γεγονός ότι η παραπάνω εξίσωση ισχ υει για τους πρωταρχικούς χαρακτήρες $\chi(r)$, οι οποίοι συνιστούν μια βάση του $(D-1)$-διάστατου διανυσματικού χώρου των συναρτήσεων $c(r)$.

Επεκτείνουμε την δεξιά δράση της $\mathrm{GL}_2(\mathbb{R})^+$ στις ολόμορφες συναρτήσεις του $\mathbb{H}$ σε μια δράση της άλγεβρας $\mathbb{C}[\mathrm{GL}_2(\mathbb{R})^+]$. Έστω Ω ο annihilator του g σε αυτόν τον δακτύλιο. Τότε

$$\sum_{r \mod D,(r,D)=1} c(r) \begin{pmatrix} D & -r \\ -Nm & s \end{pmatrix} \begin{pmatrix} 1 & r/D \\ 0 & 1 \end{pmatrix}$$

$$\equiv \sum_{r \mod D,(r,D)=1} c(r)\psi(D) \begin{pmatrix} 1 & r/D \\ 0 & 1 \end{pmatrix} \mod \Omega.$$

Ειδικότερα, αν ο D είναι περιττός, μπορούμε να επιλέξουμε ως συνάρτηση c αυτήν που είναι 1 στις residue κλάσεις του r, -1 στις residue κλάσεις του $-r$ και 0 παντού αλλού. Τότε, έχουμε

$$\left(\begin{pmatrix} D & -r \\ -Nm & s \end{pmatrix} - \psi(D) \right) \begin{pmatrix} 1 & r/D \\ 0 & 1 \end{pmatrix}$$

$$\equiv \left(\begin{pmatrix} D & r \\ Nm & s \end{pmatrix} - \psi(D) \right) \begin{pmatrix} 1 & r/D \\ 0 & 1 \end{pmatrix} \mod \Omega. \tag{5.5}$$

Υποθέτουμε τώρα πως οι D και s είναι διαφορετικοί πρώτοι που δεν ανήκουν στο S, και τέτοιοι ώστε $Ds \equiv 1 \mod N$. Επιλέγουμε r και m ούτως ώστε να ισχύει $Ds - Nmr = 1$. Παίνρουμε έτσι και την εξίσωση

$$\left(\begin{pmatrix} s & -r \\ -Nm & D \end{pmatrix} - \psi(s) \right) \begin{pmatrix} 1 & r/s \\ 0 & 1 \end{pmatrix}$$

$$\equiv \left(\begin{pmatrix} s & r \\ Nm & D \end{pmatrix} - \psi(s) \right) \begin{pmatrix} 1 & r/s \\ 0 & 1 \end{pmatrix} \mod \Omega. \tag{5.6}$$

Πολλαπλασιάζοντας από δεξία την εξίσωση (5.5) με τον πίνακα

$$\begin{pmatrix} 1 & r/D \\ 0 & 1 \end{pmatrix}$$

παίρνουμε

(5.7)
$$\left(\begin{pmatrix} D & -r \\ -Nm & s \end{pmatrix} - \psi(D)\right)\begin{pmatrix} 1 & 2r/D \\ 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} D & r \\ Nm & s \end{pmatrix} - \psi(D) \mod \Omega,$$

και πολλαπλασιάζοντας την εξίσωση (5.6) από δεξιά με

$$-\psi(D)\begin{pmatrix} 1 & r/s \\ 0 & 1 \end{pmatrix}\begin{pmatrix} D & -r \\ -Nm & s \end{pmatrix}\begin{pmatrix} 1 & 2r/D \\ 0 & 1 \end{pmatrix},$$

παίρνουμε

$$-\psi(D)\left(\begin{pmatrix} s & -r \\ -Nm & D \end{pmatrix} - \psi(s)\right)\begin{pmatrix} 1 & 2r/s \\ 0 & 1 \end{pmatrix}\begin{pmatrix} D & -r \\ -Nm & s \end{pmatrix}\begin{pmatrix} 1 & 2r/D \\ 0 & 1 \end{pmatrix}$$

(5.8)
$$\equiv \left(\begin{pmatrix} D & -r \\ -Nm & s \end{pmatrix} - \psi(D)\right)\begin{pmatrix} 1 & 2r/D \\ 0 & 1 \end{pmatrix} \mod \Omega$$

ή

$$\left(\begin{pmatrix} D & r \\ Nm & s \end{pmatrix} - \psi(D)\right)\begin{pmatrix} s & -r \\ -Nm & D \end{pmatrix}\begin{pmatrix} 1 & 2r/s \\ 0 & 1 \end{pmatrix}\begin{pmatrix} D & -r \\ -Nm & s \end{pmatrix}$$

(5.9)
$$\times\begin{pmatrix} 1 & 2r/D \\ 0 & 1 \end{pmatrix} \equiv \left(\begin{pmatrix} D & -r \\ -Nm & s \end{pmatrix} - \psi(D)\right)\begin{pmatrix} 1 & 2r/D \\ 0 & 1 \end{pmatrix} \mod \Omega.$$

Συνδυάζοντας τις εξισώσεις (5.8) και (5.9) βλέπουμε ότι

$$\left(\begin{pmatrix} D & r \\ Nm & s \end{pmatrix} - \psi(D)\right)(1 - M) \in \Omega,$$

όπου

$$M = \begin{pmatrix} s & -r \\ -Nm & D \end{pmatrix}\begin{pmatrix} 1 & 2r/s \\ 0 & 1 \end{pmatrix}\begin{pmatrix} D & -r \\ -Nm & s \end{pmatrix}\begin{pmatrix} 1 & 2r/D \\ 0 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 1 & 2r/D \\ -2Nm/s & -3 + 4/Ds \end{pmatrix}.$$

Έστω

$$g_1 = g\left|\begin{pmatrix} D & r \\ Nm & s \end{pmatrix} - \psi(D)g.\right.$$

Τότε, η g_1 είναι ολόμορφη συνάρτηση στο $\mathbb{H}$, και ικανοποιεί την σχέση $g_1 = g_1|M$. Όμως, ο M είναι ελλειπτικός, επειδή $|tr(M)| < 2$, και επιπλέον έχει άπειρη τάξη. Από το λήμμα 5.3.11, έπεται ότι $g_1 = 0$.

Δείχνουμε τώρα ότι $g \in M_k(\Gamma_0(N), \overline{\psi})$. Θα δείξουμε ότι

$$g\left|\begin{pmatrix} a & b \\ Nc & d \end{pmatrix}\right. = \psi(a)g.$$

Παραπάνω, δείξαμε την σχέση αυτήν για a και d πρώτους που δεν ανήκουν στο S. Πιο γενικά, το θεώρημα του Dirichlet για πρώτους σε αριθμητικές προόδους εγγυάται την ύπαρξη δύο u και v, τέτοιων ώστε οι $D = a - uNc$ και $s = d - vNc$ να είναι τέτοιοι πρώτοι. Θέτουμε $r = -av + uvNc - ud$, και έχουμε

$$g\left|\begin{pmatrix} a & b \\ Nc & d \end{pmatrix}\right. = g\left|\begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix}\begin{pmatrix} D & r \\ Nc & s \end{pmatrix}\begin{pmatrix} 1 & v \\ 0 & 1 \end{pmatrix}\right. = \psi(D)g = \psi(a)g.$$

Άρα, $g \in M_k(\Gamma_0(N), \overline{\psi})$, το οποίο συνεπάγεται ότι $f \in M_k(\Gamma_0(N), \psi)$. □

Το αποτέλεσμα του Weil θεωρείται, ιστορικά, σημαντικό, επειδή βοήθησε να επαληθευτεί η εικασία Taniyama-Shimura για έναν σημαντικό αριθμό modular μορφών. Περαιτέρω γενικεύσεις του για automorphic αναπαραστάσεις της $\mathrm{GL}(n)$ έχουν αποδειχθεί από τους Langlands, Jacquet, Piatetski-Shapiro, Shalika και Cogdell.

Μπορούμε τώρα να εξηγήσουμε σε κάποιον βαθμό τι λέει ένα από τα σημαντικότερα θεωρήματα που αποδείχθηκαν στην θεωρία αριθμών τα τελευταία χρόνια.

5.4 Το Modularity Θεώρημα

Σε αυτήν την τελευταία παράγραφο περιγράφουμε ορισμένες ισοδύναμες διατυπώσεις του Modularity Θεωρήματος.

Το 1955 πρώτος ο Taniyama είκασε μια σύνδεση των ελλειπτικών καμπυλών και των modular forms, και αργότερα, με την συμβολή του Shimura, μια πιο ξεκάθαρη διατύπωση της εικασίας έγινε ευρέως γνωστή. Το 1967, ο Weil, αποδεικνύοντας το αντίστροφο θεώρημα (θεώρημα 5.3.10) προσέφερε ισχυρές αριθμητικές ενδείξεις για την αλήθεια της. Έτσι, η ακόλουθη εικασία έγινε γνωστή με πολλά διαφορετικά ονόματα, μέχρι την μερική απόδειξη της από τους Wiles και Taylor (για ημιευσταθείς καμπύλες) το 1995, και την πλήρη απόδειξη της το 2001 από τους Breuil, Conrad, Diamond και Taylor ([4]).

Θεώρημα 5.4.1 (Modularity Θεώρημα (Εικασία Taniyama-Shimura-Weil), (Breuil, Conrad, Diamond, Taylor))**.** *Κάθε ελλειπτική καμπύλη E που ορίζεται πάνω από το $\mathbb{Q}$ είναι modular.*

Κατ΄ αρχάς, θα πρέπει να δώσουμε μια ερμηνεία στο πότε μια ρητή ελλειπτική καμπύλη λέγεται modular. Η εικασία αυτή μπορεί να διατυπωθεί με πολλούς διαφορετικούς τρόπους. Ξεκινάμε με έναν που είναι σαφής, όχι όμως ιδιαίτερα διαφωτιστικός.

Θεώρημα 5.4.2 (Modularity Θεώρημα (Μορφή $X_{\mathbb{C}}$))**.** *Έστω E μια μιγαδική ελλειπτική καμπύλη (δηλαδή ένας τόρος) με $j(E) \in \mathbb{Q}$. Τότε, υπάρχει θετικός ακέραιος N και ολόμορφη και επί απεικόνιση f συμπαγών επιφανειών Riemann*

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

Η συνάρτηση του θεωρήματος καλείται modular παραμετρικοποίηση της E. Η διατύπωση αυτή δεν δείχνει καμία σαφή και άμεση σύνδεση με την θεωρία αριθμών.

Κάποιες modular καμπύλες, για παράδειγμα κάποιες της μορφής $X_0(N)$, είναι βέβαια από μόνες τους ελλειπτικές καμπύλες. Μια ελλειπτική καμπύλη που είναι από μόνη της και modular καμπύλη έχει επιπλέον δομή, και μπορεί κανείς να μελετήσει μέσω αυτής την αριθμητική της. Όμως, υπάρχουν πεπερασμένες modular καμπύλες σταθερού γένους, οπότε αυτή η παρατήρηση δεν συνεισφέρει παρά στην μελέτη ελάχιστων καμπυλών. Για την υπέρβαση αυτού του εμποδίου, δίνεται ο ακόλουθος ορισμός.

Ορισμός 5.4.3. *Μια ελλειπτική καμπύλη $E/\mathbb{Q}$ λέγεται modular αν υπάρχει $N > 0$ και μορφισμός επί αλγεβρικών καμπυλών $X_0(N)_{\mathbb{Q}} \to E$ που να ορίζεται πάνω από το $\mathbb{Q}$.*

Ο ορισμός αυτός τώρα αποσαφηνίζει την πρώτη διατύπωση του θεωρήματος (5.4.1), την οποία θα ονομάσουμε μορφή $X_{\mathbb{Q}}$.

Ορισμός 5.4.4. *Ο αναλυτικός conductor της $E/\mathbb{Q}$ είναι ο ελάχιστος $N > 0$ που ικανοποιεί την διατύπωση $X_{\mathbb{Q}}$ του Modularity θεωρήματος.*

Αποδεικνύεται ότι ο αναλυτικός conductor της E είναι καλά ορισμένος στις κλάσεις ισοδυναμίας των ρητών ελλειπτικών καμπυλών, και επιπλέον οι δύο conductors της E εξαρτώνται μόνο στην κλάση ισογένειας της E. Επιπλέον αποδεικνύεται ότι οι δύο conductors είναι ίσοι.

Με χρήση του Eichler-Shimura, το οποίο συνδέει τους τελεστές Hecke με τον μορφισμό του Frobenius, αποδεικνύεται τώρα το ακόλουθο:

Θεώρημα 5.4.5. *Έστω $E/\mathbb{Q}$ μια ελλειπτική καμπύλη με conductor N_E και N ένας θετικός ακέραιος, για τον οποίον υπάρχει ένας μη τετριμμένος μορφισμός πάνω από το $\mathbb{Q}$*

$$a : X_0(N) \longrightarrow E$$

καμπυλών πάνω από το $\mathbb{Q}$. Τότε, για κάποια newform $f \in S_2(\Gamma_0(M_f))$, όπου $M_f | N$, ισχύει

$$a_p(f) = a_p(E)$$

για κάθε πρώτο p που δεν διαιρεί τον $N_E N$.

Απόδειξη. [Diamond, Shurman, κεφ.8]. □

Αυτό τώρα δίνει την ακόλουθη μορφή του Modularity:

Θεώρημα 5.4.6 (Modularity Θεώρημα (Μορφή a_p))**.** *Έστω E μια ελλειπτική καμπύλη που ορίζεται πάνω από το $\mathbb{Q}$, με conductor N. Τότε, υπάρχει μια newform $f \in S_2(\Gamma_0(N))$, τέτοια ώστε*

$$a_p(f) = a_p(E).$$

Άρα, οι ιδιοτιμές των τελεστών Hecke αντιστοιχούν σε λύσεις ελλειπτικών καμπυλών. Επιβεβαιώνεται έτσι ο αρχικός ισχυρισμός πως το αριθμοθεωρητικό ενδιαφέρον των modular μορφών πηγάζει εν μέρει από την αριθμοθεωρητική φύση των συντελεστών Fourier τους.

Το φράγμα

$$|a_p(E)| \leq 2\sqrt{p}$$

που δίνει η αρχή του Hasse αντιστοιχεί στο φράγμα

$$|a_p(f)| \leq 2\sqrt{p}$$

της εικασίας του Ramanujan για τις cusp forms.

Σε κάποιον βαθμό, η a_p-διατύπωση του Modularity θεωρήματος συνδέεται με τον νόμο τετραγωνικής αντιστροφής του Causs.

Εκεί, θεωρώντας την εξίσωση

$$Q : x^2 = d, d \in \mathbb{Z}, d \neq 0,$$

και ορίζοντας το $a_p(Q)$ να είναι το (πλήθος των λύσεων της Q modulo p)-1, δηλαδή το συμβολο Legendre (για $p > 2$), μια διατύπωση του νόμου τετραγωνικής αντιστροφής είναι πως το σύνολο των λύσεων $\{a_p(Q)\}$ είναι ένα σύνολο ιδιοτιμών στον χώρο V_N των συναρτήσεων από τις residue κλάσεις ισοδυναμίας modulo N (όπου $N = 4|d|$), στο $\mathbb{C}$.

Η σύνδεση είναι τώρα σαφής αν θυμηθεί κανείς ότι ορίσαμε τα $a_p(E)$ να είναι εξ΄ ορισμού ίσα με $p + 1$-(πλήθος των λύσεων της καμπύλης E modulo p).

Τέλος, μιας και οι τιμές $a_p(f)$ και $a_p(E)$ ορίζουν τις L-σειρές των f και E, το Modularity θεώρημα στην γλώσσα των L-σειρών παίρνει την ακόλουθη μορφή:

Θεώρημα 5.4.7 (Modularity Θεώρημα(Μορφή L))**.** *Έστω E μια ελλειπτική καμπύλη που ορίζεται πάνω από το $\mathbb{Q}$, με conductor N. Τότε, υπάρχει μια newform $f \in S_2(\Gamma_0(N))$, τέτοια ώστε*

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

Υπάρχουν διάφορες περαιτέρω μορφές του Modularity. Για παράδειγμα, υπάρχουν διατυπώσεις στην γλώσσα των αβελιανών varieties, καθώς και στην θεωρία των Galois αναπαραστάσεων. Η τελευταία, την οποία θα συμβολίσουμε Μορφή R, ήταν αυτή η οποία αποδείχθηκε.

Η σύνδεση της μορφής R με την μορφή L έπεται από ένα θεώρημα του Carayol και ένα θεώρημα του Faltings. Η σύνδεση που κάναμε παραπάνω ανάμεσα στην μορφή L και την $X_{\mathbb{Q}}$ αποδείχθηκε από τον Shimura, βασιζόμενος σε ένα θεώρημα του Faltings. Η σύνδεση της μορφής $X_{\mathbb{C}}$ με την μορφή R οφείλεται στον Mazur.

Η μορφή Lτου Modularity θεωρήματος δείχνει ότι η εικασία Hasse-Weil ισχύει για $K = \mathbb{Q}$, αφού οι $L(s, f)$ επεκτείνονται στο $\mathbb{C}$. Μάλιστα, ισχύει ότι η ισχυρή Hasse-Weil για το $\mathbb{Q}$ είναι ακριβώς ισοδύναμη με το Modularity. Μια σκιαγράφηση της απόδειξης αυτού του αποτελέσματος υπάρχει στον [Milne, [22], κεφ. 11].

Το πιο γνωστό πόρισμα του Modularity θεωρήματος είναι το Τελευταίο θεώρημα του Fermat.

Θεώρημα 5.4.8 (Τελευταίο Θεώρημα του Fermat)**.** *Δεν υπάχρχουν ακέραιοι $x, y, z > 0$ και $n \geq 3$ τέτοιοι ώστε*

$$x^n + y^n = z^n.$$

Ορισμός 5.4.9. *Μια ρητή ελλειπτική καμπύλη E λέγεται ημιευσταθής αν σε κάθε πρώτο που δεν έχει καλή αναγωγή έχει ημιευσταθή αναγωγή.*

Το 5.4.8 προκύπτει ως εξής:

1) Την δεκαετία του ′80 ο Frey είκασε ότι αν οι a, b, c, με $abc \neq 0$, ικανοποιούν την εξίσωση

$$a^p + b^p = c^p$$

για κάποιον πρώτο $p \geq 3$, τότε η ελλειπτική καμπύλη

$$E : y^2 = x(x + a^p)(x - b^p)$$

δεν είναι modular. Το 1987 ο Serre συνέδεσε την εικασία του Frey με τις modular forms, και το 1990 ο Ribet απέδειξε ότι η καμπύλη του Frey δεν είναι modular. Επειδή η καμπύλη του Frey είναι ημιευσταθής, το θεώρημα 5.4.8 έπεται από το θεώρημα των Wiles και Taylor:

Θεώρημα 5.4.10 (Wiles, Taylor, 1995)**.** *Κάθε ημιευσταθής ελλειπτική καμπύλη $E/\mathbb{Q}$ είναι modular.*

Σκοπός μας σε αυτήν την τελευταία παράγραφο ήταν να εξηγήσουμε εν συντομία την βαθύτερη σχέση που υπάρχει ανάμεσα στις ελλειπτικές καμπύλες και τις modular μορφές. Παρόμοιες συνάφειες ανάμεσα στις automorphic forms (γενικεύσεις, όπως είδαμε, των modular forms) και σε γενικότερα γεωμετρικά αντικείμενα της αλγεβρικής γεωμετρίας αποτελούν εικασίες του Προγράμματος Langlands, το οποίο είναι ένα σύνολο από διάφορες εικασίες που επιχειρούν να συνδέσουν την θεωρία Galois με τις automorphic forms και την θεωρία αναπαραστάσεων, και αποτελεί έναν από τους γονιμότερους τομείς έρευνας στην μοντέρνα θεωρία αριθμών.

Βιβλιογραφία

[1] L. V. Ahlfors, *Complex Analysis,* Mc Graw-Hill, 1979

[2] T. Apostol, *Modular Functions and Dirichlet Series in Number Theory,* Springer, Graduate Texts in Mathematics 41, 1976

[3] G. Billing, K. Mahler, *On exceptional points on cubic curves,* J. London Math. Soc. 15 : (32-43), 1940

[4] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises,* J. Amer. Math. Soc., 14(4): (843-939), 2001.

[5] D. Bump, *Automorphic Forms and Representations,* Cambridge University Press, Cambridge Studies in Advanced Mathematics 55, 1998

[6] D. Bump, J. W. Cogdell, D. Gaitsgory, E. de Shalit, E. Kowalski, S. S. Kudla, *An Introduction to the Langlands Program,* Birkhauser, 2004

[7] G. Cornell, J. H. Silverman, G. Stevens, *Modular Forms and Fermat's Last Theorem,* Springer, 1997

[8] F. Diamond, J. Shurman, *A First Course in Modular forms,* Springer, Graduate Texts in Mathematics 228, 2005

[9] H. M. Farkas, I. Kra, *Riemannian Surfaces,* Springer, Graduate Texts in Mathematics 71, 1980

[10] R. Hartshorne, *Algebraic Geometry,* Springer, Graduate Texts in Mathematics 52, 1977

[11] M. Hindry, J. H. Silverman, *Diophantine geometry, An introduction,* Springer, Graduate Texts in Mathematics 201, 2000

[12] J. Harris, I. Morrison, *Moduli of Curves,* Springer, Graduate Texts in Mathematics 187, 1998

[13] J. Igusa, *Kroneckerian model of fields of elliptic modular functions,* Amer. J. Math., 81 : 561-577, 1959

[14] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory,* Springer, Graduate Texts in Mathematics 84, second edition, 1992

[15] G. J. Janusz, *Algebraic Number Fields,* American Mathematical Society, Graduate Studies in Mathematics 7, second edition, 1996

[16] S. Kleinerman, *On the torsion points of elliptic curves & modular abelian varieties,* (Senior thesis)

[17] D. Lorenzini, *An invitation to Arithmetic Geometry,* American Mathematical Society, Graduate Studies in Mathematics 9, 1991

[18] B. Mazur, *Modular Curves and the Eisenstein Ideal,* I.H.E.S. Publications mathematiques, (47), (33-186), 1977

[19] B. Mazur, *Number Theory as Gadfly,* American Mathematical Monthly, Volume 98, Issue 7 : (593-610), 1991

[20] L. Merel, *Bornes pour la Torsion des Courbes Elliptiques sur les Corps des Nombres,* Invent. Math., 124(1-3): 437-449

[21] T. Miyake, *Modular Forms,* Springer, Springer Monographs in Mathematics, 1989

[22] J. S. Milne, *Modular Functions and Modular Forms,* Notes, 2009

[23] J. S. Milne, *Abelian Varieties,* Notes, 2008

[24] L. J. Mordell, *On Mr. Ramanujan's empirical expansions of modular functions,* Proceedings of the Cambridge Philosophical Society 19 : 117-124, 1917

[25] R. Moreno, *Algebraic Fields and Goppa Codes,* Cambridge University Press, Cambridge Tracts in Mathematics, 1991

[26] Y. Petridis, *L-functions,* Notes

[27] J-P. Serre, *A Course in Arithmetic,* Springer, Graduate Texts in Mathematics 7, 1973

[28] J-P. Serre, *Topics in Galois Theory,*

[29] G. Shimura, *Introduction to the Arithmetic Theory of Automorphic Functions,* Iwanami Shoten and Princeton University Press, 1973

[30] J. H. Silverman, *The Arithmetic of Elliptic Curves,* Springer, Graduate Texts in Mathematics 106, 1986

[31] J. H. Silverman, *Advanced Topics in the Arithmetic of Elliptic Curves,* Springer, Graduate Texts in Mathematics 151, 1994.

[32] J. H. Silverman, J. Tate, *Rational points on Elliptic Curves,* Springer, Undergraduate Texts in Mathematics 106,

[33] W. A. Stein, *Modular Forms: A Computational Approach,* AMS, Graduate Studies in Mathematics, Volume 79, 2007

[34] K. Ueno, *Algebraic Geometry 1: From Algebraic Varities to Schemes,* Iwanami Series in Modern Mathematics

[35] L. C. Washington, *Elliptic Curves: Number Theory and Cryptography, second edition* Discrete Mathematics and Its Applications, Chapman and Hall, 2008

[36] A. Weil, *Basic Number Theory,* Springer, 1974

[37] A. Wiles, *Modular elliptic curves and Fermat"s last theorem,* Annals of Mathematics, (2), 141(3): (443-551), 1995

[38] Α. Αγγελάκης, *Απαρίθμηση Σημείων ελλειπτικών καμπυλών σε πεπερασμένα σώματα* (Διπλωματική Εργασία)

[39] Γ. Α. Αντωνιάδης, *Αριθμητική Ελλειπτικών Καμπυλών: Το Θεώρημα του Mordell*

[40] Σ. Καρανικολόπουλος, *Uniformization Ελλειπτικών Καμπυλών* (Διπλωματική Εργασία)

[41] Α. Κοντογεώργης, *Ημιευσταθείς Ελλειπτικές Καμπύλες και το τελευταίο Θεώρημα του Fermat* (Διπλωματική Εργασία)

[42] Μ. Μαλιάκας, *Εισαγωγή στην Μεταθετική Άλγεβρα,* Σοφία, 2008